Körner, Marita

Book

Wirksamer Beschäftigtendatenschutz im Lichte der Europäischen Datenschutz-Grundverordnung (DS-GVO)

HSI-Schriftenreihe, No. 18

Provided in Cooperation with:
Hugo Sinzheimer Institute for Labour and Social Security Law (HSI), Hans Böckler Foundation

Suggested Citation: Körner, Marita (2017) : Wirksamer Beschäftigtendatenschutz im Lichte der Europäischen Datenschutz-Grundverordnung (DS-GVO), HSI-Schriftenreihe, No. 18, ISBN 978-3-7663-6637-5, Bund-Verlag, Frankfurt a. M.

This Version is available at:
https://hdl.handle.net/10419/303094

Marita Körner

Wirksamer Beschäftigtendatenschutz im Lichte der Europäischen Datenschutz-Grundverordnung (DS-GVO)

HSI-Schriftenreihe
Band 18

Marita Körner

Wirksamer Beschäftigtendatenschutz im Lichte der Europäischen Datenschutz-Grundverordnung (DS-GVO)

BUND VERLAG

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

Herstellung: Betina Hunger
Umschlaggestaltung: Neil McBeath, Stuttgart
Satz: Beltz Bad Langensalza GmbH, Bad Langensalza
Druck: CPI books GmbH, Leck
Printed in Germany 2017
ISBN 978-3-7663-6637-5

www.bund-verlag.de

Vorwort

Im April 2016 wurde die neue EU-Datenschutz-Grundverordnung verabschiedet, die am 25. Mai 2018 in Kraft treten wird. Ziel der Grundverordnung ist es, im Lichte der aktuellen Entwicklungen wie Big Data etc., eine zeitgemäße und umfassende Antwort auf Fragen des Datenschutzes zu geben. Ob sie diesem Anspruch gerecht wird, ist schon heute durchaus zweifelhaft. Völlig unstrittig ist jedenfalls, dass sie den nationalen Gesetzgeber zu einer grundlegenden Revision des Datenschutzrechts zwingt.

Der vorliegende Text von Prof. Marita Körner prüft, inwieweit die Grundverordnung die Voraussetzungen eines modernen Datenschutzes erfüllt und beschäftigt sich insbesondere mit den spezifischen Fragen des Beschäftigtendatenschutzrechts. Die Autorin arbeitet dabei heraus, dass Art. 88 Datenschutz-Grundverordnung eine umfassende Öffnungsklausel zur Ausgestaltung des Beschäftigtendatenschutzes durch den nationalen Gesetzgeber enthält. Eine lediglich unveränderte Fortschreibung des heutigen § 32 BDSG würde danach den Vorgaben des Unionsrechts nicht gerecht. Vor diesem Hintergrund plädiert die Autorin für eine umfassende gesetzliche Regelung des Beschäftigtendatenschutzes. Eine Forderung, der wir uns gerne anschließen möchten. In diesem Sinne wünschen wir eine anregende Lektüre.

Dr. Thomas Klebe

Dr. Johannes Heuschmid

Inhaltsverzeichnis

A. Einleitung 9

B. Genese der DS-GVO seit 2012 13

C. Ziele und Hauptinhalte der DS-GVO 15
I. Bisheriger Datenschutz 15
1. Nationale Ebene 15
2. Europäische Ebene 16
3. EU-Grundrechte und nationale Grundrechte: ein ungeklärtes Verhältnis 17
II. Herausforderungen an die Neuregelungen 19
III. Prinzipien und Instrumente der DS-GVO 20
IV. Betroffenenrechte 26
V. Datenschutz-Folgenabschätzung 28
VI. Durchsetzung und Sanktionen 28
VII. Aufsichts- und Auslegungsinstanzen 31
1. Datenschutzbehörden 32
2. Rechtsschutz 35
a) Institutioneller Rechtsschutz 35
b) Individueller Rechtsschutz 35
VIII. Übermittlung an Drittstaaten 38
IX. Fortschritte und Defizite der DS-GVO 40

D. Verhältnis der DS-GVO zum nationalen Datenschutz 45

E. Beschäftigtendatenschutz 48
I. Status quo in Deutschland 48
II. Datenschutz-Grundverordnung (DS-GVO) 49
1. Rechtslage ohne Regelung des deutschen Gesetzgebers 49
2. Art. 88 DS-GVO 50
a) Beschäftigtenbegriff 51
b) „Spezifischere“ (nationale) Regelungen 52
c) Verordnungsrahmen 54
d) Sonderstellung sensibler Daten in Art. 9 DS-GVO 57
e) Bedeutung der Meldepflicht in Art. 88 Abs. 3 DS-GVO 58
3. Betrieblicher Datenschutzbeauftragter 60

4. Datenschutz durch Technik (Privacy by Design) ... 63
5. Konzerndatenverarbeitung ... 65
III. Nationale Regelungsmöglichkeiten für Beschäftigtendatenschutz ... 67
1. EU-Rechtsgrundlage für Beschäftigtendatenschutz ... 67
2. (Erweiterte) Fortgeltung von § 32 BDSG ... 67
3. Beschäftigtendatenschutzgesetz ... 69
a) Erforderlichkeit einer gesetzlichen Regelung ... 69
b) Bisherige Entwürfe ... 70
c) Mindestinhalte einer nationalen Regelung zum Beschäftigtendatenschutz ... 71
aa) Mindestrechte der DS-GVO ... 72
bb) Vorschriften für typische Verarbeitungsformen ... 72
cc) Vorschriften für neue Verarbeitungsformen ... 73
dd) Telekommunikation ... 73
ee) Auffang-Generalklausel ... 73
ff) Einschränkung der Einwilligung ... 73
gg) Verwertungsverbot ... 74
4. Einwilligung als Erlaubnis, Art. 6 Abs. 1 lit. a, Art. 7 DS-GVO ... 74
a) Einwilligung als Ausdruck der informationellen Selbstbestimmung ... 74
b) Einwilligung als Fiktion ... 75
c) Einwilligung im Beschäftigungsverhältnis ... 76
d) Handlungsmöglichkeiten des nationalen Gesetzgebers bei der Einwilligung ... 79
aa) Grundsätze ... 79
bb) Sensible Daten, Art. 9 DS-GVO ... 83
IV. Handlungsspielraum der Betriebs- und Tarifvertragsparteien ... 84
1. Kollektivvereinbarungen als „spezifischere Vorschriften“ ... 84
2. Verbandsklagerecht, Art. 80 DS-GVO ... 87

F. Ergebnisse und Schlussfolgerungen ... 91

I. Allgemeine Ziele der DS-GVO ... 91
II. Beschäftigtendatenschutz ... 93

Literaturverzeichnis ... 97

A. Einleitung

Der Datenschutz ist ein junges Rechtsgebiet – das erste Datenschutzgesetz der Welt, das des Bundeslandes Hessen, datiert von 1970.[1] Das Thema erlebte eine erste Hochzeit in den 1980er Jahren, insbesondere durch das Volkszählungsurteil des Bundesverfassungsgerichts (BVerfG), das aus den Art. 2 Abs. 1 und Art. 1 Abs. 1 GG ein Recht auf informationelle Selbstbestimmung ablas. Danach muss jeder Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen können.[2]

In dieser Epoche der Datenverarbeitung, vor 40 Jahren also, erfolgte Datenverarbeitung in Rechenzentren mit Großrechnern. Personenbezogene Daten sammelte vor allem der Staat, demgegenüber es den Einzelnen durch Datenverarbeitungsvorgaben zu schützen galt. Aus dieser Anfangszeit stammt der Grundsatz des Verbots mit Erlaubnisvorbehalt, wonach die Erhebung, Speicherung und Verarbeitung personenbezogener Daten gesetzlich oder durch Einwilligung des Betroffenen gerechtfertigt sein muss. Nach einem Datenschutzjahrzehnt in den 1980er Jahren geriet das Thema aus dem Blick der Öffentlichkeit, also der Betroffenen. Entsprechend zäh verlief seine Weiterentwicklung. Die Innovationszyklen der Informationstechnologie nahmen dagegen immer mehr Fahrt auf – seit 1993 ist das Internet allgemein zugänglich, aber der Datenschutz blieb bei seinen alten Strukturen.

Eine zweite Welle des allgemeinen Interesses am Datenschutz wurde zum einen durch Skandale im Zusammenhang mit Beschäftigtendaten[3] in den Jahren 2007/2008 ausgelöst. Zum anderen klärten die Enthüllungen des ehemaligen US-amerikanischen Geheimdienstmitarbeiters Edward Snowdon im Jahr 2013 über das zwar von manchen befürchtete, aber von vielen nicht für möglich gehaltene Ausmaß der weltweiten Sammlung, Speicherung, Neuzusammenfügung und kommerziellen, aber auch staatlichen und geheimdienstlichen Nutzung von personenbezogenen Daten von Abermillionen Menschen auf. Das war möglich geworden, da sich auch die Speichertechnik und Auswertungsverfahren rasant weiterentwickelt haben. Gefahren für die Privatsphäre drohen heute aber nicht mehr

---

1 GVBl. I 1970, 625.
2 BVerfGE 65, 1.
3 *Körner*, AuR 2010, 416, 417.

nur vom datensammelnden kontrollafinen Staat, sondern vor allem von Unternehmen, die personenbezogene Daten als einen der lukrativsten Märkte des 21. Jahrhunderts entdeckt haben. Big Data ist hier nur ein Stichwort. Dabei geht es darum, durch die Auswertung einst für ganz andere Zusammenhänge gesammelter großer Datenmengen Trends zu erkennen, zukünftiges Verhalten zu berechnen oder Investitionsentscheidungen zu steuern.

Vor diesem Hintergrund hat die Europäische Union (EU) im Jahr 2012 einen Verordnungsentwurf zum Datenschutz vorgelegt, der eine janusköpfige Antwort auf die skizzierte Entwicklung liefern sollte: den Weg frei machen, um das wirtschaftliche Potential der Digitalisierung zu erschließen, ohne den Schutz der Betroffenen völlig über Bord zu werfen. Entsprechend hatte die 2012 zuständige Kommissarin Vivian Reding bei der Vorstellung des Kommissionsentwurfs der Datenschutz-Grundverordnung (DS-GVO) die wirtschaftlichen Chancen für den digitalen Binnenmarkt durch personenbezogene Daten hervorgehoben und betont, dass die europäische Bevölkerung in ihrer Funktion als Verbraucher und Verbraucherinnen ohne ausreichenden Datenschutz zu verhalten auf die digitalen Angebote reagiert.

Auch die Digitalisierung der Arbeitswelt ist so weit fortgeschritten, dass man in Anlehnung an die industrielle Revolution des 19. Jahrhunderts von einer digitalen Revolution sprechen kann, die die Arten von Arbeit, die Strukturen, in denen Arbeit erbracht wird, und nahezu alle bisherigen Beschäftigungsformen grundlegend verändern wird.[4] Diese Entwicklung hat rechtlich betrachtet mindestens zwei Seiten, zum einen die arbeitsrechtliche, bei der es um sozialen Schutz der (abhängig) beschäftigten Menschen geht, der sich bei fluiden, virtuellen Formen der Arbeitserbringung immer weniger mit den seit Jahrzehnten entwickelten und bewährten arbeitsrechtlichen Instrumenten gewährleisten lässt. Zum anderen geht es um die datenschutzrechtliche Seite dieser Entwicklung, die dazu führt bzw. in vielen Bereichen schon dazu geführt hat, dass ein privater, abgeschirmter, vor Blicken von außen geschützter Raum für Individuen kaum noch existiert. Ob und inwieweit die DS-GVO hier eine wirksame „Firewall" errichten kann, steht

---

4 Vgl. zur Digitalisierung der Arbeitswelt: Bundesministerium für Arbeit und Soziales (Hrsg.), Grünbuch – Arbeiten 4.0, Berlin 2015 sowie vor allem zu den Auswirkungen auf die Arbeitszeit das Gutachten von *Rüdiger Krause* zum 71. DJT 2016: Digitalisierung der Arbeitswelt – Herausforderungen und Regelungsbedarf, Verhandlungen des 71. Deutschen Juristentags, Band I: Gutachten/Teil B, Essen 2016; *Giesen/Junker/Rieble* (Hrsg.), Industrie 4.0 als Herausforderung des Arbeitsrechts, ZAAR Schriftenreihe, Band 39, München 2016; *Däubler*, Digitalisierung und Arbeitsrecht, SR Sonderheft, Juli 2016.

nicht im Mittelpunkt der folgenden Untersuchung, darf aber schon deshalb bezweifelt werden, weil das europäische Recht zum einen bereits keinen Zugriff auf das globale Phänomen Digitalisierung aller Lebensbereiche hat. Zum anderen greift die DS-GVO trotz gegenteiliger Beteuerung ihrer Macher im Wesentlichen auf die alten Instrumente zurück, die seit Jahren als unzureichend kritisiert werden, und nur punktuell vermeintlich Neues einführt, das aber bei näherer Betrachtung in internationalem Zusammenhang oft nur schwer oder gar nicht kontrollierbar sein wird, etwa ein Recht auf Vergessenwerden.

Der Beschäftigtendatenschutz führt die beiden Ebenen – Arbeitsrecht und Datenschutz – zusammen und weckt, da die DS-GVO Raum für nationale bereichsspezifische Regelungen gibt, Hoffnung für wirkungsvollere Regelungen als es die sehr allgemeine DS-GVO im Übrigen verspricht.

Lange war unbestritten, dass wirkungsvoller Datenschutz bereichsspezifischer Datenschutz sein muss,[5] weil nur Regelungen, die die konkreten Verarbeitungsformen berücksichtigen, deren besondere Gefahren eindämmen können. Das hat sich auch in § 1 Abs. 3 BDSG niedergeschlagen, wonach das BDSG hinter bereichsspezifischen Regelungen zurücktreten muss. Angesichts der Digitalisierung aller Lebensbereiche würde ein vorwiegend bereichsspezifischer Ansatz allerdings zu einem unübersehbaren Regelungsdickicht und damit in der Praxis zu weniger Schutz führen.[6] Insofern ist der generell-abstrakte Ansatz der DS-GVO vernünftig. Der Verordnungsgeber sieht aber selbst, dass es Lebensbereiche gibt, wo die generellen Regelungen nicht ausreichen und öffnet daher die Grundverordnung, trotz des obersten Zieles der Rechtsvereinheitlichung, für nationale „spezifischere" Regelungen. Das gilt vor allem für den Beschäftigtendatenschutz, da gerade im Beschäftigungsverhältnis die ohnehin schon weitgehende Überwachung noch verschärft wird durch die Kontrolle des Kommunikationsverhaltens von Beschäftigten (Internet, Mail), durch Ortungssysteme oder die Überwachungsmöglichkeit privater Aktivitäten des Beschäftigten während der Arbeitszeit bei der Nutzung von privaten Geräten für berufliche Zwecke (Bring your own device – BYOD). Vor allem die unter dem Label „Arbeit/Industrie 4.0"[7] stattfindende Entwicklung der zunehmenden Interaktion Mensch-Maschine macht

---

5 Vgl. etwa *Simitis*, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 2014, 8. Aufl., Einleitung Rn. 20.

6 Zum Problem der eventuellen Überregulierung durch bereichsspezifischen Datenschutz: *Kingreen/Kühling*, JZ 2015, 213.

7 Dieser Begriff ist nur im deutschsprachigen Raum gebräuchlich und beschreibt die Stufen der technisch-wirtschaftlichen Entwicklung von der Mechanisierung (Dampfmaschine) über die Massenfertigung (Elektrizität, Fließband) und Automatisierung (Elektronik, IT) bis zur Digitalisierung. In der englischsprachigen Welt heißt es „connected industry".

das Verhalten von Beschäftigten lückenlos nachvollziehbar. Industrie 4.0 zeichnet sich durch eine horizontale und vertikale Vernetzung von Datenströmen aus, die ganz neue Wertschöpfungsketten erlaubt. Auch künstliche Intelligenz spielt entlang ihrer stetigen technischen Weiterentwicklung auch zunehmend im Arbeitsleben eine Rolle. So sind etwa sprach- und sonstige IT-gestützte Analysen emotionaler Befindlichkeiten längst möglich. Mit Big Data schließlich lässt sich wahrscheinliches Verhalten voraussagen und daran früher oder später Rechtsfolgen knüpfen. Aber auch außerhalb des Beschäftigungsverhältnisses ist der Betroffene nicht mehr frei von Überwachung durch seinen Arbeitgeber, etwa wenn es um das Screening sozialer und beruflicher internetbasierter Netzwerke geht.

Neben einem Überblick über Genese, Grundprinzipien und Struktur des europäischen Datenschutzes in der DS-GVO geht es im Folgenden vor allem um die Auswirkungen der Datenschutz-Grundverordnung auf den Beschäftigtendatenschutz in Deutschland, besonders um den verbleibenden nationalen Regelungsspielraum und die Ausgestaltungsoptionen für Beschäftigtendatenschutzregelungen.

B. Genese der DS-GVO seit 2012

Am 4. 5. 2016 wurde die Europäische Datenschutz-Grundverordnung (DS-GVO) im Amtsblatt der EU veröffentlicht[8] und trat am 25. 5. 2016 in Kraft, nachdem der Rat am 8. 4. 2016 und das Europäische Parlament am 14. 4. 2016 die endgültige Fassung förmlich angenommen hatten. Nach einer zweijährigen Übergangszeit wird sie gemäß ihres Art. 99 Abs. 2 am 25. 5. 2018 für staatliche Stellen und Unternehmen anwendbar – wie schon die Datenschutzrichtlinie von 1995 gilt die DS-GVO gleichermaßen für den öffentlichen wie den privaten Bereich. Auch wenn die DS-GVO als EU-Verordnung gemäß Art. 288 AEUV unmittelbar anwendbar ist, gibt es erheblichen nationalen Anpassungsbedarf. Abgesehen davon, dass die DS-GVO mit ihren 99 Artikeln und 173 Erwägungsgründen viel umfangreicher ist als das BDSG und daher allein schon die Anpassung der Datenverarbeitungsprozesse an die neuen Regelungen eine Herausforderung darstellt, hat der europäische Gesetzgeber nun doch, trotz des ursprünglichen Hauptziels der Verordnung, den Datenschutz europaweit zu harmonisieren, zahlreiche Regelungsgegenstände dem nationalen Gesetzgeber zur Konkretisierung oder gar, wie beim Beschäftigtendatenschutz in Art. 88 DS-GVO, umfassend den Einzelstaaten zur Ausgestaltung überlassen.[9]

Dabei hat der vierjährige europäische Gesetzgebungsprozess mehrere Stadien durchlaufen, die nicht nur von historischem Interesse sind, sondern wichtig bei der Auslegung der schließlich verabschiedeten Version, die ebenso wie die erste von 2012 unzählige unbestimmte Rechtsbegriffe und Generalklauseln enthält. Die parallel zur DS-GVO erarbeitete Richtlinie für den Datenschutz bei der Polizei und in der Strafjustiz,[10] die den Rahmenbeschluss von 2008 für die Polizei und

---

8 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).

9 So auch *Kühling/Martini et al.*, Die Datenschutzgrundverordnung und das nationale Recht, 2016, S. 298.

10 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, L 119/89.

Strafjustiz aktualisiert, ist Teil der EU-Datenschutzreform, spielt aber für die folgenden Betrachtungen keine Rolle und wird daher nicht behandelt.

Bereits im Januar 2012 hatte die Europäische Kommission einen Reformvorschlag für das europäische Datenschutzrecht vorgelegt,[11] nachdem Datenschutzrecht auf europäischer Ebene umfassend erstmals 1995 in einer Richtlinie thematisiert worden war[12] und nach rund zwei Jahrzehnten rasanter Digitalisierung nahezu aller Lebenszusammenhänge eine europäische Datenschutzantwort auf die Entwicklung der Informationstechnologie überfällig war. Diese Fassung löste große Kontroversen mit ca. 4.000 Änderungsvorschlägen aus.[13] U. a. wurde kritisiert, dass sich die Kommission selbst in 26 Fällen im Wege so genannter delegierter Rechtsakte Konkretisierungsbefugnisse für in der Verordnung nur vage formulierte Regelungen eingeräumt hatte. Das Europäische Parlament legte im März 2014 eine modifizierte Fassung vor, in die zahlreiche der Änderungsvorschläge eingegangen sind.[14] U. a. wurde die Anzahl der Kommissionsermächtigungen zu delegierten Rechtsakten auf zehn reduziert. Der Rat machte seine Verhandlungsposition zur DS-GVO und damit die Sichtweise der Mitgliedstaaten am 11. 6. 2015 deutlich.[15] Damit reagierte er auf den Kommissionsentwurf von 2012, nicht aber auf die Fassung des Europäischen Parlaments. Delegierte Rechtsakte zugunsten der Kommission sind in der Ratsfassung nahezu vollständig verschwunden.

Schließlich einigten sich Kommission, Parlament und Rat im Dezember 2015 im informellen Trilog auf die Version, die dann im April 2016 im Wesentlichen unverändert verabschiedet wurde. Allerdings wurde in der endgültigen Version z. T. noch einmal die Nummerierung der Artikel geändert, was die Nachverfolgung der Argumentationslinien partiell erschweren kann. Im Folgenden wird bei der Nennung von Artikeln aus Vorversionen jeweils auf das Pendant in der verabschiedeten Version hingewiesen. Für den Beschäftigtendatenschutz ist dieser Umstand relevant, da die entsprechende Öffnungsklausel bis einschließlich zur Trilog-Version vom Dezember 2015 in Art. 82 DS-GVO-E zu finden war, in der im April 2016 verabschiedeten Verordnung nun in Art. 88 DS-GVO.

---

11 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) vom 25. 1. 2012: KOM (2012) 11 endg.

12 Richtlinie des Europäischen Parlaments und des Rates 95/46/EG vom 24. 10. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG Nr. L 281 S. 31 ff.

13 *Hornung*, ZD 2012, 104; *Schild/Tinnefeld*, DuD 2012, 312.

14 TA 2014/212/P7. Dazu *Roßnagel/Kroschwald*, ZD 2014, 495.

15 Rat der Europäischen Union, Dok. 9565/15. Dazu *Roßnagel/Nebel/Richter*, Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO, ZD 2015, 455.

C. Ziele und Hauptinhalte der DS-GVO

I. Bisheriger Datenschutz

1. Nationale Ebene

Das deutsche Datenschutzrecht ist stark ausdifferenziert und war nicht von vornherein verfassungsrechtlich verankert. Mehr als eine Dekade vor dem Volkszählungsurteil des BVerfG von 1983 basierte es auf den im Laufe der Zeit inhaltlich stark angenäherten Landesdatenschutzgesetzen und dem Bundesdatenschutzgesetz. Der in diesen Gesetzen geregelte allgemeine Datenschutz wurde im Laufe der Jahrzehnte durch eine große Zahl an bereichsspezifischen Regelungen im öffentlichen wie im privaten Bereich ergänzt, die gemäß § 1 Abs. 3 BDSG immer Vorrang vor den allgemeinen Bestimmungen haben. Zum bereichsspezifischen Datenschutz zählt etwa der Sozial- und Gesundheitsdatenschutz (insbesondere § 35 SGB I i. V. m. §§ 67 ff. SGB X) oder das Telemedien- sowie Telekommunikationsdatenschutzrecht (§§ 1 ff. TMG und §§ 91 ff. TKG), aber auch viele Einzelregelungen, wie etwa § 14 SigG, § 21g EnWG oder § 213 VVG.[16] Trotz des Vorrangs bereichsspezifischer Regelungen gibt es allerdings immer wieder Abgrenzungsprobleme.[17]

Erst 1983 erfolgte die verfassungsrechtliche Verankerung durch das im Volkszählungsurteil aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitete Recht auf informationelle Selbstbestimmung als Abwehrrecht des Einzelnen gegen staatliche Eingriffe,[18] dem 2008 das kurz als IT-Grundrecht bezeichnete Recht auf die Vertraulichkeit informationstechnischer Systeme[19] zur Seite gestellt wurde. Seit gut 30 Jahren also ist Datenschutz in Deutschland auch ein verfassungsrechtliches Thema mit allen materiell-rechtlichen wie prozessrechtlichen Implikationen – eine individuelle Verfassungsbeschwerde zum BVerfG gemäß § 90 BVerfGG ist im Prinzip möglich.

---

16 Weitere Beispiele bei *Gola/Schomerus*, BDSG-Kommentar, 2015, 12. Aufl., Einleitung Rn. 8.

17 Vgl. etwa für den Telemedienbereich *Keppeler*, MMR 2015, 779 f.

18 BVerfGE 65, 1 ff.; dazu *Grimm*, JZ 2013, 585 f.

19 BVerfGE 120, 274 ff.

2. Europäische Ebene

Vor diesem Hintergrund wurde der europäische Datenschutz nicht selten eher als Schutz minderer Qualität angesehen. Ohnehin trat der EU-Gesetzgeber mit der Datenschutzrichtlinie von 1995[20] spät auf den Plan[21] und hatte zudem nur bedingt neue Ideen zu bieten. Im Großen und Ganzen basierte die Richtlinie auf dem deutschen Datenschutzrecht, enthielt aber auch den einen oder anderen Einzelpunkt, der zuvor national nicht realisierbar war und dann im Zuge der Umsetzung der Richtlinie ins BDSG aufgenommen wurde. Die Beteiligung des EuGH an der Fortentwicklung des Datenschutzes blieb marginal. Ein Übriges tat der Umstand, dass die meisten EU-Mitgliedstaaten die Datenschutzrichtlinie nicht angemessen umgesetzt hatten – im Jahr 2016 der Hauptgrund für eine Verordnung als Regelungsinstrument für den europäischen Datenschutz.

Erst seit der Charta der Grundrechte der EU (GR-Charta) aus dem Jahr 2000[22] zeichnet sich auch auf EU-Ebene eine Konstitutionalisierung des Datenschutzes ab. Zwar war die Grundrechte-Charta zunächst nur eine politische Erklärung und damit nicht rechtsverbindlich, was sich aber mit dem Vertrag von Lissabon durch Art. 6 Abs. 1 EUV seit dem 1. 12. 2009 änderte. Seitdem ist die Charta der Grundrechte und damit auch ihr Art. 8, der ein Grundrecht auf den Schutz personenbezogener Daten gewährleistet, rechtlich für den gesamten Geltungsbereich des Unionsrechts bindend. Jüngst hat der EuGH in drei wichtigen Entscheidungen deutlich gemacht, wie er das europäische Grundrecht auf Datenschutz zu konturieren gedenkt.[23] Aus prozessualer Sicht ist allerdings schon hier darauf hinzuweisen, dass je nachdem, ob man sich im harmonisierten – EU-Grundrechte – oder nicht harmonisierten Bereich – nationale Grundrechte – befindet, nur im letzteren Bereich noch die individuelle Verfassungsbeschwerde als Rechtsbehelf zur Verfügung steht, was auf Unionsebene nicht der Fall ist.[24]

---

20 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. 10. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Abl. Nr. L 281 S. 31.

21 *Simitis*, Die EG-Datenschutzrichtlinie: eine überfällige Reformaufgabe, in: Herzog/Neumann (Hrsg.), Festschrift für Winfried Hassemer, 2010, S. 1235.

22 Charta der Grundrechte der Union, ABl. 2000 Nr. C 364/01.

23 Dazu näher unten C.VII.2.b). Zum europäischen Datenschutzgrundrecht in Art. 8 GR-Charta vgl. auch *Heuschmid/Lörcher*, NK-GA, Art. 8 GR-Charta.

24 *Heuschmid*/Lörcher, NK-GA, Art. 51 Rn. 9 ff.

3. EU-Grundrechte und nationale Grundrechte: ein ungeklärtes Verhältnis

Das Verhältnis zwischen Unionsrecht, insbesondere EU-Grundrechten und nationalem Verfassungsrecht ist komplex und gehört zu den umstrittensten Bereichen des Verfassungs- und Europarechts,[25] was damit zusammenhängt, dass die Frage weder im nationalen noch im EU-Recht geregelt ist und es daher allein auf die Rechtsprechung des EuGH und des BVerfG ankommt. Die war seit der Entscheidung des EuGH bereits aus dem Jahr 1964, wonach Unionsrecht wegen seiner besonderen Rechtsnatur Anwendungsvorrang vor nationalem Recht hat[26] und der rasch darauf getroffenen EuGH-Entscheidung, dass das auch für das Verfassungsrecht der Mitgliedstaaten gilt,[27] lebhaft. Das BVerfG erkennt den Anwendungsvorrang zwar prinzipiell an,[28] allerdings nur – und das betont das Gericht auch noch 2009 in seiner Entscheidung zum Lissabon-Vertrag – aufgrund des deutschen Zustimmungsgesetzes. Das heißt, dass das BVerfG den Vorrang des Unionsrechts nicht für absolut hält, sondern „nur kraft und im Rahmen der verfassungsrechtlichen Ermächtigung".[29]

Für das Verhältnis zwischen deutschen Grundrechten und dem sekundären Unionsrecht gibt es seit der Solange II-Entscheidung aus dem Jahr 1986 nichts grundlegend Neues.[30] Hatte das BVerfG im Jahr 1974 noch entschieden, dass die Übertragung von Hoheitsrechten auf die EU unzulässig sei, wenn dadurch, z. B. durch den Erlass von Verordnungen, die Grundrechte des GG beeinträchtigt werden können (Solange I),[31] so ist das BVerfG eine Dekade später zu einer anderen Bewertung gekommen. Mittlerweile hielt es die Einhaltung der Grundrechte durch die Rechtsprechung des EuGH dadurch für gewährleistet, dass der EuGH grundrechtsgleiche allgemeine Rechtsgrundsätze aus den Verfassungstraditionen der Mitgliedstaaten abgeleitet hatte, mit der Folge, dass das BVerfG seitdem die Vereinbarkeit von EU-Recht mit dem GG nicht mehr prüft (Solange II). Eine Hintertür hatte sich das Gericht offen gelassen: Sollte der vom GG gewährte Grundrechtsschutz – im vorliegenden Zusammenhang das Recht auf informationelle Selbstbestimmung – auf EU-Ebene „generell" nicht mehr gewährleistet werden, käme wieder das GG für die Prüfung von EU-Sekundärrecht zum Zuge.[32] Neben

---

25 *Polzin*, JuS 2012, 1, Fn. 3 m. w. N.; dazu auch schon *Körner*, ZESAR 2013, 153, 155 ff.
26 EuGH, Urt. v. 15. 7. 1964 – C-6/64, Slg. 1964, 1251, 1269 f. (Costa/E.N.E.L.).
27 EuGH, Urt. v. 17. 12. 1970 – C-11/70, Slg. 1970, 1125 (Internationale Handelsgesellschaft).
28 BVerfGE 31, 145, 174.
29 BVerfGE 123, 267, 354; BVerfG, Urt. v. 21. 6. 2016 – 2 BvR 2728/13.
30 *Masing*, JZ 2015, 477, 480.
31 BVerfGE 37, 271, 279 f.
32 BVerfGE 73, 339, 377; BVerfGE 102, 147, 164.

diesem grundrechtlichen Kontrollanspruch hat sich das BVerfG im Maastricht-Urteil für das Handeln von Unionsorganen eine Ultra-vires-Kontrolle vorbehalten,[33] wonach im Einzelfall geprüft werden kann, ob Kompetenzgrenzen für den Erlass von EU-Rechtsakten offensichtlich verletzt wurden. Diese Linie wurde im Lissabon-Urteil bestätigt und durch den weiteren Vorbehalt einer Identitätskontrolle ergänzt.[34] Es geht dabei um die Identität des GG, die in Art. 79 Abs. 3 GG garantiert ist und nicht aufgegeben werden darf, sowie um bestimmte, sich aus Art. 20 Abs. 1 und 2 sowie Art. 38 Abs. 1 Satz 1 GG ergebende Bereiche, die zur Gewährleistung „demokratischer Selbstgestaltungsfähigkeit"[35] nicht auf die EU übertragen werden dürfen.[36]

Seitdem ist die europäische GR-Charta in Kraft getreten, die in Art. 8 sogar ein eigenes Datenschutzgrundrecht enthält, so dass von einer „generell" nicht gewährleisteten Grundrechtssicherung auf EU-Ebene keine Rede sein kann. Es gilt gemäß Art. 51 Abs. 1 GR-Charta eine Art Arbeitsteilung: für vereinheitlichtes Unionsrecht, wie in der DS-GVO der harmonisierte Teil, gilt der EU-Grundrechtsschutz,[37] für das einzelstaatliche Recht gelten die Grundrechte der jeweiligen Verfassung.[38] Hieraus ergebe sich allerdings, so der ehemalige Bundesverfassungsrichter *Masing*, ein „Grundrechtsüberdruck".[39] Beim Datenschutz ist dieser durch die Konkurrenz zwischen dem ausdrücklichen Datenschutzgrundrecht in Art. 8 GR-Charta und der aus Art. 2 Abs. 1 GG abgeleiteten informationellen Selbstbestimmung besonders sichtbar und fällt eher zugunsten der EU-Grundrechte aus,[40] zumal der EuGH sich von der Abgrenzung der Grundrechtssphären in Art. 51 Abs. 1 GR-Charta kaum beeindrucken lässt und darauf abstellt, ob die vom Mitgliedstaat angewandte Rechtsnorm „in den Anwendungs- oder Geltungsbereich" des Unionsrechts fällt.[41] Das war in der Rechtssache Akerberg/Fransson der Fall, wo es um Mehrwertsteuerbetrug ging und der EuGH daher die Grundrechtecharta für anwendbar hielt, [42] obwohl selbst der Generalanwalt in dieser Sache den EuGH nicht für zuständig gehalten hatte.

---

33 BVerfGE 89, 155, 188.
34 BVerfGE 123, 267, 340 ff.
35 BVerfGE 123, 267, 358 ff.
36 Vgl. dazu auch *Dederer*, JZ 2014, 313, der die These vertritt, dass sich die drei Prüfungsmaßstäbe des BVerfG harmonisieren lassen.
37 *Heuschmid/Lörcher*, NK-GA, Art. 51 Rn. 9 ff.
38 *Masing*, JZ 2015, 477, 480.
39 A. a. O., S. 481.
40 *Grimm*, JZ 2013, 585, 590 f.
41 A. a. O.
42 EuGH, Urt. v. 26. 2. 2013 – C-617/10, NJW 2013, 1415 (Akerberg/Fransson).

Das BVerfG wiederum hat in seiner Entscheidung zur Antiterrordatei vom 24. 4. 2013[43] angemerkt, dass der EuGH keine allgemeinen Aussagen treffen wollte, sondern es nur um seine Zuständigkeit für Grundrechtsfragen im Zusammenhang mit dem europäisch geregelten Umsatzsteuerrecht ging. Allerdings geht dann das BVerfG im Urteil ungewöhnlich ausführlich darauf ein, dass es keinen Anlass für ein Vorabentscheidungsverfahren vor dem EuGH gebe, da das Antiterrordateigesetz keine Durchführung europäischen Rechts i. S. v. Art. 51 Abs. 1 Satz 1 GR-Charta sei. Das ist zwar in der Sache richtig. Das Vorgehen deutet aber auf Abgrenzung hin. Für den Datenschutz gemäß der DS-GVO kann es in Zukunft zu einer Doppelzuständigkeit kommen: der EuGH ist zuständig, soweit es um „Durchführung des Rechts der Union" geht, also im harmonisierten Bereich. In den Bereichen, wo, wie im Beschäftigtendatenschutz, die DS-GVO eine Öffnung für nationale Regelungen enthält, sieht es anders aus. Sofern der nationale Gesetzgeber von den Regelungsoptionen Gebrauch macht, handelt es sich gerade nicht um harmonisiertes Recht und es bleibt bei der Zuständigkeit des BVerfG.[44] Allerdings muss der EuGH überprüfen können, ob sich die nationale Regelung, die nur aufgrund der Verordnung überhaupt zulässig ist, im Bereich der Verordnung hält.[45]

II. Herausforderungen an die Neuregelungen

Die im Wesentlichen drei Herausforderungen an die Neuregelung sind schwer zu erfüllen. Naturgemäß ist bei der Bewertung, inwieweit den eigenen Ansprüchen Genüge getan wurde, der politische Blick auf die Einigung in der Grundverordnung milder[46] als der nüchterne Blick der Fachöffentlichkeit.

Hauptanspruch der DS-GVO ist es, in allen 28 Mitgliedstaaten einen einheitlichen Datenschutzstandard zu schaffen, nicht zuletzt um die digitale Wirtschaft in der EU zu beflügeln. Entsprechend stellt Art. 1 DS-GVO Datenschutz und Datenfreiheit als ein einheitliches Ziel dar. Nach Art. 1 Abs. 1 enthält die Verordnung Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, aber auch für den Schutz des freien Datenverkehrs in der Union.

---

43 BVerfG, Urt. v. 24. 4. 2013 – 1 BvR 1215/07, NJW 2013, 1499, Rn. 91.

44 Vgl. auch NK-GA, Art. 23 ff.; *Kingreen*, JZ 2013, 801; BVerfG, Urt. v. 15. 12. 2015 – 2 BvR 2735/14, NJW 2016, 1149.

45 Hierbei wird es vor allem um die Auslegung von Art. 88 Abs. 2 DS-GVO gehen. Dazu unten E.II.2.

46 *Maas*, DuD 2015, 579; *Albrecht*, CR 2016, 88; *ders.*, ZD 2013, 587.

Darüber hinaus soll ein moderner Datenschutz geschaffen werden, wobei weitgehend unklar bleibt, was mit „modern" genau gemeint ist. Schließlich soll der Datenschutz in Zukunft technikneutral ausgestaltet sein, um mit den rasant weiterentwickelten Informations- und Kommunikationstechnologien Schritt halten zu können.

Die DS-GVO soll wegen der Verordnungswirkung in Art. 288 Abs. 2 Satz 2 AEUV zu einer deutlichen Vereinheitlichung des Datenschutzniveaus in den 28 Mitgliedstaaten führen. Anders als bei der Datenschutzrichtlinie vom 24. 10. 1995, die auch die geregelte Rechtsmaterie harmonisieren will, gibt es bei einer Verordnung kein Umsetzungserfordernis und damit auch keinen entsprechenden Spielraum. Bei der europäischen Datenschutzrichtlinie hatte der dazu geführt, dass die nationalen Vorgaben zum Datenschutzrecht sehr unterschiedlich blieben,[47] so dass sich nicht nur Unternehmen wie Google oder Facebook einen datenschutzgenehmen Standort innerhalb der EU aussuchen konnten.

Schließlich trägt zu einer vereinheitlichenden Wirkung auch der weite Anwendungsbereich der DS-GVO bei. Die nach Art. 3 Abs. 1 DS-GVO für die Datenverarbeitung von Unternehmen gültige Verordnung wendet, anders als die DS-Richtlinie mit dem Territorialitätsprinzip, das Sitz- sowie das Marktortprinzip an. Hiernach werden einerseits Unternehmen erfasst, die eine Niederlassung in der EU haben, unabhängig davon, ob die Datenverarbeitung innerhalb oder außerhalb der EU stattfindet. Andererseits muss das EU-Datenschutzrecht gemäß Art. 3 Abs. 2 DS-GVO aber auch von Unternehmen beachtet werden, die – auch ohne Niederlassung in einem Mitgliedstaat – in der EU entgeltlich oder unentgeltlich Waren oder Dienstleistungen anbieten und dazu Daten von Personen innerhalb der EU verarbeiten. Damit werden auch Unternehmen aus dem EU-Ausland von der DS-GVO erfasst, was vor allem für US-amerikanische Unternehmen, die innerhalb der EU aktiv sind, eine Änderung bedeuten wird, da deren Datenerhebung und -verarbeitung ab Mai 2018 an europäischem Datenschutzrecht gemessen wird. Ganz fremd war das Marktortprinzip aber auch unter der Geltung der Datenschutzrichtlinie nicht, da der EuGH in jüngerer Zeit diesem Prinzip in seiner Rechtsprechung z. T. bereits Geltung verschafft hatte.[48]

III. Prinzipien und Instrumente der DS-GVO

Die DS-GVO hat gemäß Art. 1 Abs. 1 nicht nur den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, also deren informationelle

---

47 Vgl. EuGH, Urt. v. 24. 11. 2011 – C-468/10, C-469/10, RDV 2012, 22 (ASNEF).

48 So etwa in der Google Spain-Entscheidung, dazu *Kühling*, EuZW 2014, 527.

Selbstbestimmung zum Ziel, sondern gleichgewichtig auch das Gegenteil, nämlich gerade den freien Verkehr solcher Daten. Der darf sogar nach Art. 1 Abs. 3 nicht allein mit der Begründung eingeschränkt werden, es gehe um den Schutz natürlicher Personen bei der Verarbeitung von deren personenbezogenen Daten. Der freie Datenverkehr erhält damit einen ebenso hohen Stellenwert wie der Persönlichkeitsschutz. Für die zukünftige Auslegung der DS-GVO dürfte das bedeuten, dass immer eine Interessenabwägung zwischen diesen beiden Polen stattzufinden hat. Die bisherige grundrechtliche Perspektive des deutschen Datenschutzrechts kollidiert mit dem europarechtlichen Spannungsverhältnis zwischen Grundrechten und Grundfreiheiten. Die „historisch bedingte Schieflage“[49] zugunsten der Förderung des Binnenmarktes und also zugunsten der Grundfreiheiten hat erst durch die verbindliche Verankerung der GR-Charta als Primärrecht in Art. 6 Abs. 1 EUV und die Aufnahme von sozialer Marktwirtschaft und sozialem Fortschritt als Ziele der Union in Art. 3 Abs. 3 Satz 2 EUV etwas mehr Balance erhalten. Ob dadurch EuGH-Bewertungen wie in den Fällen *Viking*[50] und *Laval*,[51] in denen das Grundrecht auf Koalitionsfreiheit zugunsten der Grundfreiheiten des freien Dienstleistungsverkehrs bzw. der Niederlassungsfreiheit zurückstehen musste, beim Datenschutz in Zukunft grundrechtsorientierter ausfallen werden, bleibt abzuwarten. Erste Entscheidungen des EuGH aus jüngerer Zeit deuten in die richtige Richtung.[52]

Im Übrigen führt die DS-GVO nicht grundsätzlich zu einer völligen Umwertung des Datenschutzes, denn sie gründet nicht nur auf ihrer 20 Jahre alten Vorgängerin, der EU-Datenschutzrichtlinie, sondern nimmt auch Strukturen aus den nationalen Datenschutzbestimmungen der Mitgliedstaaten auf, nicht zuletzt auch den deutschen. Daher werden die Auswirkungen der DS-GVO für Unternehmen in Deutschland auch für „überschaubar“ gehalten.[53] So geht auch die DS-GVO von einem weiten Datenverarbeitungsbegriff aus (Art. 2 Abs. 1), der sowohl die automatisierte wie die nicht automatisierte Verarbeitung personenbezogener Daten umfasst – analoge Daten sind allerdings nicht gemeint –, wobei auch in der DS-GVO der Streit über den absoluten (objektive, technische Bestimmbarkeit des

---

49 *Pötters*, Grundrechte und Beschäftigtendatenschutz, 2013, S. 259.

50 EuGH, Urt. v. 11. 12. 2007 – C-438/05, Slg. 2007, I-10779 (Viking).

51 EuGH, Urt. v. 18. 12. 2007 – C-341/05, Slg. 2007, I-11767 (Laval).

52 EuGH, Urt. v. 8. 4. 2014 – C-293/12, C-594/12, DuD 2014, 488 (Vorratsdatenspeicherung); EuGH, Urt. v. 13. 5. 2014 – C-131/12, DuD 2014, 559 (Google); EuGH, Urt. v. 6. 10. 2015 – C-362/14, DuD 2015, 823 (Safe Harbor). Vgl. dazu auch noch unten C.VII.2.b).

53 U. a. *Kraska*, ZD-Aktuell 2016, 04173.

Personenbezuges) oder relativen Personenbezug (subjektive Möglichkeit des Datenverarbeiters, den Personenbezug herzustellen) nicht geklärt wird.[54]

Begrifflich wird im Verordnungstext nicht zwischen Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten unterschieden, wie in § 1 Abs. 2 BDSG, sondern es ist einheitlich von „Verarbeitung" solcher Daten die Rede (Art. 1 Abs. 1 DS-GVO). Dieser Verarbeitungsbegriff ist aber weit gemeint, wie die Definitionsnorm Art. 4 Nr. 2 DS-GVO deutlich macht. Danach umfasst der Begriff „Verarbeitung" nicht nur das bisherige Erheben, Verarbeiten und Nutzen von personenbezogenen Daten, sondern „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang", wozu u. a. auch Organisation, Ordnen, Anpassung oder Veränderung, Auslesen, Abfragen, Abgleich und Verknüpfung personenbezogener Daten gehören.

Darüber hinaus findet sich der wesentliche Grundsatz des Datenschutzes in § 4 Abs. 1 BDSG, das Verbot mit Erlaubnisvorbehalt, auch in der Verordnung (Art. 6 Abs. 1), wonach die Verarbeitung personenbezogener Daten im Prinzip verboten ist und erst durch einen Erlaubnistatbestand, vor allem eine gesetzliche Regelung, eine Einwilligung[55] oder eine der weiteren in Art. 6 genannten Verarbeitungszusammenhänge gerechtfertigt werden muss. Dazu gehört die Verarbeitung zur Erfüllung eines Vertrages der betroffenen Person (Art. 6 Abs. 1 lit. a) oder zum Schutz lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person (Art. 6 Abs. 1 lit. d). Bei der Verarbeitung zur Erfüllung rechtlicher Verpflichtungen des Verantwortlichen (Art. 6 Abs. 1 lit. c) oder für die Wahrnehmung einer Aufgabe im öffentlichen Interesse (Art. 6 Abs. 1 lit. e) eröffnet Art. 6 Abs. 2 DS-GVO den Mitgliedstaaten die Möglichkeit, „spezifischere Bestimmungen" zu erlassen. In der Liste der Verarbeitungsgründe ist Art. 6 Abs. 1 lit. f der problematischste, denn er erlaubt die Verarbeitung im berechtigten Interesse des Verantwortlichen.[56] Darüber hinaus können auch berechtigte Interessen Dritter Datenerhebung und -verarbeitung rechtfertigen, eine Vorschrift, die im Laufe des Gesetzgebungsverfahrens sehr umstritten war, sich aber im Trilog schließlich durchsetzen konnte.[57] Zwar muss im Vergleich zur Datenschutzrichtlinie von 1995 zumindest eine Abwägung mit den „Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person" erfolgen. Kriterien für diese Abwägung enthält die DS-GVO aber nicht. Art. 6 Abs. 1 lit. f DS-GVO

---

54 *Kort*, DB 2016, 711.

55 Dazu näher für den Beschäftigungskontext unten E.III.4.

56 Kritisch *Roßnagel/Nebel/Richter*, ZD 2015, 455, 457.

57 Zur Kritik *Roßnagel/Kroschwald*, ZD 2014, 45, 499; gefordert worden war die Berücksichtigung von Drittinteressen u. a. von *Gola/Schulz*, RDV 2013, 1, 6, 7.

wird wohl der Maßstab für neue Geschäftsmodelle im Internet werden. Sollte Beschäftigtendatenschutz nicht national geregelt werden, wäre es sehr problematisch, dass das berechtigte Interesse eines jeden Dritten an den personenbezogenen Daten eines Beschäftigten als Rechtfertigung für die Datennutzung reicht, auch wenn in diesen Fällen zumindest eine Interessenabwägung notwendig wäre.

Auch am Zweckbindungsgrundsatz, dem Leitprinzip des Datenschutzes, das aber im BDSG nicht klar kodifiziert ist,[58] hält die DS-GVO in Art. 5 Abs. 1 lit. b fest, wonach personenbezogene Daten nur für die zuvor festgelegten legitimen Zwecke erhoben und weiterverarbeitet werden dürfen. In Art. 6 Abs. 2 erlaubt die DS-GVO für bestimmte Datenverarbeitungserlaubnisse nationale Verschärfungen. Allerdings sind nach Art. 6 Abs. 4 DS-GVO unter bestimmten Voraussetzungen spätere Zweckänderungen erlaubt. Hierunter dürften – im Prinzip – Big Data-Anwendungen fallen, bei denen große Datenmengen zunächst zweckfrei gesammelt werden, um durch spätere Auswertungen neue Kenntnisse zu generieren.[59] Auch der aus § 3a Satz 2 BDSG bekannte Grundsatz der Datenvermeidung und Datensparsamkeit, der gemäß BDSG durch Anonymisierung und Pseudonymisierung gewährleistet werden soll, taucht in Art. 5 Abs. 1 lit. c DS-GVO wieder auf, wenn auch vager: die Datenerhebung soll auf das notwendige Maß beschränkt werden.

Eine Sonderstellung nehmen die sensiblen Daten gemäß Art. 9 DS-GVO ein. Schon in § 3 Abs. 9 BDSG sind weitgehend dem Allgemeinen Gleichbehandlungsgesetz (AGG) entsprechende Merkmale definiert, deren Erhebung und Verarbeitung nach § 28 Abs. 6–9 BDSG strengeren Verarbeitungsvoraussetzungen unterliegen als sonstige personenbezogene Daten; Regelungen, die in Deutschland bislang auch für den Beschäftigtendatenschutz gelten. Diesen Ansatz greift Art. 9 DS-GVO auf und regelt im Großen und Ganzen sogar strenger als das deutsche Recht. So dürfen die in Art. 9 Abs. 1 aufgezählten sensiblen Daten nach Abs. 3 nur von Fachpersonal verarbeitet werden, das einer Geheimhaltungspflicht unterliegt. Diese Einschränkung gilt nach § 28 Abs. 7 BDSG nur für Gesundheitsdaten.[60]

Daneben enthält die DS-GVO weitere Instrumente, wie umfangreichere Informationspflichten als im BDSG in Art. 13 f. oder hohe Transparenzanforderungen in

---

58 *Kühling/Seidel/Sivridis*, Datenschutzrecht, 2015, 3. Aufl., Rn. 286.

59 Kritisch zur Ausgestaltung des Zweckbindungsgrundsatzes in der DS-GVO schon zum Ratsentwurf: *Richter*, DuD 2015, 735, 740.

60 Näher zu Art. 9 DS-GVO im Beschäftigungszusammenhang noch unten E.II.2.d) und mit Bezug zur Einwilligung unter E.III.4.d)bb).

Art. 12. Allerdings muss bedacht werden, dass es angesichts der unübersehbaren Menge an Daten, die bei der IT-Nutzung im nicht-öffentlichen Bereich laufend entsteht, zwar rechtlich möglich ist, Transparenzanforderungen festzulegen, faktisch aber unmöglich sein wird, eine umfassende Transparenz zu schaffen (und zu kontrollieren). In Bezug auf bestimmte Daten oder/und gegenüber bestimmten Akteuren, wie etwa im Beschäftigtendatenschutz, mag sich das jedoch eher realisieren lassen.[61]

Von eher anekdotischem Wert ist der Werdegang des „Rechts auf Vergessenwerden" in Art. 17 DS-GVO. Das im Kommissionsentwurf mit großem Marketingaufwand beworbene Recht auf Vergessenwerden[62] war von vornherein nur ein Löschungsrecht, wie es schon existiert. Das Europäische Parlament hatte Art. 17 daher konsequenterweise mit „Recht auf Löschung" überschrieben, der Rat griff auf die ursprüngliche Version (in Anführungsstrichen) zurück und in der verabschiedeten Fassung heißt es nun „Recht auf Löschung („Recht auf Vergessenwerden")". Selbst ein solches (bescheidenes) Löschungsrecht wird im privaten Bereich kaum umfassend, sondern allenfalls bereichsspezifisch wirkungsvoll umsetzbar sein. Was es konkret bedeutet, hat der EuGH bereits in der Google-Spain-Entscheidung festgelegt:[63] Auf eine für den Betroffenen negative Information, die für die Öffentlichkeit nicht (mehr) von Interesse ist, darf eine Suchmaschine nicht mehr hinweisen. Das heißt aber nicht, dass die Information nicht mehr auffindbar ist. Im entschiedenen Fall blieb die ungünstige Information im fraglichen Register enthalten.

Die DS-GVO formuliert als eines von zwei Hauptzielen neben der Modernisierung des Datenschutzes die Vereinheitlichung der Regeln in allen Mitgliedstaaten. Dem dienen die o. a. für alle 28 Mitgliedstaaten einheitlichen gesetzlichen Erlaubnistatbestände für Datenerhebung und -verarbeitung. Zusätzlich können natürlich auch andere EU-Normen Erlaubnistatbestände i. S. des Grundsatzes Verbot mit Erlaubnisvorbehalt sein. Ob, wie und wann es möglich sein wird, aus derartigen Generalklauseln den mit der Verordnung anvisierten einheitlichen europäischen Datenschutz zu schaffen, bleibt abzuwarten. Das Ziel dürfte allerdings schon allein aufgrund der zahlreichen Öffnungsklauseln nicht erreichbar sein.

---

61 *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 121 ff., 133 ff.

62 Kritisch schon zum Kommissionsvorschlag *Körner,* ZESAR 2013, 99 ff. und 153 ff.; richtig hat *Grimm* angemerkt, dass ein solches Recht jenseits rechtlicher Gewährleistungsmöglichkeiten liegt, a. a. O., S. 589.

63 EuGH, Urt. v. 13. 5. 2014 – C-131/12, NJW 2014, 2257.

Wegen der entsprechenden Schwierigkeiten und der mit unbestimmten Rechtsbegriffen einhergehenden Rechtsunsicherheit war bislang anerkannt, dass effizienter Datenschutz am besten mit bereichsspezifischen Regelungen zu erzielen ist,[64] da generalklauselartige Regeln zwar eine Vielzahl von Fällen erfassen können, jedoch den spezifischen Datenverarbeitungsbedingungen in sehr unterschiedlichen Zusammenhängen nicht gerecht werden. Entsprechend haben im deutschen Datenschutzrecht gemäß § 1 Abs. 3 BDSG spezialgesetzliche Rechtsvorschriften zum Datenschutz Vorrang vor dem BDSG. Dieses allgemeine Subsidiaritätsprinzip ist in der DS-GVO nicht mehr vorhanden, was z. T. in der Literatur für einen Paradigmenwechsel gehalten wird,[65] der die Frage aufwirft, was aus dem bisherigen bereichsspezifischen deutschen Datenschutzrecht, etwa dem GenDG oder den Datenschutznormen des SGB wird. Vor diesem Hintergrund sind die ca. zehn Regelungsaufträge an den nationalen Gesetzgeber (insbesondere zur Aufsicht) und ca. 30 Regelungsoptionen,[66] darunter zum Beschäftigtendatenschutz, zu begrüßen. Über diesen Weg sind doch noch bereichsspezifische Regelungen möglich, etwa auch aus den Sachzusammenhängen, die bislang in Deutschland in bereichsspezifischen Datenschutzgesetzen geregelt waren und Beschäftigtendaten betreffen.

Diese Öffnung für nationale Regelungen, insbesondere in brisanten Bereichen, war zunächst nicht geplant. Die Fortentwicklung des Datenschutzes sollte bei der Kommission zentralisiert werden, die in so genannten delegierten Rechtsakten jeweils Regelungen zu speziellen Verarbeitungszusammenhängen hätte erlassen dürfen, auch im Beschäftigtendatenschutz. Dabei hätte es sich dann nach Art. 290 AEUV um verbindliche exekutive Rechtsetzung gehandelt.[67] Dieser Plan wurde fallengelassen. Nur noch in zwei Fällen darf die Kommission delegierte Rechtsakte erlassen: gemäß Art. 40 Abs. 9 und Art. 12 Abs. 8 DS-GVO.

Das erlaubt den Mitgliedstaaten in einem unerwartet weiten Umfang doch noch ihre nationalen Vorstellungen von Datenschutz umzusetzen. Der Preis ist allerdings, dass es keinen einheitlichen Datenschutz in allen Mitgliedstaaten geben wird. Ähnliches kennt man schon von der Europäischen Aktiengesellschaft (SE),

---

64 *Simitis*, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 2014, 8. Aufl., Einleitung Rn. 20, 32.

65 *Brink*, in: Boecken/Düwell/Diller/H. Hanau (Hrsg.), Nomos-Kommentar Gesamtes Arbeitsrecht, 2016, 1. Aufl., § 32 BDSG Rn. 22.

66 Einige davon genannt bei *Buchner*, DuD 2016, 155, 160, und bei *Kraska*, ZD-Aktuell 2016, 04173.

67 So genanntes „tertiäres Unionsrecht", *Kühling*/*Seidel*/*Sivridis*, Datenschutzrecht, 2015, 3. Aufl., Rn. 141.

wo es keine EU-einheitliche europäische Aktiengesellschaft gibt, sondern 28 verschiedene Gesellschaften, da an zahlreichen Stellen auf das nationale Recht zurückgegriffen wird.[68] Faktisch nimmt die DS-GVO damit eine Zwitterstellung zwischen Verordnung und Richtlinie ein, was zu weniger statt mehr Rechtsangleichung beim Datenschutz führt. Je nachdem, in welchem Umfang die Mitgliedstaaten von den Regelungsbefugnissen Gebrauch machen, wird die Unübersichtlichkeit der Datenschutzregelungen in den 28 Staaten zwar z. T. abgebaut, aber nicht beseitigt werden, was sich auch auf den Grundrechtsschutz auswirkt.[69]

IV. Betroffenenrechte

Die Betroffenenrechte in Art. 13 ff. DS-GVO entsprechen im Wesentlichen dem bekannten System,[70] sind sogar z. T. weitgehender als die in §§ 33–35 BDSG geregelten. Sie umfassen Informationsrechte (Art. 13 f.), Löschungsrechte (Art. 17), die Datenübertragbarkeit (Art. 20) und Widerspruchsrechte (Art. 21). Da die DS-GVO vor allem die Transparenz der Datenverarbeitung erhöhen will, sind die Informationsrechte des Betroffenen in Art. 13 und 14 deutlich weiter gefasst als im BDSG. Neben Pflichtinformationen, wie zur verantwortlichen Datenverarbeitungsstelle, über die Zwecke der Verarbeitung, die berechtigten Interessen eines Dritten i. S. v. Art. 6 Abs. 1 lit. f und die Absicht des Verantwortlichen, Daten in ein Drittland zu übermitteln, gibt es fakultative Informationspflichten, die erfüllt werden müssen, wenn sie für eine transparente Datenverarbeitung erforderlich sind. Hierzu zählen u. a. die Kriterien für die Festlegung der Dauer der Datenspeicherung oder die Quellen der Daten. Im Bereich der Informationsrechte des Betroffenen hat die Kommission eine ihrer im Vergleich zum DS-GVO-Entwurf von 2012 zahlenmäßig stark reduzierten Befugnisse für den Erlass delegierter Rechtsakte behalten. Gemäß Art. 12 Abs. 8 DS-GVO darf sie entsprechend vorschreiben, die Information im Wege standardisierter Bildsymbole zu erteilen.

Die Löschungsrechte dagegen gehen nicht viel weiter als schon nach dem BDSG, zumal das „Recht auf Vergessenwerden" in Art. 17 Abs. 2 DS-GVO, wenn es auch begrifflich neu ist, nur bedeutet, dass der Verantwortliche, der personenbezogene Daten öffentlich gemacht hat (i. d. R. im Internet), andere Stellen, die die Daten weiterverarbeiten, darüber informieren muss, dass ein Betroffener die Löschung von Links zu diesen personenbezogenen Daten verlangt hat, wobei diese Pflicht durch Implementierungskosten des Verpflichteten relativiert wird.

---

68 Vgl. Art. 9 SE-VO.
69 Dazu schon oben C.I.3.
70 Ausführlich beschrieben von *Franck*, RDV 2016, 111.

Neu ist dagegen das unterhalb des Löschungsrechts angesiedelte Recht auf Einschränkung der Verarbeitung in Art. 18 DS-GVO. Die vier genannten, abschließenden Voraussetzungen betreffen Situationen, in denen der Betroffene zwar (noch) keine Löschung, aber die Einschränkung der Verarbeitung seiner personenbezogenen Daten wünscht. Dies ist z. B. der Fall, wenn die betroffene Person die Richtigkeit ihrer Daten bestreitet, dieser Umstand aber noch geprüft werden muss (Art. 18 Abs. 1 lit. a) oder wenn der Verantwortliche die Daten für den Verarbeitungszweck nicht mehr benötigt, die betroffene Person sie aber zur Ausübung von Rechtsansprüchen noch braucht (Art. 18 Abs. 1 lit. c).

Eine problematische Seite hat das Recht auf Datenübertragbarkeit in Art. 20 DS-GVO. Damit soll Betroffenen vor allem ermöglicht werden, ihre Profile in sozialen Netzwerken oder ihre E-Mail-Konten zu anderen Anbietern mitzunehmen. Art. 20 erlaubt daher, ihre personenbezogenen Daten in einem „strukturierten, gängigen und maschinenlesbaren Format" zu erhalten. Zum Problem für den Datenschutz Dritter kann dieses Betroffenenrecht deshalb werden, weil bei der Übertragung von Profilen oder E-Mail-Konten unvermeidlich auch Daten Dritter mitübertragen werden, etwa empfangene Mails oder Chat-Verläufe.[71]

Erwägungsgrund 59 der DS-GVO verweist schließlich darauf, dass die Betroffenenrechte unentgeltlich ausgeübt werden sollen, Anträge auch elektronisch gestellt werden dürfen und der Verantwortliche „verpflichtet werden sollte", innerhalb eines Monats zu antworten, allerdings nur „gegebenenfalls" mit einer Begründung. Sind diese Anforderungen schon etwas vage formuliert, so bleibt abzuwarten, inwieweit die Mitgliedstaaten von den Regelungsbefugnissen nach Art. 23 DS-GVO Gebrauch machen werden. Bei Art. 23 handelt es sich um eine der Öffnungsklauseln, nach denen die Mitgliedstaaten ausdrücklich Beschränkungen der Verordnung einführen dürfen. Zwar sollen solche Beschränkungen „den Wesensgehalt der Grundrechte und Grundfreiheiten achten und eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme" darstellen, jedoch reicht die Liste der Gründe, aus denen Einschränkungen erlaubt sind, von der nationalen (Art. 23 Abs. 1 lit. a) über die öffentliche Sicherheit (Art. 23 Abs. 1 lit. c), den Schutz „sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses" (Art. 23 Abs. 1 lit. e) bis zur Durchsetzung zivilrechtlicher Ansprüche" (Art. 23 Abs. 1 lit. j).

---

71 Das hält *Schantz*, NJW 2016, 1841, 1845, für unproblematisch, da das Recht auf Datenübertragbarkeit sonst leer liefe.

V. Datenschutz-Folgenabschätzung

Im Vergleich zur Vorabkontrolle nach § 4d Abs. 5 BDSG neu und weitreichender ist die Pflicht des Datenverarbeiters zur Datenschutz-Folgenabschätzung nach Art. 35 Abs. 1 DS-GVO. Diese besteht, wenn die Form der Verarbeitung, vor allem bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für Rechte und Freiheiten natürlicher Personen zur Folge hat. Beispielhaft sind die umfangreiche Verarbeitung sensibler Daten (Art. 35 Abs. 3 lit. b) oder die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (Art. 35 Abs. 3 lit. c) genannt. Dann muss gemäß Art. 36 DS-GVO eine vorherige Konsultation mit der Aufsichtsbehörde stattfinden. Eine Vorab-Genehmigungspflicht bedeutet das nicht, aber die Aufsichtsbehörde kann schriftliche Empfehlungen abgeben (Art. 36 Abs. 2 DS-GVO). Außerdem bleiben ihre sonstigen Aufsichts- und Abhilfebefugnisse nach Art. 58 DS-GVO[72] unberührt.

In den Regelungen über die Folgenabschätzung werden z. T. „Informationsmöglichkeiten" für den Betriebsrat gesehen.[73] Ein rechtlicher Anspruch hinsichtlich des durch die DS-GVO neu geschaffenen Instruments der Datenschutz-Folgenabschätzung ergibt sich allerdings weder aus den allgemeinen Informationsrechten des Betriebsrats nach dem BetrVG (§§ 75 und 80) noch aus der DS-GVO direkt.[74] Die enthält in Art. 35 Abs. 2 eine ausdrückliche Regelung im Zusammenhang mit der Datenschutz-Folgenabschätzung nur zum Datenschutzbeauftragen. Sofern vorhanden, muss der Datenschutzbeauftragte konsultiert werden.

VI. Durchsetzung und Sanktionen

Zum Zwecke der Durchsetzung der DS-GVO und der Sanktionierung von Verstößen wurden Meldepflichten, Beschwerderechte der Betroffenen, Bußgelder, Haftung und Schadensersatz sowie ein Verbandsklagerecht geregelt. In diesem Bereich gibt es auch etliche Regelungsaufträge an die nationalen Gesetzgeber, etwa zur Festlegung weiterer Sanktionsarten in Art. 84 DS-GVO. Für Deutschland bedeutet das, dass die strafrechtlichen Sanktionen in § 44 Abs. 1 BDSG beibehalten werden könnten.

---

72 Zur Aufsicht unten C.VII.
73 *Wedde*, CuA 2016, 8 ff.
74 Zur Rolle des Betriebsrats s. unten E.IV.1.

Die Dokumentationspflicht in § 4g Abs. 2 i. V. m. § 4e BDSG wird in Art. 28 DS-GVO aufgegriffen und vergleichbar geregelt.[75] Weiter als § 42a BDSG regeln Art. 31 und 32 DS-GVO Meldepflichten bei Datenschutzverstößen, wobei allerdings durch technische und organisatorische Maßnahmen die Meldepflicht entfallen kann.

Bußgelder nach § 43 BDSG wurden bislang eher zurückhaltend verhängt, von einzelnen Ausnahmen, wie der Geldbuße in Höhe von ca. 1,5 Millionen Euro für die Supermarktkette Lidl im Jahre 2008 abgesehen,[76] die Verstöße gegen den Beschäftigtendatenschutz betraf.[77] Nun wird in der DS-GVO der Rahmen für Bußgelder an das Kartellrecht angelehnt und in Art. 83 Abs. 4 DS-GVO deutlich auf bis zu 10 Millionen Euro oder bei Unternehmen auf bis zu 2 % des weltweiten Jahresumsatzes erhöht. Bei Verstößen gegen die Verarbeitungsgrundsätze der DS-GVO – ausdrücklich auch bei Verstößen gegen die Voraussetzungen einer rechtmäßigen Einwilligung –, bei Verstößen gegen die Betroffenenrechte und bei Missachtung von Anweisungen der Aufsichtsbehörden kann gemäß Art. 83 Abs. 5 DS-GVO das Bußgeld sogar bis zu 20 Millionen Euro oder 4 % des Jahresumsatzes betragen. Allerdings könnte diese Bußgeldhöhe eher symbolischen Wert haben. Zum einen funktioniert diese Abschreckung nur bei effizienter Aufsicht, deren Verfahren sehr komplex geregelt ist. Zum anderen ist zweifelhaft, ob entsprechende Beträge je verhängt würden, da die Aufsichtsbehörden ein erhebliches Prozessrisiko tragen würden. Allerdings wird in der Diskussion um die Auswirkungen der DS-GVO gerade von Unternehmensseite immer wieder auf die Risiken durch die hohen Bußgelder verwiesen[78] und in der Bußgeldregelung gar die praxisrelevanteste Neuerung der DS-GVO gesehen.[79] Verhängt werden könnten die hohen Bußgelder jedenfalls im Prinzip auch bei Verstößen gegen den Beschäftigtendatenschutz.

Neben den staatlichen Bußgeldern könnte in Zukunft die zivilrechtliche Haftung mit Schadensersatzansprüchen bei der Sanktionierung von Datenschutzverstößen eine größere Rolle spielen. Eine Schadensersatznorm enthält zwar auch schon § 7 BDSG, der Art. 23 der EG-Datenschutzrichtlinie umsetzt und sowohl für schuldhafte Datenschutzverstöße von öffentlichen wie nichtöffentlichen Stellen

---

75 *Gierschmann*, ZD 2016, 51, 53.

76 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, Dem Datenschutz wachsen Zähne, Pressemitteilung 11. 9. 2008, abrufbar unter: *www.datenschutzzentrum.de/presse/20080911-lidl-bussgeldverfahren.html* (abgerufen am 6. 7. 2016).

77 § 32 BDSG gab es da allerdings noch nicht. Diese Norm war gerade die gesetzgeberische Reaktion u. a. auf den Lidl-Fall.

78 *Faust/Spittka/Wybitul*, ZD 2016, 120.

79 *Ashkar*, DuD 2015, 796, 799.

gilt. Nur für öffentliche Stellen regelt § 8 BDSG zusätzlich eine verschuldensunabhängige Gefährdungshaftung. Der Schadensersatzanspruch spielt auch deshalb bislang, vor allem bei Unternehmen, in der Praxis so gut wie keine Rolle.[80]

Eine verschuldensunabhängige Haftung führt zwar auch die DS-GVO nicht ein (Art. 82 Abs. 3). Dennoch bringt Art. 82 DS-GVO zwei Verbesserungen im Vergleich zur derzeitigen Rechtslage. Zum einen wird eine Regelungslücke des bisherigen Rechts geschlossen, indem nicht nur der Verantwortliche, sondern gemäß Art. 82 Abs. 2 auch der Auftragsdatenverarbeiter haftet, wenn auch beschränkt auf die Nichteinhaltung der ihm auferlegten Pflichten aus der Verordnung bzw. der rechtmäßig erteilten Anweisungen des Verantwortlichen. Verantwortlicher und Auftragsdatenverarbeiter haften nach Art. 82 Abs. 4 als Gesamtschuldner, können sich also gegenüber dem Geschädigten nicht auf den jeweils anderen Verarbeitungszusammenhang berufen. Zum anderen ist gemäß Art. 82 Abs. 1 nicht nur der materielle, sondern auch der immaterielle Schaden zu ersetzen. Nach deutschem Recht ist der Ersatz immateriellen Schadens bei einer Datenschutzverletzung nur ausnahmsweise bei besonders schwerer Verletzung des allgemeinen Persönlichkeitsrechts zu gewähren. Diese Einschränkung wird in Zukunft nicht mehr möglich sein. Das gilt auch für den im Rahmen von Art. 88 DS-GVO national geregelten Beschäftigtendatenschutz, denn Erwägungsgrund 146 stellt klar, dass als Verstöße gegen die DS-GVO, die Schadensersatzansprüche auslösen können, auch Verstöße gegen Rechtsvorschriften der Mitgliedstaaten gelten, die aufgrund der DS-GVO erlassen wurden. Das bedeutet, dass ein Verstoß gegen einen im Rahmen von Art. 88 Abs. 3 DS-GVO[81] der Kommission gemeldeten § 32 BDSG die Schadensersatzansprüche (und auch die Bußgeldhöhen) der Verordnung auslöst.

Wie sich schließlich der immaterielle Schadensersatzanspruch in der europäischen Rechtspraxis konkret darstellen wird, bleibt abzuwarten. Jedenfalls sind die Kriterien europarechtsautonom auszulegen. In den Mitgliedstaaten ist der Umgang mit immateriellem Ersatz sehr unterschiedlich. Insbesondere in Deutschland sind die Ersatzbeträge niedrig. Erwägungsgrund 146 verlangt „vollständigen und wirksamen" Schadensersatz und verweist für die Bemessung des Ersatzes auf die Rechtsprechung des EuGH. Der betont, dass zivilrechtliche Sanktionen abschreckend sein müssen.[82]

---

80 *Gola/Schomerus*, BDSG, Kommentar, 2015, 12. Aufl., § 7 Rn 2.

81 Dazu genauer unten E.II.2.d).

82 Etwa EuGH, Urt. v. 17. 12. 2015 – C-407/14, EuZW 2016, 183 m. w. N. (Arjona Camacho).

Kapitel VIII der DS-GVO über Haftung und Sanktionen erleichtert den Rechtsweg für Betroffene bei ihren Klagen gegen Verantwortliche oder Auftragsdatenverarbeiter. Nach Art. 79 Abs. 2 DS-GVO i. V. m. Erwägungsgrund 145 bleibt es dem Betroffenen überlassen, ob er die Gerichte des Mitgliedstaates anruft, in dem der Verantwortliche oder der Auftragsdatenverarbeiter eine Niederlassung hat oder in dem die betroffene Person ihren Aufenthaltsort hat. Von dieser Wahlfreiheit des Betroffenen gibt es nur eine Ausnahme für Behörden, die in Ausübung ihrer hoheitlichen Befugnisse handeln (Art. 79 Abs. 2 Satz 2 Halbs. 2).

Schließlich sieht die DS-GVO in Art. 80 Abs. 1 noch eine Art Prozessführungsbefugnis vor. Organisationen oder Vereinigungen ohne Gewinnerzielungsabsicht können von betroffenen Personen beauftragt werden, diese vor Aufsichtsbehörden oder Gerichten zu vertreten. Das geht weiter als der auch auf EU-Recht basierende § 23 Abs. 2 AGG, der die Möglichkeit einer Beistandschaft für Antidiskriminierungsverbände regelt, allerdings auf die Unterstützung in der mündlichen Verhandlung beschränkt ist und nach Abs. 3 nur die Möglichkeit eröffnet, bei der Formulierung von Klageanträgen zu unterstützen, ohne selbst als Vertreter aufzutreten.

Neben der Prozessführungsbefugnis in Art. 80 Abs. 1 eröffnet Art. 80 Abs. 2 DS-GVO für die Mitgliedstaaten die Möglichkeit, ein Verbandsklagerecht einzuführen.[83]

VII. Aufsichts- und Auslegungsinstanzen

So wichtig umfassende materielle Regelungen zur Zulässigkeit von Datenverarbeitung und gestärkte Betroffenenrechte sind, kommt es für die Wirksamkeit der Regelungen auf die Durchsetzung, also auf die Vollzugsebene an. Die ist in der DS-GVO in den Kapiteln VI und VII über die Aufsichtsbehörden (Art. 51 ff.) und die Zusammenarbeit zwischen den Aufsichtsbehörden aus verschiedenen Mitgliedstaaten (Art. 60 ff.) geregelt. Der Umstand allein, dass die Regelungen Teil einer unmittelbar geltenden Verordnung sind, die Anwendungsvorrang vor nationalem Recht hat, stellt keine Garantie für eine wirkungsvolle Umsetzung dar, wie die Erfahrungen mit der 14 Jahre alten verbraucherschützenden Verordnung 2001/44/EG (EuGVVO) zeigen.[84]

---

83 Zur Verbandsklage unten E.IV.2.

84 *Dieterich*, ZD 2016, 260, 263.

1. Datenschutzbehörden

Die Ausgestaltung der Datenschutzaufsicht, vor allem für die Fälle, in denen mehrere Mitgliedstaaten oder die ganze EU betroffen sind, war in den Verhandlungen zwischen Kommission, Parlament und Rat eines der umstrittensten Themen.[85]

Unter der Geltung der EG-Datenschutzrichtlinie erfolgt die Datenschutzaufsicht und -durchsetzung durch die Datenschutzbehörden der Mitgliedstaaten (Art. 28 Abs. 1 DS-RL 95/46/EG). Dabei hat nur Deutschland mit den Landes- und dem Bundesdatenschutzbeauftragten mehrere Aufsichtsbehörden. Sie sind auch für Unternehmen, also auch für den Beschäftigtendatenschutz zuständig.[86] Die Koordination der nationalen Datenschutzbehörden in den Mitgliedstaaten erfolgt bislang über Art. 28 Abs. 6 der Datenschutzrichtlinie und über die Art. 29-Datenschutzgruppe.[87] Für die Koordination innerhalb Deutschlands hat bislang der so genannte Düsseldorfer Kreis diese Funktion. Der hat sich aber auch schon mit grenzüberschreitenden Problemen befasst und im Jahr 2010 eigene verschärfende Bedingungen für die Datenübertragung in Drittstaaten nach dem EU-USA-Safe-Harbor-Abkommen aufgestellt.[88]

Die Arbeit der Aufsichtsbehörden soll harmonisiert werden. Zunächst muss jeder Mitgliedstaat gemäß Art. 51 und 52 DS-GVO überhaupt erst einmal eine unabhängige Aufsichtsbehörde[89] schaffen. Die Rolle der Aufsichtsinstanzen im privaten Bereich verändert sich in der DS-GVO. Die externe Kontrolle von Unternehmen durch Aufsichtsbehörden ist im BDSG relativ eng geregelt, da das BDSG von der Vorstellung ausgeht, dass im Unternehmen der Grundsatz der Eigenkontrolle gilt, die vor allem durch den betrieblichen Datenschutzbeauftragten ausgeübt werden soll. Bei der Verantwortung der Unternehmen für den Datenschutz bleibt es zwar auch unter der Verordnung. Sie wird eher noch gestärkt durch die Datenschutz-Folgenabschätzung (Art. 35), Datenschutz durch Technik (Art. 25),[90] Zertifizierungen (Art. 42 f.) oder die Möglichkeit, die Aufsichtsbehörden vorab

---

85 *Nguyen*, ZD 2015, 265.

86 Für das Telekommunikationsrecht (TKG und TMG) ist allerdings ausschließlich der Bundesdatenschutzbeauftragte zuständig.

87 *Dix*, DuD 2012, 318, 319.

88 *Düsseldorfer Kreis*, Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen, 2010.

89 Das war zwar auch schon unter der DS-Richtlinie so, aber gerade Deutschland musste sich erst vom EuGH ermahnen lassen, für die Unabhängigkeit seiner Aufsichtsbehörden zu sorgen: EuGH, Urt. v. 9. 3. 2010 – C-518/07 (Kommission/Deutschland), NJW 2010, 1265.

90 Dazu unten E.II.4.

zu Rate zu ziehen (Art. 36). Letzteres darf aber nicht dazu führen, die Verantwortung für die Klärung von Compliance-Fragen auf die Aufsichtsbehörden zu verlagern.[91]

Die unternehmerische Verantwortung für den Datenschutz bleibt also bestehen und wird sogar erweitert. Allerdings werden daneben in Art. 57 DS-GVO die Aufgaben der externen Aufsichtsbehörden weiter gefasst. Deren Aufgabenkatalog ist im Vergleich zur DS-Richtlinie mit 22 Einzelaufgaben in Art. 57 Abs. 1 DS-GVO erheblich ausgedehnt worden und reicht von der Kernaufgabe Überwachung und Durchsetzung der DS-GVO (Art. 57 Abs. 1 lit. a) über die Aufklärung von Unternehmen zu datenschutzrechtlichen Pflichten (Art. 57 Abs. 1 lit. d) und die Bearbeitung von Anfragen und Beschwerden von Betroffenen (Art. 57 Abs. 1 lit. e und f) bis zur Genehmigung von Standardvertragsklauseln für Datentransfers ins EU-Ausland (Art. 57 Abs. 1 lit. r). Die Untersuchungs-, Abhilfe- (weiter als § 38 Abs. 5 BDSG) und Genehmigungsbefugnisse sind in Art. 58 DS-GVO geregelt, einer Norm, die gleich zwei Öffnungsklauseln für nationale Regelungen enthält. Gemäß Art. 58 Abs. 5 müssen die Mitgliedstaaten den nationalen Aufsichtsbehörden die Befugnis einräumen, „gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben". Art. 58 Abs. 6 erlaubt es darüber hinaus den Mitgliedstaaten, die Befugnisse der Aufsichtsbehörden zu erweitern.

Neu eingerichtet wird der Europäische Datenschutzausschuss, der die Art. 29-Datenschutzgruppe der DS-Richtlinie ersetzt, und sich aus den Leitern der nationalen Aufsichtsbehörden zusammensetzt. Bei Mitgliedstaaten wie Deutschland, wo es mehrere Aufsichtsbehörden gibt, ist gemäß Art. 68 Abs. 4 DS-GVO ein gemeinsamer Vertreter zu bestimmen.[92] Der Europäische Datenschutzausschuss soll gemäß Art. 70 DS-GVO die einheitliche Anwendung der DS-GVO sicherstellen, hat dazu aber mit Stellungnahmen, Leitlinien und Empfehlungen vorwiegend nur beratende Kompetenzen, wie sich aus der langen Liste des Art. 70 Abs. 1 DS-GVO ergibt.[93]

Im Kommissionsentwurf von 2012 war noch das so genannte One-Stop-Shop-Verfahren, also das Prinzip einer einheitlichen Anlaufstelle vorgesehen,[94] wonach die einzig zuständige Datenschutzbehörde für grenzüberschreitende datenschutzrechtliche Aktivitäten eines Unternehmens diejenige des Mitgliedstaates

---

91 So auch schon in der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Struktur der künftigen Datenschutzaufsicht in Europa, 87. Konferenz der Datenschutzbeauftragten, 27. 3. 2014, Nr. 6.

92 Vorschläge zur deutschen Vertretung im Europäischen Datenschutzausschuss bei *Kühling/Martini*, EuZW 2016, 448, 453.

93 *Roßnagel/Nebel/Richter*, ZD 2015, 455.

94 *Reding*, ZD 2012, 195, 196 f.

sein sollte, in dem das datenverarbeitende Unternehmen seine Hauptniederlassung hat. Das hätte dazu geführt, dass für Unternehmen mit Niederlassungen in mehreren Mitgliedstaaten nicht mehr unterschiedliche nationale Datenschutzbehörden zuständig gewesen wären. Da dieser Weg wenig bürgerfreundlich ist,[95] ist in der verabschiedeten DS-GVO dieser Ansatz zugunsten der von Datenverarbeitung Betroffenen abgeschwächt und durch das Kooperations- und Kohärenzverfahren in Art. 60 ff. DS-GVO ersetzt worden, bei dem Aufsichtsbehörden mehrerer Mitgliedstaaten zuständig sein können und der neu einzurichtende Europäische Datenschutzausschuss nach Art. 68 DS-GVO eine wichtige Rolle bei der einheitlichen Anwendung der DS-GVO spielen wird.[96]

Nur im Kohärenzverfahren, das der Berichterstatter des Europäischen Parlaments für den innovativsten Teil der Grundverordnung hält,[97] kann der vorwiegend beratend tätige Europäische Datenschutzausschuss nach Art. 65 in bestimmten, engen Fällen verbindliche Beschlüsse treffen. Das gilt grundsätzlich für alle Datenschutzfragen der DS-GVO, auch für den Beschäftigtendatenschutz. Es wird zunächst die federführende Aufsichtsbehörde i. S. v. Art. 56 DS-GVO bestimmt – sie richtet sich nach der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen in der EU. Die federführende Aufsichtsbehörde versucht gemäß Art. 60 DS-GVO, mit den anderen betroffenen Aufsichtsbehörden einen Konsens zu erzielen. Wenn das nicht gelingt, tritt das Kohärenzverfahren nach Art. 63 ff. DS-GVO auf den Plan, in dem der Europäische Datenschutzausschuss in bestimmten Fällen nach Art. 65 verbindliche Beschlüsse erlassen kann. Die endgültige Entscheidung wird dann allerdings nach Einhaltung etlicher Fristen und weiterer Formalia von der nationalen Aufsichtsbehörde getroffen (Art. 65 Abs. 6 DS-GVO). Schließlich kann aber nach Art. 66 die nationale Aufsichtsbehörde „unter außergewöhnlichen Umständen" das Kohärenzverfahren überspielen und selbst einstweilige Maßnahmen treffen. Insgesamt dürfte das bürokratische Kohärenzverfahren eher zu einer Selbstlähmung der Aufsicht als in absehbarer Zeit zu einer Klärung der vielen offenen Auslegungsfragen und einem einheitlichen Gebrauch der Datenschutznormen der DS-GVO in den Mitgliedstaaten führen.

---

95 Daher war dieses Prinzip auch von der Konferenz der Datenschutzbeauftragten kritisiert worden: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Struktur der künftigen Datenschutzaufsicht in Europa, 87. Konferenz der Datenschutzbeauftragten, 27. 3. 2014.

96 *Nguyen*, ZD 2015, 265.

97 *Albrecht*, CR 2016, 88, 96.

2. Rechtsschutz

Daher wird es besonders auf die Rolle der Rechtsprechung ankommen und zwar zum einen im Hinblick auf die Harmonisierungsfunktion des EuGH und zum anderen beim bereichsspezifischen Datenschutz, insbesondere beim Beschäftigtendatenschutz, auf die Rolle der nationalen (Arbeits-)Gerichte. Der einheitliche Rechtsrahmen der DS-GVO führt jedenfalls nicht zwingend zu einheitlicher Rechtsanwendung,[98] schon gar nicht, wenn es zahlreiche Öffnungen für mitgliedstaatliche Regelungen gibt.

a) Institutioneller Rechtsschutz

Neben einer Prozessvertretungsbefugnis i. S. v. Art. 80 Abs. 1 DS-GVO, die durch die Mitgliedstaaten gemäß Art. 80 Abs. 2 DS-GVO in ein Verbandsklagerecht erweitert werden kann,[99] sieht Art. 58 Abs. 5 DS-GVO vor, dass die Aufsichtsbehörden den Justizbehörden Datenschutzverstöße melden bzw. ggf. gerichtliche Verfahren selbst einleiten oder sich daran beteiligen können. Die Mitgliedstaaten sind verpflichtet, die nähere Ausgestaltung in ihrem nationalen Recht vorzunehmen. Das Konzept ist nicht neu. Schon Art. 28 Abs. 3 DS-Richtlinie sieht Anzeige- und Klagerechte der Aufsichtsbehörde vor. In § 38 Abs. 1 Satz 6 und § 44 Abs. 2 BDSG sind aber nur die Anzeigebefugnisse umgesetzt worden.

b) Individueller Rechtsschutz

Zunächst haben die nationalen (Arbeits-)Gerichte die DS-GVO wie auch alles andere EU-Recht anzuwenden und auszulegen. Wegen des Anwendungsvorrangs einer Verordnung gilt das auch, wenn das nationale Datenschutzrecht nicht außer Kraft gesetzt oder angepasst wird. Wenn sich vor den nationalen Gerichten Auslegungsfragen ergeben, die im Wege europarechtskonformer Auslegung nicht beantwortet werden können, kann, bzw. wenn es sich um die letzte Instanz handelt, muss der EuGH nach Art. 267 AEUV im Wege der Vorabentscheidung angerufen werden, was Gerichtsverfahren deutlich verlängern wird, da die DS-GVO vor allem mit Generalklauseln arbeitet, die einen erheblichen Auslegungsbedarf nach sich ziehen werden. In Deutschland mit seinem umfassenden allgemeinen und bereichsspezifischen Datenschutzrecht gibt es bereits eine umfangreiche Rechtsprechung zum Datenschutz, die aber nicht ohne weiteres auf die Auslegung der DS-GVO übertragen werden kann. Es wird darauf ankommen,

---

98 *Dieterich*, ZD 2016, 260.

99 Das Thema Verbandsklage wird im Zusammenhang mit den kollektiven Rechten im Beschäftigtendatenschutz behandelt, s. unten E.IV.2.

was der deutsche Gesetzgeber im Einzelnen im Rahmen von Art. 88 DS-GVO an nationalem Beschäftigtendatenschutz wie auch im Rahmen der anderen Bereichsausnahmen der DS-GVO regelt. Ähnlich wie in der Rechtsvergleichung zwischen verschiedenen nationalen Rechtsordnungen, können gleiche oder ähnliche Begrifflichkeiten im nationalen und europäischen Recht nicht mit der Rechtsdogmatik eines Mitgliedstaates allein ausgelegt werden. Vielmehr ist die DS-GVO ein autonomer europäischer Rechtsakt, der vor dem Hintergrund seiner eigenen Entstehungsgeschichte sowie den Zielen und Zwecken, die der europäische Gesetzgeber ihm beigemessen hat, auszulegen ist. Die Auslegung des Beschäftigtenbegriffs, der für den Beschäftigtendatenschutz zentral ist, ist dafür nur ein Beispiel unter vielen.[100]

Sofern Mitgliedstaaten den Beschäftigtendatenschutz nach Art. 88 DS-GVO selbst regeln, ergibt sich nichts grundsätzlich Anderes. Zuständig sind die nationalen (Fach-)Gerichte, die aber auch bei nationaler Regelung einer Datenschutzmaterie, hier des Beschäftigtendatenschutzes, die allgemeinen Mindeststandards der Grundverordnung sowie besondere Anforderungen, wie für den Beschäftigtendatenschutz in Art. 88 Abs. 2 DS-GVO festgelegt, einhalten müssen. Bei Zweifeln an diesen beiden Punkten, ist wiederum die Sache dem EuGH gemäß Art. 267 AEUV vorzulegen.

Besonders brisant ist die Frage, inwieweit – jedenfalls bei einem national geregelten Beschäftigtendatenschutz – die Rechtsprechung des Bundesverfassungsgerichts zur informationellen Selbstbestimmung aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG ohne Einschränkung aufrechterhalten werden kann.[101] Grundsätzlich gilt, dass für Regelungen, die ihren Ursprung im EU-Recht haben, die GR-Charta der verfassungsrechtliche Maßstab ist. Haben sie ihren Ursprung im nationalen Recht, wie bei einem national geregelten Beschäftigtendatenschutz, ist der Maßstab das GG.[102] Soweit sich dann die Rechtsprechung des BVerfG mit den Anforderungen in Art. 88 Abs. 2 DS-GVO deckt – dort ist festgelegt, dass nationale Vorschriften zum Beschäftigtendatenschutz die Menschenwürde und die Grundrechte der betroffenen Person wahren müssen – können die bisherigen Auslegungsergebnisse weiter gelten. Allerdings würde der national geregelte

---

100 Dazu genauer unten E.II.2.a).

101 Zu den verfassungsrechtlichen Problemen, insbesondere dem Verhältnis von BVerfG und EuGH schon *Körner*, Die Reform des EU-Datenschutzes: Der Entwurf einer EU-Datenschutz-Grundverordnung (DS-GVO), Teil II, ZESAR 2013, 153, 155 ff.; grundlegend dazu: *Pötters, Stephan*, Grundrechte und Beschäftigtendatenschutz, 2013.

102 *Heuschmid*/Lörcher, NK-GA, Art. 51 Rn. 23–26; BVerfG, Urt. v. 15. 12. 2015 – 2 BvR 2735/14. Im Übrigen siehe schon oben C.I.2 und 3.

Beschäftigtendatenschutz nicht losgelöst von der DS-GVO gelten, sondern auf ihrer Basis.

Darüber hinaus ist für den allgemeinen Datenschutz zu bedenken, dass Datenschutz auf der höheren, der europäischen, Ebene in Art. 8 GR-Charta speziell grundrechtlich geschützt ist. Das Verhältnis zwischen EU-Grundrechten und nationalen Grundrechten ist zwar nach wie vor nicht abschließend geklärt.[103] Für die DS-GVO und das deutsche Recht auf informationelle Selbstbestimmung ist aber zu berücksichtigen, dass die unmittelbar geltende Verordnung eine andere Perspektive einnimmt als das Recht auf informationelle Selbstbestimmung. Letzteres versteht den Datenschutz ausschließlich aus der Perspektive der betroffenen Person, also als Abwehrrecht, wie es für Grundrechte charakteristisch ist. In der DS-GVO hat der Datenschutz der betroffenen Person eher eine Abwägungsfunktion. Immer müssen auch die Interessen des Datenverwenders berücksichtigt werden. Schon im ersten Artikel der DS-GVO wird deutlich, dass der freie Verkehr personenbezogener Daten gleichgewichtig neben dem Datenschutz steht. Das ist für sich betrachtet auch konsequent, da es sich bei der DS-GVO nicht primär um eine verfassungsrechtliche Schutzregelung, sondern um eine Binnenmarktregelung handelt. Da jedenfalls die Grundprinzipien der DS-GVO durch mitgliedstaatliche Gesetzgebung nicht ausgehebelt werden dürfen, hat die Rechtsprechung des BVerfG zur informationellen Selbstbestimmung für das in der DS-GVO geregelte allgemeine Datenschutzrecht nur insoweit Bestand als diesem Perspektivenwechsel im Datenschutz Rechnung getragen wird.

In Zukunft fällt der verfassungsrechtliche Schutz des Betroffenen in den Bereichen, für die die DS-GVO keine mitgliedstaatliche Öffnung enthält, dem EuGH zu. In diesen Fällen steht der Individualrechtsbehelf Verfassungsbeschwerde dann nicht mehr zur Verfügung. Der EuGH hat sich in der jüngsten Vergangenheit mehrfach mit Datenschutzfragen befasst und in drei wichtigen Urteilen – der Ungültigerklärung der EU-Richtlinie zur Vorratsdatenspeicherung,[104] zu Google[105] und zu Facebook[106] – persönlichkeitsschutzfreundliche Lösungen gefunden. In diesen Fällen war die zunächst geäußerte Befürchtung unbegründet, dass der EuGH als für sämtliche mit dem Binnenmarkt zusammenhängenden Fragen allzuständiges Gericht, auf die in Deutschland besonders starke verfassungsrechtliche Seite des Datenschutzes nicht vorbereitet und daher das

[103] Dazu schon oben C.I.3.
[104] EuGH, Urt. v. 8. 4. 2014 – C-293/12, C-594/12, DuD 2014, 488.
[105] EuGH, Urt. v. 13. 5. 2014 – C-131/12, DuD 2014, 559.
[106] EuGH, Urt. v. 6. 10. 2015 – C-362/14, DuD 2015, 823.

bisherige, durch das BVerfG gewährte hohe Schutzniveau in Zukunft nicht zu gewährleisten sei.

Allerdings handelt es sich nur um wenige Fälle, in denen der EuGH sich zu Datenschutzfragen äußern konnte. Das europäische Gericht hatte bislang viel zu selten Gelegenheit, sich mit dem Grundrecht auf Datenschutz aus Art. 8 GR-Charta zu befassen (und konnte es daher nicht effizient schützen).

In Zukunft wird also die Interpretation der unbestimmten Rechtsbegriffe der DS-GVO zunächst den einzelstaatlichen Gerichten obliegen, die sich einerseits an den bisherigen unterschiedlichen Datenschutzkulturen in den Mitgliedstaaten orientieren werden und die andererseits nicht an die Auslegungsergebnisse der Aufsichtsbehörden gebunden sind, denn diese sind, auch nach einem Kohärenzverfahren, nur an die beteiligten Aufsichtsbehörden adressiert und haben keine allgemeine Rechtswirkung. Selbst national gibt es nur Rechtsklarheit, wenn oberste Gerichte in einzelnen Fällen entscheiden. Europäisch gilt das erst recht: nur in Einzelfällen – mögen Sie auch typisch sein – kann der EuGH in einem jahre- bis jahrzehntelangen Prozess Einzelfragen beantworten. Der Rechtssicherheit sowohl für Datenverarbeiter wie für Betroffene ist das abträglich.[107]

VIII. Übermittlung an Drittstaaten

Die in Art. 44 ff. DS-GVO geregelte Datenübermittlung an Drittstaaten entsprechen im Wesentlichen dem geltenden Recht. Es bleibt gemäß Art. 45 Abs. 3 bei der Adäquanzentscheidung der Kommission, der Datenübermittlungsmöglichkeit aufgrund geeigneter Datenschutzgarantien gemäß Art. 46 oder von der Aufsichtsbehörde genehmigter Binding Corporate Rules nach Art. 47. Als Garantie i. S. v. Art. 46 gelten nun auch von der Kommission im Wege delegierter Rechtsakte für allgemeinverbindlich erklärte Verhaltensregeln (Art. 46 Abs. 2 lit. e i. V. m. Art. 40 Abs. 9) und zertifizierte Datenschutzregeln (Art. 46 Abs. 2 lit. f i. V. m. Art. 42). Liegen die genannten Voraussetzungen nicht vor, erlaubt Art. 49 Abs. 1 lit. a–g Ausnahmen für bestimmte Fälle, wie das Erfordernis der Datenübermittlung für die Erfüllung eines Vertrages. Als ganz besondere Ausnahme wird dann in Art. 49 Satz 2 i. V. m. Erwägungsgrund 113 noch der Fall angefügt, dass der Verantwortliche „zwingende berechtigte Interessen" geltend machen

---

[107] *Roßnagel*, Schriftliche Stellungnahme zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung am 24. Februar 2016 im Ausschuss Digitale Agenda des Deutschen Bundestages, S. 15.

kann. Dann muss zumindest die Aufsichtsbehörde im Nachhinein von der Übermittlung in Kenntnis gesetzt und der Betroffene informiert werden.

Das auf die Beharrlichkeit eines österreichischen Jurastudenten zurückgehende Safe Harbor-Urteil des EuGH[108] untersagt dem US-amerikanischen Unternehmen Facebook den Transfer personenbezogener Daten von EU-Bürgern in die USA, solange dort keine ausreichenden Datenschutzregeln gelten. Damit hat der EuGH die von der Kommission seit dem Jahr 2000 geübte Praxis des Datentransfers von der EU in die USA gegen im Prinzip nicht mehr als das Versprechen des Empfängers, Datenschutz zu gewähren,[109] ohne Einschränkungen verboten. Dennoch bleibt der Datentransfer aus der EU in Drittstaaten auch in Zukunft die Achillesferse des europäischen Datenschutzes, da die neuen von der Kommission mit den USA ausgehandelten Privacy Shield-Regeln noch weit von Art. 8 GR-Charta entfernt sind.[110]

Zwar haben die Aufsichtsbehörden nun gemäß Art. 58 Abs. 2 lit. j DS-GVO die Befugnis, die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland anzuordnen. Die Reichweite dieses Rechtes ist aber dennoch umstritten.[111] In der Safe Harbor-Entscheidung – die sich aber auf Art. 28 Abs. 3 der DS-Richtlinie bezieht – hat der EuGH zwar einerseits festgestellt, dass die Befugnisse der Aufsichtsbehörden nicht durch die Entscheidungskompetenz der Kommission für Drittstaatenübermittlungen beschnitten werden dürfen.[112] Andererseits hat der EuGH aber klargestellt, dass nur er selbst eine derartige Entscheidung der Kommission nach Art. 25 Abs. 6 DS-Richtlinie aufheben darf.[113] Obwohl das auch schon in den nicht abschließend formulierten Art. 28 Abs. 3 DS-Richtlinie hineingelesen wurde,[114] hat der EuGH diese Vorstellung nicht in die Safe Harbor-Entscheidung übernommen. Der Umgang des EuGH mit der Privacy Shield-Vereinbarung angesichts des neuen Art. 58 Abs. 2 lit. j DS-GVO, wenn er denn Gelegenheit bekommt, sie zu bewerten, bleibt abzuwarten.[115] Jedenfalls wird die Privacy-Shield-Vereinbarung den Grundsätzen des Safe Harbor-Urteils entsprechen müssen, wonach eine Angemessenheit des Datenschutzniveaus der USA

---

108 EuGH, Urt. v. 6. 10. 2015 – C-362/14, NJW 2015, 3151.

109 KOM 2000/520/EG (Safe Harbor).

110 *Weichert*, ZD 2016, 209, 217; vgl. auch die ausführliche Darstellung mit vergleichbarer Skepsis, was die Position des EuGH angeht: *Grau/Granetzny*, NZA 2016, 405.

111 Vgl. *Dieterich*, ZD 2016, 260, 263 m. w. N.

112 EuGH, Urt. v. 6. 10. 2015 – C-362/14, NJW 2015, 3151, Rn. 53.

113 A. a. O., Rn. 61.

114 EuGH, Schlussantrag v. 23. 9. 2015 – C-362/14, BeckRS 2015, 81603, Rn. 94; so auch in der Literatur: *Bergt*, Anm. zu EuGH (Safe Harbor), MMR 2015, 753; *Kühling/Heberlein*, NvWZ 2016, 7, 8.

115 Zweifelnd *Dieterich*, ZD 2016, 260, 264.

nur in Betracht kommt, wenn die Zugriffsbefugnisse der US-Sicherheitsbehörden auf das „absolut Notwendige" beschränkt sind und europäische Bürger die Möglichkeit haben, bei einem Gericht einen wirksamen Rechtsbehelf einzulegen.[116] Klar hat der EuGH festgestellt, dass eine Regelung nicht auf das absolut Notwendige beschränkt ist, „die generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt wurden, gestattet, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen und ohne ein objektives Kriterium vorzusehen, das es ermöglicht, den Zugang der Behörden zu den Daten und deren spätere Nutzung auf ganz bestimmte, strikt begrenzte Zwecke zu beschränken, die den sowohl mit dem Zugang zu diesen Daten als auch mit deren Nutzung verbundenen Eingriff zu rechtfertigen mögen".[117]

Eine weitere Einschränkung deutet sich an: In seinem Schlussantrag vom 8. September 2016 hat der Generalanwalt beim Europäischen Gerichtshof *Paolo Mengozzi* aufgrund eines Gutachtenauftrags des Europäischen Parlaments das Abkommen zwischen der EU und Kanada zur Fluggastdatenverarbeitung in mehreren Punkten für unvereinbar mit der GR-Charta gehalten.[118] Diese Rechtsansicht dürfte auch Auswirkungen auf die entsprechenden Abkommen mit den USA und Australien sowie auf den Umgang mit der im April 2016 beschlossenen EU-Richtlinie über die Verwendung von Fluggastdaten haben.

IX. Fortschritte und Defizite der DS-GVO

Die DS-GVO wird nicht ganz zu Unrecht z. T. für unterkomplex gehalten,[119] da sie kaum normative Inhalte hat, auch wenn es vor allem zum Verfahren Verbesserungen gibt, wie Art. 35 zur Folgenabschätzung, Art. 12–15 zur Transparenz oder Art. 85 Abs. 2, dem der bisherige § 41 BDSG zur Freistellung der Presse von Datenschutzvorgaben nicht entspricht.[120]

---

116 So auch *Roßnagel*, Stellungnahmen zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung, 24. 2. 2016, Ausschuss Digitale Agenda des Deutschen Bundestages, S. 13.

117 EuGH, Urt. v. 6. 10. 2015 – C-362/14, NJW 2015, 3151, Rn. 83.

118 Schlussanträge des Generalanwalts Paolo Mengozzi vom 8. September 2016, Gutachten 1/15, *http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9*

119 Begriff *Roßnagel/Nebel/Richter*, ZD 2015, 455, 460.

120 Auch schon Art. 9 der DS-Richtlinie hatte § 41 BDSG nicht entsprochen: Simitis-*Dix*, BDSG, Kommentar, 8. Aufl., § 41 Rn. 2.

Die beschworene Technikneutralität ist allerdings ein Mythos.[121] Wenn damit gemeint sein sollte, dass die Regelungen der DS-GVO auch für zukünftige digitale Technik ausreichend Schutz gewähren sollte, so wäre dieser Anspruch vermessen, da allenfalls absehbar ist, dass sich die digitale Technik weiterhin in hohem Tempo entwickeln wird, nicht aber, welche weiteren (Kontroll-)Möglichkeiten sich daraus in Zukunft ergeben und welche Regelungen dann nötig sein werden. Insofern hat man es in diesem Bereich immer mit einem „offenen Regelungsprozess"[122] zu tun. Wahrscheinlich ist Technikneutralität laut Erwägungsgrund 15 viel bescheidener gemeint, insofern es für den Schutz personenbezogener Daten nicht auf den Umstand ankommen soll, ob sie automatisiert oder manuell verarbeitet werden.

Zentrale Datenschutzprobleme bei Big Data, Smart Data oder Cloud Computing werden nicht gelöst, aber das könnte gerade gewollt sein, da es sich bei den genannten Formen von Datennutzung um wirtschaftliche Zukunftsmodelle handelt. Für das Cloud Computing ist Art. 28 Abs. 5 DS-GVO dann auch eher eine Erleichterung als eine Datenschutzvorschrift mit Fokus auf das Persönlichkeitsrecht. Nach Art. 28 Abs. 4 haftet der Verantwortliche zwar für Datenschutzverstöße durch Auftragnehmer. Nach Art. 28 Abs. 5 reicht es aber als Datenschutzgarantie i. S. v. Art. 28 Abs. 1 aus, wenn der Auftragnehmer die Einhaltung genehmigter Verhaltensregeln (nach Art. 40) oder eines zertifizierten Verfahrens zusagt.

Auch der Umstand, dass sich Arbeit immer mehr ins Internet verschiebt, wird in der Verordnung nicht berücksichtigt.[123] Industrie/Arbeit 4.0, d. h. die Vernetzung von arbeitenden Menschen und Maschinen oder neue Arbeitsformen auf Plattformen,[124] wie Crowdwork[125] werden nicht thematisiert. Das könnte damit zusammenhängen, dass die DS-GVO das Problem z. T. zurück auf die Mitgliedstaaten verlagert, da die gemäß Art. 88 Beschäftigtendatenschutz selbst regeln können. Wenn sie es allerdings einerseits nicht tun, gelten nur die Regeln der DS-GVO. Andererseits unterfallen viele derzeit neu erscheinende Formen von Arbeit im Internet nicht dem (deutschen) Arbeitnehmerbegriff, wären also auch bei einer nationalen Regelung zum Beschäftigtendatenschutz datenschutzrechtlich zunächst nur von der DS-GVO abgedeckt. Allerdings ist das letztlich eine Frage des

---

121 *Sydow/Kring*, ZD 2014, 271; zu Datenschutz durch Technik s. unten E.II.4.

122 *Simitis*, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 8. Aufl., Einleitung Rn. 106.

123 So kritisch auch *Däubler*, AiB Extra 2016, 26, 31.

124 Zum Phänomen nur *Däubler*, Digitalisierung und Arbeitsrecht, SR Sonderausgabe 2016. Zur Plattformökonomie vgl. *Däubler/Klebe*, NZA 2015, 1032.

125 Zu diesem Thema *Klebe*, AuR 2016, 277 m. w. N.; *Benner*, Crowdwork – zurück in die Zukunft? Perspektiven digitaler Arbeit, Frankfurt a. M. 2015.

Internationalen Privatrechts. Wenn man davon ausgeht, dass Art. 8 der Rom I VO auch Arbeitnehmerähnliche erfasst,[126] ließe sich ggf. eine Lösung finden.

Die DS-GVO geht noch ausschließlich vom althergebrachten Rechenzentrumskonzept der ersten Datenschutzregelungen aus, d. h. von einer verantwortlichen Stelle, die in der EU „greifbar" ist und bestimmte Regeln einhalten muss, was auch kontrolliert werden kann. Neue Konzepte für den Datenschutz im Internet enthält die Verordnung nicht, z. B. ein schon länger gefordertes eingebautes Verfallsdatum für gespeicherte Daten[127] oder/und den so genannten digitalen Radiergummi.[128] Datenschutz durch Technik[129] wird nur unspezifisch angesprochen, aber nicht (auf dem heutigen Stand der Technik) wenigstens in den Erwägungsgründen näher konturiert. So bleibt es den Anwendern überlassen, ob und was sie an technischem Datenschutz einführen wollen.

Auch die Datenschutzprinzipien, auf denen die Verordnung basiert, stammen aus den Anfangszeiten des Datenschutzes vor 45 Jahren.[130] Gerade dieser Umstand mag zu einer gewissen Beruhigung der vier Jahre lang aufgeregten Diskussion um – je nach Perspektive – zu viel oder zu wenig Datenschutz auf EU-Ebene geführt haben, denn die Prinzipien sind die vertrauten, allen voran der Zweckbindungsgrundsatz. Vor dem Hintergrund von Big Data allerdings, einer Datenauswertungsmethode, bei der es sich nicht um eine von vielen Verfahren, sondern um einen zentralen, längst global eingesetzten Mechanismus handelt, der in Zukunft jede Art von komplexer Organisationsplanung, Versorgungs- und Investitionsentscheidung, kurz alle Arten von Prognosen prägen wird, läuft der Zweckbindungsgrundsatz schon heute leer. Für Big Data-Anwendungen besteht der Wert der personenbezogenen Information gerade nicht im ursprünglichen Zweck, sondern in der Wiederverwertung einmal gesammelter Daten zu ganz anderen, im Zeitpunkt der Erhebung oft noch gar nicht bekannten Zwecken. Hier jeweils die erneute Zustimmung aller Betroffenen zur Zweckänderung zu verlangen, geht an der digitalen Realität vorbei. Google dürfte sich kaum mit Hunderten Millionen Nutzern seiner Suchmaschine in Verbindung setzen, um die Zustimmung zur Verwendung alter Suchanfragen für die Vorhersage einer Grippewelle einzuholen, auch wenn das technisch möglich wäre.[131] Das Phänomen wird

---

126 So *Heuschmid*, in: Kittner/Deinert/Zwanziger, HdB Arbeitsrecht, § 139 Rn. 16.

127 *Simitis*, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 8. Aufl., Einleitung Rn. 122.

128 Dazu umfassend: *Mayer-Schönberger*, Delete, 2010, 199 ff.

129 Dazu *Maas/Schmitz/Wedde*, Datenschutz 2014 – Probleme und Lösungsmöglichkeiten, Frankfurt 2014. Zu diesem wichtigen Konzept s. noch unten E.II.4.

130 Das Fehlen innovativer Lösungsansätze bemängelt auch *Härting/Schneider*, CR 2015, 819.

131 Beispiel aus *Mayer-Schönberger/Cukier*, Big Data, 2013, 2. Aufl., S. 193.

seit mindestens zehn Jahren beschrieben,[132] hat aber in die Verhandlungen um die DS-GVO und vor allem in deren Ergebnis kaum Eingang gefunden. Allerdings enthält die Verordnung etwas versteckt mit Art. 6 Abs. 4 eine Norm, die unter bestimmten Voraussetzungen spätere Zweckänderungen erlaubt und daher durchaus als Rechtsgrundlage herangezogen werden könnte, ohne den Schutzaspekt ausreichend zu thematisieren. Hier fehlen neue datenschutzrechtliche Modelle.[133]

Angesichts der beiden möglichen Regelungsmodelle – bereichsspezifisch-kasuistisch versus generell-abstrakt, die jeweils in ihrer Reinform Nachteile mit sich bringen – hat sich der europäische Gesetzgeber für eine vorwiegend generalklauselartige Regulierung entschieden. Anders wäre es auch kaum möglich, in 99 Artikeln das gesamte Datenschutzrecht im öffentlichen und nicht-öffentlichen Bereich abzudecken. Auch wenn in einem von rasanter technischer Entwicklung geprägten Rechtsgebiet eine vorwiegend kasuistische Regelung wegen ihrer Unübersichtlichkeit, aber auch weil sie schnell veraltet, jedenfalls für den allgemeinen Datenschutz – im bereichsspezifischen Datenschutz kann es anders aussehen – nicht empfehlenswert ist, führt der nun gewählte Weg mit vielen inhaltsleeren und nahezu beliebig füllbaren Kriterien zu großer Rechtsunsicherheit, was etwa die Interessenabwägungsklausel in Art. 6 Abs. 1 lit. f DS-GVO belegt.[134]

Diese sehr vagen allgemeinen Regelungen sprechen ganz besonders dafür, dass die Mitgliedstaaten gehalten sind, von den zahlreichen nationalen Regelungsbefugnissen Gebrauch zu machen, die die DS-GVO (fast schon wie eine Richtlinie) bietet. Das gilt auch und gerade für die fakultativen nationalen Regelungsbefugnisse, weil ansonsten „eine nicht hinnehmbare Rechtsunsicherheit" entstünde.[135]

Die Fortschritte der DS-GVO liegen auf der Verfahrensebene, die für die tatsächliche Durchsetzung der materiell-rechtlichen Ansprüche zentral ist. Die entscheidende Neuerung ist die Einführung des Marktortprinzips, wonach die DS-GVO auf die Verarbeitung aller personenbezogenen Daten innerhalb der EU anwendbar ist, unabhängig davon, wo der Datenverarbeiter seinen Sitz hat. Darüber hinaus stellt es für den Datenschutz in den meisten Mitgliedstaaten einen großen Fortschritt dar, dass nun in allen Mitgliedstaaten unabhängige Datenschutzbehörden geschaffen werden müssen, die für die Überwachung der Einhaltung der

---

132 U. a. *Cate, Fred*, The Failure of Fair Information Practice Principles, in: Winn, Jane (Hrsg.), Consumer Protection in the Age of the "Information Economy", Ashgate 2006, S. 341 ff.

133 So auch *Dammann*, ZD 2016, 307, 313.

134 So auch *Buchner*, DuD 2016, 155, 159; *Sydow/Kring*, ZD 2014, 271, 272.

135 *Kühling/Martini*, EuZW 2016, 448, 449.

DS-GVO in ihrem jeweiligen Land zuständig sind. Wichtig ist auch der Koordinationsmechanismus durch den Europäischen Datenschutzausschuss, der die einheitliche Anwendung der DS-GVO-Regeln in allen Mitgliedstaaten garantieren soll, wenn hier auch abzuwarten bleibt, als wie effizient sich das Verfahren in der Praxis erweisen wird. Schließlich stehen die Sanktionsregelungen auf der Haben-Seite der Verordnung, insbesondere die hohen Bußgelder. Auch hier wird aber erst die Zukunft zeigen, inwieweit diese in der Praxis tatsächlich verhängt werden.

D. Verhältnis der DS-GVO zum nationalen Datenschutz

Nach Art. 288 Abs. 2 Satz 2 AEUV ist eine Verordnung in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat. Entsprechend genießt auch die DS-GVO Anwendungsvorrang, d. h. sie verdrängt in ihrem Anwendungsbereich entgegenstehendes nationales Recht. Geltungsvorrang hat sie dagegen nicht, denn die EU hat keine Kompetenz, nationale Gesetze zu ändern oder außer Kraft zu setzen. Also würden auch das BDSG und andere Datenschutzgesetze weiter gelten, sofern der nationale Gesetzgeber nicht tätig würde. Da jedoch bei Kollisionen die Verordnung Anwendungsvorrang hat, müssen die nationalen Behörden und Gerichte die DS-GVO anwenden.[136] Vor diesem Hintergrund und auch, da die DS-GVO doch in weitem Umfang Raum für nationale Konkretisierung lässt, muss der nationale Gesetzgeber handeln und klarstellen, welches nationale Datenschutzrecht außer Kraft gesetzt wird und welche nationalen Regeln weiter gelten dürfen bzw. neu zu erlassen sind, um fortbestehendes nationales Datenschutzrecht mit der DS-GVO in Einklang zu bringen und unübersehbare Anwendungsprobleme zu vermeiden.

Ganz einfach ist das angesichts der Vielzahl der verschieden ausgestalteten Öffnungsklauseln in der DS-GVO nicht, denn das deutsche Datenschutzrecht ist mit seinen vielen bereichsspezifischen Regelungen komplex und unübersichtlich. Einerseits bedeutet die unmittelbare Geltung der Verordnung, dass nationale Rechtsakte, die den Inhalt der Verordnung berühren, nicht mehr erlassen werden dürfen[137] – sogar inhaltsgleiche nationale Regelungen erlaubt der EuGH nur in engen Ausnahmefällen[138] –, andererseits enthält die DS-GVO Dutzende von Öffnungen für nationale Datenschutzregelungen. Erwägungsgrund 8 der DS-GVO legt daher ausdrücklich fest, dass „wenn in dieser Verordnung Präzisierungen oder Einschränkungen ihrer Vorschriften durch das Recht der Mitgliedstaaten vorgesehen sind, können die Mitgliedstaaten Teile dieser Verordnung in ihr

136 Vgl. Protokollerklärung Nr. 17 zum Vertrag von Lissabon.

137 So der EuGH schon früh, etwa EuGH, Urt. v. 18. 2. 1970 – C-40/69, Slg. 1970, 69, 80 (Hauptzollamt Hamburg/Bollmann); *Ruffert*, in: Callies/Ruffert, EUV/AEUV, 2016, 5. Aufl., Art. 288 AEUV Rn. 20.

138 EuGH, Urt. v. 28. 3. 1985 – C-272/83, Slg. 1985, 1057 (Kommission/Italien); *Ruffert*, in: Calliess/Ruffert, AEUV, 2016, 5. Aufl., Art. 288 AEUV Rn 20.

nationales Recht aufnehmen, soweit dies erforderlich ist, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen". Das gilt für über 30 Öffnungen in der DS-GVO, die entweder in Kapitel IX („Vorschriften für besondere Verarbeitungssituationen"), im Zusammenhang mit der jeweiligen DS-GVO-Vorschrift oder durch Bezugnahme auf das Recht der Mitgliedstaaten enthalten sind.[139]

Anders als § 1 Abs. 3 BDSG enthält die DS-GVO kein Subsidiaritätsprinzip, wonach bereichsspezifische Datenschutzregeln Vorrang vor den allgemeinen Regeln des BDSG haben. Das ist für das deutsche Datenschutzrecht gravierend, weil große Teile des Datenschutzrechts bislang bereichsspezifisch geregelt sind. Soweit die DS-GVO keine Öffnung für nationale Regelungen enthält, gelten also in Zukunft nur noch die allgemeinen Datenschutzregeln der DS-GVO und die deutschen bereichsspezifischen Regelungen, etwa §§ 19–21 GenDG, entfallen.

Fraglich ist dabei u. a., wie es sich mit dem Telekommunikationsrecht verhält. Auch für den Beschäftigtendatenschutz ist das relevant, da bislang für die rechtliche Datenschutzbeurteilung, etwa von E-Mail-Kontrollen durch den Arbeitgeber das TMG und das TKG herangezogen wurden. Gemäß Art. 95 DS-GVO soll die Richtlinie für elektronische Kommunikation 2002/58/EG,[140] anders als die Datenschutzrichtlinie von 1995, die gemäß Art. 94 DS-GVO aufgehoben wird, in Kraft bleiben. Was das genau für TMK und TKG bedeutet, ist nicht ganz klar. Z. T. werden TMG sowie TKG weitgehend als die deutsche Umsetzung der Richtlinie über elektronische Kommunikation gesehen, mit der Folge, dass TMG und TKG weiter anwendbar blieben.[141] Für den Beschäftigtendatenschutz würde das bedeuten, dass weiterhin unklar wäre, wie der Arbeitgeber unter dem Gesichtspunkt der Telekommunikation zu behandeln ist. Die DS-GVO enthält dazu nichts. Schon deshalb ist eine spezialgesetzliche Regelung auf der Basis von Art. 88 Abs. 1 DS-GVO erforderlich,[142] denn die Telekommunikationsgesetze richten sich an Telemedienanbieter und sind nicht für das Beschäftigungsverhältnis gedacht. Nur weil eine passgenaue Regelung in Gestalt eines Beschäftigtendatenschutzgesetzes immer wieder verschoben wurde, mussten sie bislang für die Telekommunikationsvorgänge im Beschäftigungsverhältnis als analoge Notlösung herangezogen werden. Allerdings ist ohnehin fraglich, ob die Ansicht,

---

139 Zu einigen der Regelungsvorbehalte siehe *Dammann*, ZD 2016, 307, 310.

140 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. 7. 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. Nr. L 201 S. 37.

141 So *Kort*, NZA 2016 (erscheint demnächst), I.3.a).

142 Dazu genauer unten E.III.3.a).

wonach TMG und TKG als Umsetzung der Richtlinie über elektronische Kommunikation weitergelten können, haltbar ist. Hinsichtlich des TMG ist das wohl auszuschließen, denn bei seiner Verabschiedung hat der deutsche Gesetzgeber an keiner Stelle erkennen lassen, dass damit die Kommunikationsrichtlinie umgesetzt werden soll.[143] Also könnte das Datenschutzrecht des TMG (§§ 11 ff.) in Zukunft nicht mehr anwendbar sein. Anders verhält es sich beim TKG, das ausdrücklich zur Umsetzung mehrerer EU-Richtlinien dient, u. a. auch der Richtlinie 2002/58/EG und das daher wegen Art. 95 DS-GVO neben der Grundverordnung weitergelten kann, soweit es tatsächlich nur die Richtlinie umsetzt.[144] Für den Beschäftigtendatenschutz bedeutet das, dass der bislang das Fernmeldegeheimnis schützende § 88 TKG auch weiterhin entsprechend im Beschäftigungsverhältnis für die Privatnutzung von Arbeitgeber-Telekommunikationseinrichtungen herangezogen werden könnte. Ob das sinnvoll ist oder eine eigene, passendere Regelung erlassen werden sollte, ist eine andere Frage.[145]

143 *Keppeler*, MMR 2015, 779, 781; BT-Drs. 16/3078, S. 15 f.

144 Das ist z. B. bei § 94 TKG über die Einwilligung im elektronischen Verfahren nicht der Fall, da die Richtlinie eine solche Einwilligung nicht vorsieht. Hier werden in Zukunft dann nur noch die Einwilligungsregelungen der DS-GVO gelten, was aber für das Beschäftigungsverhältnis nicht relevant ist.

145 Dazu genauer unten E.III.

E. Beschäftigtendatenschutz

I. Status quo in Deutschland

Beschäftigtendatenschutz ist seit 25 Jahren ein rechtswissenschaftliches Thema,[146] aber erst der rechtswidrige Umgang mit personenbezogenen Beschäftigtendaten bei mehreren deutschen Großunternehmen im Jahr 2008 hat die öffentliche Wahrnehmung geschärft und den Gesetzgeber auf den Plan gerufen. Bis dahin wurde die allgemein für Verträge gedachte Ermächtigungsgrundlage in § 28 Abs. 1 Nr. 1 BDSG auch für die Erhebung, Speicherung und Übermittlung personenbezogener Daten im Rahmen des Arbeitsverhältnisses herangezogen. 2009 wurde dann § 32 in das BDSG aufgenommen, der Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses erlaubt. Die Erhebung und Verarbeitung von personenbezogenen Beschäftigtendaten muss für das Beschäftigungsverhältnis erforderlich sein. Gleichzeitig wurde der Beschäftigtenbegriff in § 3 Abs. 11 BDSG weiter formuliert als im Sozialversicherungs- oder Gleichstellungsrecht und umfasst auch die Bewerbungsphase sowie ehemalige Beschäftigte. § 32 Abs. 2 BDSG stellt auch für das Beschäftigungsverhältnis klar, dass analoge personenbezogene Daten geschützt sind, etwa solche in Papier-Personalakten. Darüber hinaus regelt § 32 BDSG nichts Neues. Der Gesetzgeber hatte das auch gar nicht vor, sondern wollte nur den bis dahin für Beschäftigungsverhältnisse geltenden § 28 Abs. 1 Nr. 1 BDSG konkretisieren und die Rechtsprechungsgrundsätze dazu zusammenfassen.[147] So ist auch § 32 Abs. 1 Satz 2 BDSG zu verstehen, der neben der Generalklausel in Satz 1 den Sonderfall der Erhebung und Verarbeitung personenbezogener Daten zur Aufdeckung von Straftaten dahingehend regelt, dass tatsächliche Anhaltspunkte für einen konkreten Verdacht vorliegen müssen. Für besonders sensible Beschäftigtendaten muss doch wieder auf § 28 BDSG zurückgegriffen werden und zwar auf die Einschränkung in § 28 Abs. 6 i. V. m. § 3 Abs. 9 BDSG.

Im Übrigen blieb es seit 2009 beim allgemeinen § 32 BDSG und der punktuellen Rechtsprechung dazu.[148] Die ist meist noch nicht einmal primär datenschutzrechtlich ausgerichtet. Vielmehr ergeben sich die Datenschutzfragen als Annex

---

146 Vgl. nur *Däubler*, Gläserne Belegschaften, seit 1990, zuletzt 2015, 6. Aufl.
147 BT Drs. 16/13657, S. 35.
148 Zu den bisher entschiedenen Einzelfällen vgl. *Taeger*/*Rose*, BB 2016, 819, 824 ff.

zu anderen arbeitsrechtlichen Aufhängern, etwa wenn das BAG feststellt, dass es sich beim Fragerecht des Arbeitgebers auch um eine datenschutzrechtliche Materie handelt,[149] oder klarstellt, dass Beweismittel, die unter Verstoß gegen Datenschutzregeln erhoben wurden, im Kündigungsschutzprozess nicht verwertet werden dürfen.[150] Darüber hinaus behilft man sich für den Beschäftigtendatenschutz mit Analogien zu Normen, die ein ganz anderes Regelungsziel haben, auf die man aber in Ermangelung konkreter Normen bei der Nutzung von Telekommunikationseinrichtungen im Beschäftigungsverhältnis zurückgreift. Hier geht es zum einen um das Telekommunikationsgeheimnis in §§ 88 ff. TKG sowie um die Datenschutzregeln in §§ 11 ff. TMG, die alle als Rechtsgrundlagen herangezogen werden, wenn Beschäftigte Internet- und Telefonanschluss des Arbeitgebers privat nutzen dürfen.[151]

Beschäftigtendatenschutz ist also in Deutschland derzeit keineswegs in der nötigen Tiefe geregelt, weshalb die Forderung nach einem eigenen Beschäftigtendatenschutzgesetz auch nie verstummt ist.[152]

II. Datenschutz-Grundverordnung (DS-GVO)

1. Rechtslage ohne Regelung des deutschen Gesetzgebers

In keiner der Entwurfsversionen zur DS-GVO ist der Beschäftigtendatenschutz konkret geregelt. Das Europäische Parlament hatte das zwar vorgeschlagen, sich aber nicht durchsetzen können. Eine inhaltlich konkrete Bereichsausnahme für das Arbeitsrecht enthält allerdings auch das derzeitige BDSG nicht und einen einzigen Paragraphen dazu erst seit wenigen Jahren. 2009 wurde eilig und als Notlösung der weitgehend inhaltsleere § 32 BDSG eingefügt, der insoweit auch als rein „symbolische Gesetzgebung" bezeichnet wurde.[153]

Wenn der deutsche Gesetzgeber den Beschäftigtendatenschutz nicht spezifischer regelt als die DS-GVO, gelten nicht § 32 BDSG und die Rechtsprechung dazu weiter, sondern die unmittelbar anwendbaren Regelungen der Verordnung. Die Rechtslage wäre dann in etwa mit der vor der Einfügung von § 32 BDSG vergleichbar als die Verarbeitung personenbezogener Beschäftigtendaten vor allem auf § 28 BDSG gestützt wurde. Nach der DS-GVO würden jedenfalls das Verbot mit Erlaubnisvorbehalt (Art. 6 Abs. 1) und der Zweckbindungsgrundsatz (Art. 5

149 BAG 15. 11. 2012, NZA 2013, 429.
150 BAG 20. 6. 2013, BB 2014, 179.
151 *Däubler*, Gläserne Belegschaften, 2015, 6. Aufl., Rn. 336 ff.; 342 ff.
152 Dazu genauer unten E.III.3.b).
153 *Thüsing*, NZA 2009, 865, 870.

Abs. 1 lit. b) gelten. Analoge Daten würden nicht dem Schutz der DS-GVO unterfallen und die Regelung in § 32 Abs. 1 Satz 2 BDSG über die Einschränkung der Datenerhebung zur Aufdeckung von Straftaten durch den Arbeitgeber ebenso wenig. Die Rechtsprechung der Arbeitsgerichte zu § 32 BDSG ließe sich allenfalls insoweit auf die Auslegung der DS-GVO-Normen übertragen als sie den Grundsätzen der europarechtskonformen Auslegung nationaler Regelungen durch nationale Gerichte entsprechen würde,[154] was jeweils im Einzelfall zu prüfen wäre. Die Weitergeltung von TMG und TKG, die z. T. auf einer EU-Richtlinie basieren, wird uneinheitlich bewertet,[155] so dass die Rechtsprechung, wonach die Telekommunikationsgesetze in bestimmten Fällen auch auf Arbeitgeber in Bezug auf ihre Beschäftigten herangezogen werden können, jedenfalls was das TMG angeht, nicht haltbar sein dürfte.

Auch ohne gesetzliche Regelung des Beschäftigtendatenschutzes durch den deutschen Gesetzgeber wären allerdings Datenschutzregeln durch Betriebsvereinbarungen möglich, da Art. 88 Abs. 1 nationale Rechtsvorschriften oder Kollektivvereinbarungen als Alternative formuliert und nicht vom Erlass nationaler gesetzlicher Beschäftigtendatenschutzregeln abhängig macht. Die Betriebsvereinbarungen müssten dann nicht einmal nach Art. 88 Abs. 3 DS-GVO der Kommission gemeldet werden.[156]

2. Art. 88 DS-GVO

Die Verordnung soll aber nicht abschließend sein, wie die vielen Öffnungsklauseln belegen, allen voran der insbesondere auf deutsche Initiative zurückgehende Art. 88 DS-GVO im Kapitel IX über „besondere Verarbeitungssituationen", das eine Reihe von Bereichen herausgreift, in denen weiterhin nationaler Datenschutz möglich sein soll.

Die Entwürfe zur DS-GVO schwanken zwischen dem absoluten Vorrang der europäischen Regelung mit umfassenden Konkretisierungsrechten für die Kommission im Wege so genannter delegierter Rechtsakte und möglichst großzügiger Regelungsfreiheit für die Mitgliedstaaten. Diesen letzten Aspekt hat vor allem der Ratsentwurf vom Juni 2015 betont. In dessen Erwägungsgrund 35a schließt die DS-GVO „nicht Rechtsvorschriften der Mitgliedstaaten aus, in denen die

---

154 *Schulze/Zuleeg/Kadelbach*, Europarecht – Handbuch für die Rechtspraxis, 2015, 3. Aufl., § 15 Rn. 66 ff.; *von der Groeben/Schwarze/Hatje*, Europäisches Unionsrecht, 2015, 7. Aufl., Art. 4 EUV Rn. 116 ff.

155 *Kort*, NZA 2016 (erscheint im Okt.), I.3.a) geht von der Weitergeltung aus. *Keppeler*, MMR 2015, 779, 781, sieht das anders, da jedenfalls das TMG nicht die Richtlinie 2002/58/EG umsetze und daher die Ausnahme in Art. 95 DS-GVO nicht greife.

156 Zur Meldepflicht s. unten 2.e).

Umstände spezifischer Verarbeitungssituationen festgelegt werden, einschließlich einer genaueren Bestimmung der Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist. Das nationale Recht kann auch spezielle Verarbeitungsbedingungen für spezifische Sektoren und für die Verarbeitung spezieller Kategorien von Daten vorsehen".

Eine Bereichsausnahme für den Beschäftigtendatenschutz gehörte zu den umstrittensten Regelungen im Gesetzgebungsprozess. Bereits seit dem ersten Entwurf der Kommission von 2012 war sie in Art. 82 DS-GVO-E enthalten, allerdings flankiert von der Befugnis der Kommission, konkretisierende delegierte Rechtsakte auch für den Beschäftigtendatenschutz zu erlassen. In der schließlich verabschiedeten Datenschutz-Grundverordnung wird die grundsätzliche Konzeption eines Verbots der Verarbeitung personenbezogener Daten mit Erlaubnisvorbehalt (Art. 6 DS-GVO) sowie die Möglichkeit, die Datenverarbeitung aufgrund einer Einwilligung nach Art. 7 DS-GVO und Erwägungsgrund Nr. 34 zu rechtfertigen, beibehalten. Für den Beschäftigtendatenschutz bedeutet das, dass es Erlaubnisnormen für die Erhebung, Speicherung und Verarbeitung von Beschäftigtendaten geben muss und es stellt sich darüber hinaus die Frage, inwieweit in diesem Bereich eine Einwilligung die Verarbeitung legitimieren kann.

a) Beschäftigtenbegriff

Wie häufig bei internationalen Dokumenten gibt auch die DS-GVO im Rahmen des Beschäftigtendatenschutzes Anlass zu sprachlichen und damit zu inhaltlichen Abgrenzungsproblemen. Es geht um die vermeintliche Kollision zwischen dem deutschen weiten datenschutzrechtlichen Beschäftigtenbegriff, wie er sich aus § 3 Abs. 11 BDSG ergibt und dem anscheinend engeren arbeitsrechtlichen Beschäftigtenbegriff in Art. 88 der DS-GVO. Das Problem trat besonders deutlich in der deutschen Version der Ratsfassung der DS-GVO vom Juni 2015 zu Tage, wo in Art. 82 (jetzt Art. 88) von „Arbeitnehmerdaten" die Rede war. In Art. 88 der verabschiedeten Fassung sind daraus zwar „Beschäftigtendaten" geworden, aber die Regelbeispiele im weiteren Text des Art. 88 Abs. 1 scheinen eher auf den deutschen klassischen (engen) Arbeitnehmerbegriff zu deuten. Der Blick auf die englische Version „employee" hilft nicht weiter, da zum einen der „employee" in allen Versionen seit 2012 verwendet wird – zu einem Bedeutungswandel der gemeinten Schutzgruppen im Laufe des Gesetzgebungsprozesses also nicht nur nichts aussagt, sondern gegen einen solchen spricht – und zum anderen der englische Employee-Begriff zwar weiter ist als der deutsche Arbeitnehmerbegriff,[157]

---

157 Zum englischen Begriff des „employee" vgl. *Harth/Taggert*, in: Henssler/Braun, Arbeitsrecht in Europa, Köln 2011, Arbeitsrecht in Großbritannien, Rn. 6 ff.

aber auch nicht deckungsgleich mit dem sehr weiten Beschäftigtenbegriff, wie er in § 3 Nr. 11 BDSG gemeint ist, der 2009 ins BDSG eingefügt wurde und erstmals den datenschutzrechtlichen Beschäftigtenbegriff regelt.

Da es sich bei der DS-GVO um EU-Gesetzgebung handelt, ist eine europäische Perspektive zugrunde zu legen. Einen einheitlichen autonomen europäischen Arbeitnehmerbegriff gibt es zwar noch nicht. Man kann aber auf den vom EuGH anhand von Art. 45 AEUV entwickelten Arbeitnehmerbegriff abstellen, der jedenfalls weiter geht als das deutsche Verständnis und etwa auch Beamte umfasst.[158] Der EuGH legt den Arbeitnehmer-/Beschäftigtenbegriff grundsätzlich weit aus und orientiert sich dabei zunehmend für alle Arbeitnehmerbegriffe im europäischen Arbeitsrecht am schon lange weit verstandenen Arbeitnehmerbegriff der Arbeitnehmerfreizügigkeit in Art. 45 AEUV.[159] Dabei betont der EuGH, dass der (weite) Arbeitnehmer-/Beschäftigtenbegriff in Art. 45 AEUV auch für Arbeitnehmerbegriffe in Rechtsakten nach Art. 288 AEUV gelten soll,[160] sofern in den Rechtsakten nicht auf den Arbeitnehmerbegriff des nationalen Rechts verwiesen wird. Folglich ist auch der Beschäftigtenbegriff in Art. 88 DS-GVO weit zu verstehen, so dass eine § 3 Abs. 11 BDSG entsprechende nationale Regelung aufgrund der Öffnungsklausel in Art. 88 DS-GVO möglich wäre.

b) „Spezifischere“ (nationale) Regelungen

Im Regelungsbereich einer Verordnung dürfen die Mitgliedstaaten konkretisierendes oder ausfüllendes Recht im Prinzip nur erlassen, wenn die Verordnung das vorsieht.[161] Allerdings weist Art. 291 Abs. 1 AEUV darauf hin, dass eine Verordnung auch ohne eine solche ausdrückliche Befugnis implizit voraussetzen kann, dass die Mitgliedstaaten Durchführungsregeln erlassen, um den Verordnungsinhalt überhaupt handhabbar zu machen.[162] In der DS-GVO liegt aber mit den „spezifischeren“ Regelungen für die Beschäftigtendaten eine ausdrückliche Öffnungsklausel vor, die es zu interpretieren gilt. Geht es nur um eine Konkretisierung der DS-GVO oder sollen eigenständige nationale Regelungen erlaubt sein? Bei diesen wäre dann zu klären, ob und inwieweit sie nach unten bzw. nach oben vom Niveau der DS-GVO abweichen dürften.

---

158 EuGH, Urt. v. 3. 5. 2012 – C-337/10, NVwZ 2012, 688 (Neidel).

159 *Steinmeyer*, in: Franzen/Gallner/Oetker, Kommentar zum europäischen Arbeitsrecht, 2016, Art. 45 AEUV Rn. 10 ff.

160 EuGH, Urt. v. 7. 4. 2011 – C-519/09 (May), Slg. 2011, I-2761, Rn. 22; vgl. zu den Arbeitnehmerbegriffen auch *Klebe*, AuR 2016, 277.

161 *Oppermann/Classon/Nettesheim*, Europarecht, München 2016, 7. Aufl., § 9 Rn. 80.

162 *Grabitz/Hilf/Nettersheim*, Das Recht der Europäischen Union, Loseblatt, 58. EL, Stand: Januar 2016, Rn. 101.

Die Öffnungsklausel für den Beschäftigtendatenschutz in Art. 88 DS-GVO spielt in der Liste der DS-GVO-Öffnungen auch für andere nationale Datenschutzregeln eine Sonderrolle. Erst in der Ratsversion der DS-GVO vom Juni 2015 wurden entgegen der Vorstellungen der Kommission die doch bei den Mitgliedstaaten verbleibenden Datenschutzbefugnisse deutlich ausgeweitet.[163] Der Beschäftigtendatenschutz war allerdings selbst von der Kommission, die an möglichst wenigen bei den Mitgliedstaaten verbleibenden Datenschutzbefugnissen interessiert war, bereits in Art. 82 des DS-GVO-Entwurfs vom 25. 1. 2012 für nationale Regelungen geöffnet worden. Jedoch hieß es dort noch, wohl auch vor dem Hintergrund von Art. 1 Abs. 3 DS-GVO, wonach der freie Verkehr personenbezogener Daten in der Union nicht eingeschränkt werden darf, die Mitgliedstaaten können (nur) „in den Grenzen dieser Verordnung" Beschäftigtendatenschutz regeln. Das war eine Einschränkung der nationalen Regelungsbefugnis, zumal Abs. 3 des Art. 82 in der Kommissionsfassung von 2012 auch noch vorsah, dass die Kommission durch delegierte Rechtsakte genauere Regelungen für den Beschäftigtendatenschutz festlegen sollte. In dieser ersten Konzeption der DS-GVO hätte wohl die nationale Regelungsbefugnis für den Beschäftigtendatenschutz bedeutet, dass nur auf dem Niveau der Verordnung („im Rahmen der Verordnung") Konkretisierungen derselben national hätten geregelt werden dürfen, sofern nicht die Kommission selbst delegierte Rechtsakte erlassen hätte, etwa für bestimmte Datenverarbeitungsformen im Beschäftigungsverhältnis. Wie der „Rahmen der Verordnung" angesichts vorwiegend unbestimmter Rechtsbegriffe im Einzelnen hätte ausgelotet werden können, kann jetzt für den Beschäftigtendatenschutz offen bleiben, da sich der Rat für ein anderes, die Kompetenzen der Mitgliedstaaten beim Beschäftigtendatenschutz betonendes Konzept entschieden hat, das in der schließlich verabschiedeten Version beibehalten wurde.

Dort erlaubt Art. 88 Abs. 1 den Mitgliedstaaten nun, „spezifischere Vorschriften" für Beschäftigtendaten vorzusehen, ohne die Einschränkung, dass sich diese „in den Grenzen der Verordnung" halten müssen. Auch andere Öffnungsklauseln der DS-GVO sehen diese Einschränkung nicht mehr vor.[164] Lediglich in einigen Erwägungsgründen, die aber nicht den Beschäftigtendatenschutz betreffen, wird die einschränkende Formulierung noch benutzt.[165] Nach der beispielhaften, aber nicht abschließenden Aufzählung in Art. 88 Abs. 1 DS-GVO[166] können nationale Regelungen erlassen werden, u. a. für „Zwecke der Einstellung, der Erfüllung des

---

163 Vgl. u. a. Art. 1 Abs. 2a DS-GVO-Ratsversion (jetzt Art. 6 Abs. 2 DS-GVO).

164 Z. B. Art. 85 Abs. 1, Art. 86 oder Art. 80 Abs. 2 DS-GVO.

165 Etwa Erwägungsgrund 98, 149, 162 oder 164.

166 So auch, wenn auch etwas widerwillig *Schüßler/Zöll*, DuD 2013, 639, 640 noch zu Art. 82 DS-GVO-E.

Arbeitsvertrages, einschließlich der Erfüllung von gesetzlich oder kollektivrechtlich festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses".

Diese lange Aufzählung umfasst – zumal sie nicht abschließend ist („insbesondere") – jedenfalls die derzeit in Deutschland geltenden Datenschutzregeln für Beschäftigte und erlaubt daher weiterhin deren nationale Regelung.

Allerdings enthält Art. 88 Abs. 1 DS-GVO nicht nur eine Öffnung für nationale Datenschutzregeln zugunsten der Beschäftigten, sondern auch für Kontrollbefugnisse der Unternehmen, denn die Mitgliedstaaten können Regelungen zum „Schutz der Rechte", aber auch zum Schutz der „Freiheiten" (der Datenverarbeiter) treffen. Letzteres ergibt sich auch aus der exemplarischen Aufzählung von typischen Datenverarbeitungssituationen im Beschäftigungskontext. Nicht nur Datenverarbeitung bei der Einstellung, für die Erfüllung des Arbeitsvertrages oder die Beendigung des Arbeitsverhältnisses sind erwähnt, sondern auch Pflichten des Managements, Planung und Organisation der Arbeit oder Schutz des Eigentums des Arbeitgebers und der Kunden, Konstellationen also, bei denen es typischerweise um Kontrolle der Beschäftigten geht. Darin spiegelt sich das in Art. 1 Abs. 3 DS-GVO niedergelegte Konzept, wonach nicht nur der Persönlichkeitsschutz der Betroffenen, sondern auch der freie Verkehr personenbezogener Daten in der Union durch die DS-GVO gewährleistet werden soll.

c) Verordnungsrahmen

Ganz allgemein wird man sagen können, dass „spezifischer" i. S. der Verordnung jedenfalls Regelungen meint, die über die Grundsätze und die allgemeinen Vorschriften der DS-GVO für Bürger/Verbraucher hinausgehen und typischerweise den Beschäftigungskontext betreffen.[167] Dabei ergibt sich aber aus der Konzeption, Entstehungsgeschichte und Sinn und Zweck der Verordnung, dass die DS-GVO jedenfalls als Mindeststandard gemeint ist und also die allgemeinen Datenschutzregeln der Verordnung nicht unterschritten werden dürfen. Dieser Grundsatz ist allerdings leichter festgestellt als umgesetzt, da weite Teile der DS-GVO generalklauselartig formuliert sind. Ein völliges Verbot von Datenverarbeitung

[167] In diesem Sinne u. a. auch *Düwell/Brink*, NZA 2016, 665, 666.

im Beschäftigungsverhältnis wäre jedenfalls nicht von Art. 88 Abs. 1 DS-GVO gedeckt. Darüber hinaus würde darin auch ein Verstoß gegen Art. 1 Abs. 3 DS-GVO liegen.

Ein Höchststandard wird in der verabschiedeten DS-GVO nicht mehr postuliert. Selbst in der ursprünglichen Kommissionsformulierung in Art. 82 Abs. 1 – „in den Grenzen der Verordnung" – wurde z. T. keine Regelungsbegrenzung für den nationalen Gesetzgeber gesehen.[168] Zwar gilt allgemein, dass bei einer Verordnung mit Öffnungsklauseln, die in der europarechtlichen Terminologie auch „hinkende Verordnung" genannt wird,[169] die Öffnungsklausel eng auszulegen ist,[170] um dem Harmonisierungsziel der Verordnung gerecht zu werden. Dabei kommt es aber auf die konkrete Formulierung der Öffnungsklausel an. In der Genese des Art. 82 von der Kommissionsfassung bis zur verabschiedeten Version in Art. 88, hat es noch weitere Formulierungsvorschläge gegeben. Dem Berichterstatter des Europäischen Parlaments war die Kommissionsformulierung zu eng. Er wollte nationale Regelungen „nach oben" zulassen und formulierte, die nationalen Datenschutznormen sollten „in Übereinstimmung mit den Bestimmungen der Verordnung" sein und ergänzte in den Erwägungsgründen, das nationale Datenschutzrecht, das aufgrund der Öffnung erlassen würde, solle „im Einklang" mit der Verordnung stehen.[171] Im verabschiedeten Art. 88 Abs. 1 DS-GVO sind nun „spezifischere Vorschriften" sogar ohne jede Einschränkung durch die Verordnung selbst erlaubt. Auch Art. 1 Abs. 3 DS-GVO führt eine solche Beschränkung nicht herbei, da die Genese von Art. 82 bzw. 88 zeigt, dass eine solche, ursprünglich vorgesehene Einschränkung, gerade nicht beibehalten werden sollte.

Wenn also auch die enge Öffnungsklausel der Kommissionsfassung von 2012 im weiteren Gesetzgebungsprozess verworfen wurde, so müssen doch die Grundprinzipien der Grundverordnung aus Art. 5, allen voran der Zweckbindungsgrundsatz (Art. 5 Abs. 1 lit. b) auch beim nationalen Beschäftigungsdatenschutz beachtet werden. Außerdem enthält der verabschiedete Art. 88 Abs. 2 DS-GVO

---

168 *Hirsch* (MdEP), Stellungnahme vom 4. 3. 2013 zum Kommissionsentwurf, C7-0025/2012 – 2012/0011 (COD).

169 *Ruffert*, in: Callies/Ruffert, EUV/AEUV, 2016, 5. Aufl., Art. 288 AEUV Rn. 21.

170 Vgl. etwa EuGH, Urt. v. 15. 12. 1976 – C-41/76, NJW 1977, 1007; BGH, NJOZ 2010, 1274, 1282; *Schüßler/Zöll,* DuD 2013, 639, 640.

171 Erwägungsgrund 124 im Entwurf eines Berichts über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 16. 1. 2013, vorgelegt vom Berichterstatter im zuständigen Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments, 2012/0011 (COD) (Berichtsentwurf).

einen Rahmen für die Wahrung von Schutzgütern, der von nationaler Gesetzgebung zum Beschäftigtendatenschutz eingehalten werden muss. Art. 88 Abs. 2 stellt inhaltliche Voraussetzungen auf, die die nationalen Regeln zum Beschäftigtendatenschutz – seien es Gesetze oder Kollektivverträge – erfüllen müssen. Nach Art. 88 Abs. 2 müssen die spezifischeren nationalen Vorschriften Maßnahmen zur Wahrung der Menschenwürde, der Grundrechte und der berechtigten Interessen der betroffenen Personen wahren, vor allem im Hinblick auf die Transparenz der Datenverarbeitung, der Übermittlung von personenbezogenen Daten innerhalb eines Konzerns und bei Überwachungssystemen am Arbeitsplatz, fast alles Grundsätze, die ohnehin schon nach nationalem Verfassungsrecht eingehalten werden müssen.[172]

Zu diesen Mindestanforderungen an nationale Beschäftigtendatenschutzregeln gehören jedenfalls Art. 8 GR-Charta, also das europäische Datenschutzgrundrecht, sowie die seit den 1950er Jahren erarbeiteten Grundsätze zum Allgemeinen Persönlichkeitsrecht – in den 1980er Jahren vom BVerfG zum informationellen Selbstbestimmungsrecht weiterentwickelt. Das BAG hat bei der Auslegung des Beschäftigtendatenschutzes i. d. R. auch auf das Allgemeine Persönlichkeitsrecht von Beschäftigten und Bewerbern rekurriert.[173] Dabei wird es auch unter der DS-GVO bleiben, ohne dass die deutschen zivilrechtlichen Normen, die für das Allgemeine Persönlichkeitsrecht herangezogen werden (§§ 823, 1004 BGB) meldepflichtig i. S. v. Art. 88 Abs. 3 DS-GVO[174] wären.[175]

Es fällt auf, dass anders als bei Art. 1 Abs. 3 DS-GVO, der Persönlichkeitsschutz und Informationsfreiheit gleichgewichtig nebeneinander stellt, in Art. 88 Abs. 2 betont wird, dass mit nationalen Regeln zum Beschäftigtendatenschutz „die Grundrechte der betroffenen Person" geschützt werden müssen. Eine Abwägung etwa mit der unternehmerischen Freiheit in Art. 16 GR-Charta wird in Art. 88 Abs. 2 DS-GVO nicht gefordert.

Daher erlaubt Art. 88 DS-GVO keine Abweichungen „nach unten".[176] „Nach oben" dagegen sollen Abweichungen zulässig sein. Das ergibt sich auch aus dem Vergleich zu anderen Artikeln in der DS-GVO, die nationale „spezifischere Anforderungen" erlauben. Vor allem sollte mit diesen anderen Artikeln ermöglicht werden, das umfangreiche Datenschutzrecht der Mitgliedstaaten im öffentlichen

---

172 So auch *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016, 298.
173 Vgl. nur *Venetis/Oberwetter*, NZA 2016, 1051, oder *Klein/Roos*, ZD 2016, 65.
174 Zur Meldepflicht s. unten E.II.e).
175 So auch *Kort*, NZA 2016 (erscheint demnächst), I.9. m. w. N.
176 So auch *Wybitul*, BB Die erste Seite 2016, Nr. 02; *Gola/Pötters/Thüsing*, RDV 2016, 57, 59.

Bereich aufrecht zu erhalten und fortzuentwickeln.[177] Für denselben Begriff („spezifischere Anforderungen") in Art. 88 Abs. 1 DS-GVO gilt das daher ebenso. Auch der Berichterstatter der DS-GVO im Europäischen Parlament sieht in Art. 88 Abs. 1 eine Öffnung für „Spezialdatenschutz und Raum für mitgliedstaatliche Sonderwege".[178] Er hält es darüber hinaus für denkbar, dass der EU-Gesetzgeber zum Beschäftigtendatenschutz auch noch eine Richtlinie erlässt, um eine Mindestharmonisierung auf diesem Feld zu erreichen.

Für § 32 Abs. 2 BDSG würde diese Auslegung bedeuten, dass der Inhalt dieser Norm weiter fortbestehen kann, wonach nicht nur automatisierte, sondern auch analoge Verarbeitung geschützt ist,[179] anders als in der DS-GVO, wo nur Verarbeitung in Dateien gemeint ist. Wird § 32 BDSG allerdings nicht beibehalten oder werden in einem nationalen Beschäftigtendatenschutzgesetz die analogen Daten nicht umfasst, bliebe es bei der Regelung der Verordnung und analoge personenbezogene Daten unterfielen nicht dem Datenschutz.

d) Sonderstellung sensibler Daten in Art. 9 DS-GVO

Die bisherigen Merkmale des § 3 Abs. 9 BDSG sind nun in Art. 9 DS-GVO abgebildet. Art. 9 Abs. 1 DS-GVO verbietet die Verarbeitung besonderer Kategorien personenbezogener Daten, die die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit offenbaren sowie die Verarbeitung von genetischen, biometrischen und Gesundheitsdaten und Daten, die Aufschluss über die sexuelle Orientierung geben können. Abs. 2 allerdings sieht zehn Erlaubnistatbestände für die Verarbeitung dieser Kategorien von personenbezogenen Daten vor, wenn auch insgesamt unter der DS-GVO strengere Regelungen gelten als in §§ 4a, 28 Abs. 6–9 BDSG. Für den arbeitsrechtlichen Zusammenhang ist vor allem Art. 9 Abs. 2 lit. b DS-GVO i. V. m. mit Erwägungsgrund 52 von Bedeutung, wonach vom Verarbeitungsverbot abgewichen werden darf, wenn die Verarbeitung erforderlich ist, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit erwachsenden Rechte ausüben kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist, etwa für die Übermittlung von Beschäftigtendaten an Sozialversicherungsträger. Derartige Sonderregelungen dürfen die Mitgliedstaaten also treffen. Diese nationalen Regeln müssen dann aber gemäß Art. 9 Abs. 2

177 *Buchner*, DuD 2016, 155, 159, Anm. 31; *Will*, ZD 2015, 345; s. auch BR-Drs. 290/15, S. 2.
178 *Albrecht*, CR 2016, 88, 97.
179 *Taeger/Rose*, BB 2016, 819, 823; *Gola/Pötters/Thüsing*, RDV 2016, 57, 60.

lit. b DS-GVO geeignete Garantien zum Schutz personenbezogener Daten und anderer Grundrechte der betroffenen Personen enthalten.

Einerseits können also die Mitgliedstaaten die Verarbeitung besonderer, also der genannten sensiblen Daten zulassen. Andererseits sieht Art. 9 Abs. 4 aber auch vor, dass die Mitgliedstaaten grundsätzlich, also nicht nur wie in Art. 9 Abs. 2 lit. b im arbeits- und sozialrechtlichen Zusammenhang, bei genetischen, biometrischen oder Gesundheitsdaten zusätzliche Verarbeitungsbedingungen bzw. Beschränkungen einführen dürfen. Da das in Bezug auf diese drei Arten von sensiblen Daten für alle Verarbeitungszusammenhänge gilt, sind entsprechende Einschränkungen gerade auch im Beschäftigungsverhältnis möglich, für das die Mitgliedstaaten darüber hinaus ohnehin in Art. 88 DS-GVO eine Öffnungsklausel vorfinden. Eine einschränkende nationale Regelung für die Erhebung und Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten bietet sich vor allem für die Einwilligung des Beschäftigten in die Verarbeitung derartiger Daten an.[180]

Umgekehrt gilt, dass wenn die Mitgliedstaaten von Art. 88 Abs. 1 Gebrauch machen und Beschäftigtendatenschutz national regeln, Art. 9 DS-GVO eingehalten werden muss, wenn die dort genannten sensiblen Daten betroffen sind. Das ergibt sich auch aus der systematischen Stellung der beiden Normen. Art. 9 gehört zum Kapitel II der DS-GVO, in dem die Grundsätze der Verordnung geregelt sind. Grundsätze müssen auch dann eingehalten werden, wenn Öffnungsklauseln nationale „spezifischere" Regeln erlauben. Art. 88 findet sich ganz am Ende der Verordnung in Kapitel IX über besondere Verarbeitungsformen.

e) Bedeutung der Meldepflicht in Art. 88 Abs. 3 DS-GVO

Art. 88 Abs. 3 DS-GVO sieht für die nationalen Regelungen zum Beschäftigtendatenschutz eine Meldepflicht vor. Innerhalb von zwei Jahren ab Erlass der DS-GVO, also bis zum 25. 5. 2018 teilt der Mitgliedstaat die nationalen Regeln der Kommission mit, unverzüglich alle späteren Änderungen dieser Vorschriften. Die Bedeutung der Vorschrift ist nicht ganz klar. Es dürfte sich dabei um eine Mitteilungspflicht handeln. Im Englischen heißt es „each Member State shall notify to the Commission". Wenn auch das englische „shall" in manchen Zusammenhängen für „sollen" steht, bedeutet es in Rechtstexten i. d. R. „müssen". Im Deutschen entspricht dem der Indikativ, der in der deutschen Version der DS-GVO auch gewählt wurde. Ein Indikativ steht allerdings auch in § 1 BetrVG und

[180] Zur Einwilligung s. unten in einem eigenen Kapitel E.III.4.

wird trotzdem als „können/dürfen“ gelesen. Auf deutsche Interpretationsgepflogenheiten kommt es allerdings bei einem EU-Rechtstext nicht an. Es ist also von einer Meldepflicht auszugehen.

Die Bedeutung und Wirkung der Meldepflicht bzw. die Rechtsfolgen bei Nichtmeldung ergeben sich nicht aus dem Text des Art. 88 Abs. 3. Aus der Genese des Wortlauts lässt sich auch nichts ableiten, denn der ist seit dem Kommissionsentwurf von 2012 unverändert geblieben. Z. T. wird der Absatz als eine Art Ausschlussfrist verstanden,[181] nach deren Ablauf nur noch auf die ursprüngliche Meldung bezogene Änderungen, aber nichts mehr neu gemeldet werden dürfte. Die Mitgliedstaaten müssten also nationale Regelungen sehr rasch verabschieden, angesichts der kurzen Frist ggf. ohne sorgfältige Prüfung.

Dieser Aspekt, aber vor allem der Gesamtzusammenhang spricht eher dafür, dass die Norm zunächst eine Informationsfunktion haben soll.[182] Dafür spricht auch der Umstand, dass etliche andere Artikel in der DS-GVO gleichlautende Melderegelungen enthalten (z. B. Art. 84 Abs. 2, 85 Abs. 3, 90 Abs. 2). Die Kommission soll in einem überschaubaren Zeitrahmen erste nationale Regelungen auf die Einhaltung der Mindestvoraussetzungen der DS-GVO überprüfen können, aber auch darauf, ob der in der DS-GVO vorgegebene Rahmen wie etwa Art. 88 Abs. 2 oder Art. 9 Abs. 2 lit. b eingehalten wurde. Darüber hinaus sollen die Mitgliedstaaten aus Gründen der Rechtssicherheit angehalten werden, sich zügig zu entscheiden, von welchen Öffnungsklauseln sie Gebrauch machen wollen. Selbst wenn man in Art. 88 Abs. 3 dennoch eine Ausschlussfrist sehen wollte, würde zunächst eine vorläufige Regelung, z. B. ein mehr oder weniger modifizierter § 32 BDSG für die Meldung genügen, der später im Änderungsmodus auch noch durch ein umfassenderes Beschäftigtendatenschutzgesetz ersetzt werden könnte.[183]

Gegen eine Ausschlussfrist spricht darüber hinaus der Umstand, dass nur Rechtsvorschriften, die der Mitgliedstaat erlässt, nicht aber Kollektivverträge gemeldet werden müssen, die gemäß Art. 88 Abs. 1 DS-GVO ausdrücklich auch „spezifischere“ Regelungen zum Beschäftigtendatenschutz schaffen dürfen. Insofern ist

---

181 So *Gola/Pötters/Thüsing*, RDV 2016, 57, 58.

182 *Roßnagel* sieht in einer Stellungnahme für den Deutschen Bundestag gerade für den Beschäftigtendatenschutz, anders als für Bestimmungen in der DS-GVO, die eine nationale Ausfüllungspflicht begründen, „keinen vergleichbaren Zeitdruck“, Schriftliche Stellungnahme zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung am 24. 2. 2016 im Ausschuss Digitale Agenda des Deutschen Bundestages, S. 9.

183 Auch *Kort*, NZA 2016, (erscheint demnächst), I.8.d) sieht im Art. 88 Abs. 3 keine Selbstbindung, sondern hält die Mitgliedstaaten auch über den 2. 5. 2018 hinaus für befugt, ein Beschäftigtendatenschutzgesetz zu erlassen.

schon die Grundstruktur von Art. 88 Abs. 3 DS-GVO so ausgelegt, dass die Norm ihr Transparenzziel ohnehin nie vollständig erreichen kann. Die Formulierung als Ausschlussfrist zu verstehen, ist auch aus demokratietheoretischer Sicht fraglich. Man kann einem Gesetzgeber, der sich erst zu einem späteren Zeitpunkt zum Handeln entschließt – und sei es weil das Parlament gerade vor einer Wahl steht – sein Handeln nicht aufgrund einer „Ausschlussfrist" verweigern. Schließlich ist auch damit zu rechnen, dass der Europäische Gerichtshof die Regelung nicht überbewerten wird. Jedenfalls hat er bei der Leiharbeitsrichtlinie eine ähnliche Prüfpflicht im Hinblick auf nationale Einschränkungen der Leiharbeit im Ergebnis für belanglos gehalten.[184] Es dürfte also jedenfalls reichen, dass der Gesetzgeber bis zum Stichtag Regelungsvorbehalte kommuniziert und später – ggf. nach einer vorläufigen (modifizierten) Meldung von § 32 BDSG – detailliertere Regelungen zum Beschäftigtendatenschutz erlässt.

3. Betrieblicher Datenschutzbeauftragter

Der betriebliche Datenschutzbeauftragte war aus ganz unterschiedlichen Gründen bei den Mitgliedstaaten während der Ausarbeitung der DS-GVO sehr umstritten. Im deutschen BDSG geht die entsprechende Regelung weit, in anderen Mitgliedstaaten gab es bislang überhaupt keinen betrieblichen Datenschutzbeauftragten.

Bei der in der DS-GVO gefundenen Lösung ist das deutsche Beispiel aus §§ 4f und 4g BDSG deutlich zu erkennen,[185] wenn es auch in der Verordnung einige Abweichungen, insbesondere hinsichtlich des Anwendungsbereichs gibt. Darüber hinaus waren in den ersten Versionen der DS-GVO zunächst hohe Schwellenwerte für die Einsetzung eines betrieblichen Datenschutzbeauftragten angesetzt worden, die zwischen 250 und 5.000 mit Datenverarbeitung Beschäftigten reichten und damit erheblich über der Schwelle in § 4f Abs. 1 Satz 4 BDSG mit mehr als neun lagen. Art. 37 DS-GVO legt nun keine Schwelle mehr fest. Nach Art. 37 Abs. 1 DS-GVO müssen nur in drei Fällen betriebliche Datenschutzbeauftragte bestellt werden, zum einen bei Behörden und öffentlichen Einrichtungen (lit. a) und zum anderen bei Unternehmen, wenn die Kerntätigkeit des Unternehmens in der „umfangreichen, regelmäßigen und systematischen Überwachung von betroffenen Personen" (lit. b) oder der Verarbeitung sensitiver Daten i. S. v. Art. 9 besteht (lit. c). Was diesen Kern der Unternehmenstätigkeit ausmachen soll, erhellt auch der den betrieblichen Datenschutzbeauftragten betreffende Erwägungsgrund 97 nicht.

---

184 *Heuschmid*, Anmerkung zu EuGH, Urt. v. 17. 3. 2015 – C-533/13, HSI-Newsletter 1/2015, II.

185 *Klug*, ZD 2016, 315, 319; *Jaspers/Reif*, RDV 2016, 61.

Gemäß Art. 37 Abs. 4 DS-GVO dürfen die Mitgliedstaaten aber eigene Regelungen treffen, d. h. weitere Fälle vorsehen, in denen ein betrieblicher Datenschutzbeauftragter bestellt werden muss. Daher können §§ 4f und 4g BDSG oder eine vergleichbare Regelung in einem Nachfolgegesetz erhalten bleiben, wonach Privatunternehmen dann einen Datenschutzbeauftragten bestellen müssen, wenn sie mehr als neun Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.

Allerdings hat die DS-GVO zum Thema des betrieblichen Datenschutzbeauftragten einen anderen Zungenschlag als das BDSG. Letzteres trennt deutlich zwischen der Datenschutzkontrolle durch den betrieblichen Datenschutzbeauftragten und durch die Aufsichtsbehörden. In der Literatur wird z. T. betont, dass der betriebliche Datenschutzbeauftragte gerade kein „verlängerter Arm" der Aufsichtsbehörden sei,[186] da er sein Amt unabhängig wahrnehme. Aus diesem Blickwinkel wird dann das Verordnungsgebot einer Zusammenarbeit des betrieblichen Datenschutzbeauftragten mit den Aufsichtsbehörden gemäß Art. 39 Abs. 1 lit. d und e DS-GVO kritisch gesehen.[187] Diese neue Verpflichtung zur Zusammenarbeit mit der Aufsichtsbehörde ist jedoch für die Effizienz des Datenschutzes im Unternehmen eher von Vorteil, da auf diesem Wege auch fachliche Beratung des betrieblichen Datenschutzbeauftragten stattfindet, die, sofern sie sich im Rahmen der Aufgaben der Aufsichtsbehörde bewegt, für den Datenschutzbeauftragten kostenlos ist (Art. 57 Abs. 3 DS-GVO).

Die Zusammenarbeitspflicht kann ggf. auch ein anderes Problem des betrieblichen Datenschutzbeauftragten abmildern, die Wahrung seiner Unabhängigkeit. Wie bisher liegt hierin das größte Problem im Zusammenhang mit dem betrieblichen Datenschutzbeauftragten, da er – ob intern oder extern rekrutiert, beides ermöglicht die DS-GVO – vom Unternehmen bestellt wird. Im Kommissionsentwurf war die Unabhängigkeit des betrieblichen Datenschutzbeauftragten noch im Verordnungstext genannt worden (Art. 36 DS-GVO-E). In der verabschiedeten Fassung ist sie nur noch in Erwägungsgrund 97 erwähnt. Die Formulierung in Art. 38 Abs. 3 DS-GVO geht jedenfalls nicht über die bisherige deutsche Regelung hinaus – eine Weisungsunterworfenheit des betrieblichen Datenschutzbeauftragten besteht zwar ausdrücklich nicht, er bleibt aber auch nach europäischem Recht der Unternehmensleitung unterstellt. An der grundsätzlichen Ausrichtung des betrieblichen Datenschutzbeauftragten am Unternehmensinteresse[188] ändert sich auch durch die DS-GVO nichts. Sie enthält zudem keinen Kündigungsschutz, wie

---

186 *Kort*, NZA 2015, 1345; *ders.*, DB 2016, 711, 713.

187 *Bittner*, RDV 2014, 183, 188.

188 So *Kort* ganz selbstverständlich für die deutsche Situation in: NZA 2015, 1345.

er in § 4f Abs. 3 Satz 5 BDSG seit 2009 vorgeschrieben ist. Der könnte aber wegen der Öffnungsklausel in der DS-GVO in einer deutschen Regelung zum betrieblichen Datenschutzbeauftragten beibehalten werden.

Eine Erweiterung bzw. Einschränkung – je nach Sichtweise – enthält Art. 37 Abs. 2 DS-GVO, der erlaubt, einen einzigen Konzerndatenschutzbeauftragten einzusetzen, durch den sich dann Datenschutzbeauftragte für die einzelnen Unternehmen erübrigen.[189] Allerdings gibt es die Einschränkung, dass ein Konzerndatenschutzbeauftragter von jeder Niederlassung i. S. v. Art. 4 Nr. 16 DS-GVO aus leicht erreichbar sein muss.

Gleichzeitig werden in der DS-GVO Meldepflichten bei bestimmten Arten von Datenverarbeitung erweitert: die gibt es zwar auch schon nach § 4d i. V. m. § 4e BDSG. Nach der DS-GVO bestehen diese Pflichten aber unabhängig davon, ob überhaupt ein betrieblicher Datenschutzbeauftragter bestellt worden ist.[190]

Die Aufgabenstellung des betrieblichen Datenschutzbeauftragten verschiebt sich durch die DS-GVO. Gemäß Art. 39 Abs. 1 DS-GVO hat er Berichts-, Überwachungs-, Beratungs- und Kooperationsaufgaben, wobei bei der Überwachung der Einhaltung des Datenschutzes nach Art. 39 Abs. 1 lit. b dem betrieblichen Datenschutzbeauftragten verstärkt Compliance-Aufgaben zugeordnet werden, wohingegen Aufgaben wie Mitarbeiterschulung oder Vorabkontrolle entfallen.[191]

Das immer wieder problematische (Konkurrenz-)Verhältnis zwischen betrieblichem Datenschutzbeauftragten und Betriebsrat bei Fragen des Beschäftigtendatenschutzes wird auch in der DS-GVO keiner Lösung zugeführt. Das Europäische Parlament hatte die Probleme erkannt, aber sein Vorschlag, den betrieblichen Datenschutzbeauftragten zu verpflichten, den Betriebsrat über die Verarbeitung von Beschäftigtendaten zu unterrichten,[192] wurde im Trilog nicht aufgegriffen. Daher bleiben Fragen wie die, ob ein Betriebsrat gleichzeitig betrieblicher Datenschutzbeauftragter sein kann, offen. Hier gibt es nur einen Hinweis in Art. 38 Abs. 6 DS-GVO, wonach der Datenschutzbeauftragte auch andere Aufgaben und Pflichten wahrnehmen darf, sofern es nicht zu einem Interessenkonflikt kommt. Weiter stellt sich die Frage, ob und inwieweit der betriebliche Datenschutzbeauftragte die Verarbeitung personenbezogener Beschäftigtendaten überprüfen darf,[193] bis

---

189 *Klug*, ZD 2016, 315, 317. Vgl. zur Konzerndatenverarbeitung noch im Folgenden unter 5.

190 *Gierschmann*, ZD 2016, 51, 52.

191 *Jaspers/Reif*, RDA 2016, 61, 67.

192 Art. 37 Abs. 1 lit. j des EP-Entwurfs.

193 Im deutschen Recht streitig, vgl. BAG 23. 3. 2011 – 10 AZR 562/09, NZA 2011, 1036, 1038, das die Frage ausdrücklich offen gelassen hat.

zur Kollision der jeweiligen Überwachungsbefugnisse – des Betriebsrats nach §§ 75 und 80 BetrVG und des betrieblichen Datenschutzbeauftragten nach § 4g BDSG und in Zukunft nach Art. 39 DS-GVO. Diese Rechtsunklarheiten bleiben auch auf europäischer Ebene weiterhin bestehen.[194] Jedenfalls kann der betriebliche Datenschutzbeauftragte auch künftig den Betriebsrat nicht kontrollieren.[195]

Für den deutschen Gesetzgeber bleibt einiges zu tun, wenn das derzeitige Datenschutzniveau aufrechterhalten werden soll. Zum einen sollten die Bestellungsvoraussetzungen aus § 4f BDSG beibehalten werden. Darüber hinaus sollte der arbeitsrechtliche Kündigungsschutz aus dem BDSG aufgenommen werden; die DS-GVO enthält in Art. 38 Abs. 3 nur einen Abberufungsschutz. Schließlich sollte der in Art. 38 Abs. 5 DS-GVO angesprochene Geheimhaltungs- und Vertraulichkeitsgrundsatz klarer im Sinne eines Verschwiegenheitsrechts des Datenschutzbeauftragten ausgestaltet werden.[196]

4. Datenschutz durch Technik (Privacy by Design)

Beim Datenschutz durch Technik geht es darum, Datenschutz durch technische Verfahren zu gewährleisten. Vor allem soll der Datenschutz durch die Technik selbst gewährleistet werden, die etwa den Personenbezug bei der Weiterverarbeitung von Daten reduzieren kann. Dazu gehört aber auch Systemdatenschutz.[197] Flankiert wird dieser Weg durch datenschutzspezifische Zertifizierungsverfahren in Art. 42 DS-GVO, die allerdings freiwillig bleiben sollen.

Die DS-GVO setzt in Art. 25 auf Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Privacy by Design). Die Kommission will damit „die Vorteile von massendatenbezogenen Innovationen bei gleichzeitigem Schutz der Privatsphäre“[198] vereinbaren und verweist etwa auf datenschutzfreundliche Techniken wie Pseudonymisierung, die in Art. 25 DS-GVO neben Datenminimierung (ohne spezifischen Hinweis, wie diese genau zu erfolgen habe) genannt ist. Damit greift die Grundverordnung den Wandel in der Konzeption eines wirkungsvollen Datenschutzes auch in Zeiten des Internets auf, in denen allein normative Vorgaben für Datenschutz nicht mehr ausreichend sind. Sie müssen durch technische Maßnahmen ergänzt werden, die die Hard- und Software so gestalten, dass bestimmte Verarbeitungsoptionen gar nicht erst bereitgestellt und auf diese Weise weniger

194 *Taeger/Rose*, BB 2016, 819, 828 f.
195 Vgl. dazu DKKW-*Klebe*, BetrVG, § 94.
196 So auch *Jaspers/Reif*, RDV 2016, 61, 68.
197 *Dix*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht 2003, Kap. 3.5.
198 Pressemitteilung der Europäischen Kommission vom 15. 12. 2015, DuD 2/2016, 70.

Daten gesammelt werden.[199] Allerdings muss beachtet werden, dass die technischen Maßnahmen nicht etwa primär im Wege von „Selbstdatenschutz" von den Betroffenen ergriffen werden müssen, die dann für ihr Schutzniveau selbst verantwortlich wären. Natürlich muss aber auch mehr Bewusstsein bei den Betroffenen etwa für Zugangsschutz oder Sicherheitssoftware gefördert werden, ohne den Datenschutz auf sie abzuwälzen.[200] Eine derartige Individualisierungstendenz ist jedoch in der Datenschutzdiskussion nicht zu übersehen.[201]

Art. 25 DS-GVO adressiert zwar den für die Verarbeitung Verantwortlichen, lässt aber außer vagen Hinweisen und dem genannten Beispiel Pseudonymisierung weitgehend offen, wie die Technik gestaltet werden soll. Bei der Pseudonymisierung handelt es sich um ein Verfahren, bei dem der Name und andere Identifikationsmerkmale durch ein Kennzeichen, i. d. R. einen Code, ersetzt werden, um die Bestimmung des Betroffenen auszuschließen oder zumindest zu erschweren (§ 3 Abs. 6a BDSG). Mit Hilfe eines Schlüssels allerdings können die Daten den Personen wieder zugeordnet werden. Ähnliches gilt auch bei der Reanonymisierung.[202]

Im Kommissionsentwurf von 2012 war dieser Ansatz in sich schlüssig, da im dortigen Art. 23 Nr. 4 die Kommission nachträglich technische Standards festlegen konnte. Das war insofern ein zukunftsfähiges Konzept als sich die Technik laufend weiterentwickelt und die Verantwortlichen allein aufgrund einer Generalklausel nicht rechtssicher wissen, welchen technischen Datenschutz sie wann implementieren müssen. Da sich die Kommission in der DS-GVO von 2012 sehr viele eigene Konkretisierungsbefugnisse eingeräumt hatte, die vom Rat nahezu vollständig zusammengestrichen wurden, entfiel auch die in Art. 23 Nr. 4 DS-GVO-E (2012). Folglich enthält Art. 25 DS-GVO nun nur noch die allgemeine Verpflichtung des Verantwortlichen, „geeignete technische und organisatorische Maßnahmen" zu treffen – mit dem einzigen Beispiel Pseudonymisierung (Abs. 1) – und durch Voreinstellungen nur „erforderliche" personenbezogene Daten zu erheben (Abs. 2). Auch Erwägungsgrund 78 bietet nicht mehr Substanz. Danach soll der Verantwortliche „interne Strategien festlegen und Maßnahmen ergreifen, die den Grundsätzen des Datenschutzes durch Technik (data protection by design) und datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun".

---

199 Dazu auch *Maas*/*Schmitz*/*Wedde*, Datenschutz 2014 – Probleme und Lösungsmöglichkeiten, 2014.

200 So auch *Däubler*, AiB Extra 2016, 29, 31.

201 Kritisch *Simitis*, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 2014, 8. Aufl., Einleitung Rn. 113 ff.

202 Zur relativ einfachen Wiederherstellung des Zusammenhangs zwischen Daten und Betroffenen siehe *Mayer-Schönberger*/*Cukier*, Big Data, 2013, 2. Aufl., S. 194.

Ein großes Defizit der DS-GVO besteht darin, dass Art. 25 nur den für die Datenverarbeitung Verantwortlichen verpflichtet, nicht aber die Hersteller von Datenverarbeitungstechnik. Die Pflicht der verantwortlichen Stelle wird sogar noch dadurch eingeschränkt, dass sie unter mehreren Vorbehalten steht. Dass der Verantwortliche nicht über den Stand der Technik hinaus verpflichtet werden kann, ist selbstverständlich. Es bedeutet aber eine erhebliche Relativierung der Pflicht, Datenschutz durch Technik zu gewährleisten, dass es auch auf die Implementierungskosten, die Eintrittswahrscheinlichkeit und Schwere von Risiken sowie ganz allgemein die Umstände der Verarbeitung ankommen soll. Auch Erwägungsgrund 78 bleibt sehr vage. Hersteller der Produkte, Dienste und Anwendungen „sollten ermutigt werden", Datenschutz durch Technik zu berücksichtigen. Durch diese Einschränkungen, aber vor allem, weil die Hersteller der Technologie nicht verpflichtet werden können, wird man beim allgemeinen Datenschutz an Schutz durch die Technik keine allzu großen Hoffnungen knüpfen dürfen.

Anders sieht es in den Bereichen aus, in denen die Mitgliedstaaten eigene Regelungskompetenzen behalten, wie beim Beschäftigtendatenschutz. Hier darf, wie oben ausgeführt, mehr und spezifischer geregelt werden als in der Verordnung. Der nationale Gesetzgeber könnte und sollte also viel genauer die zu treffenden technischen Maßnahmen bestimmen, mit deren Hilfe Beschäftigtendaten verarbeitet werden, etwa Löschroutinen, Verfalltermine für gespeicherte Daten oder Vier-Augen-Prinzip bei Zugriffsrechten.[203] Vor allem aber wären für Datenschutz durch Technik auch die Kollektivparteien[204] aufgerufen, Standards für technische Voreinstellungen für die Verarbeitung von Beschäftigtendaten zu definieren. Dabei dürfte sich allerdings das Problem stellen, dass viele Betriebsräte, vor allem in kleineren Unternehmen, die hochkomplexen Verarbeitungsbedingungen gar nicht bewerten können und eher auf eine Entlastung mittels Datenschutz durch Technik hoffen dürften als fachlich selbst in der Lage zu sein, Standards zu definieren. Hier bedarf es umfangreicher IT-Beratung von außen. Ein betrieblicher Datenschutzbeauftragter befindet sich im Übrigen bei der Definition technischer Standards in einer vergleichbar überfordernden Situation. Das gilt auch für die Kontrolle, ob implementierte technische Standards eingehalten werden.

5. Konzerndatenverarbeitung

Der Austausch von Beschäftigtendaten zwischen konzernabhängigen Unternehmen ist nicht privilegiert, sondern erfolgt derzeit nach den Regeln der Auftrags-

---

203 Detaillierte Vorschläge hierzu finden sich in einem HSI-Gutachten von 2014: *Maas/Schmitz/Wedde*, Datenschutz 2014 – Probleme und Lösungsmöglichkeiten, 2014, insbesondere S. 56 ff., 93 ff.

204 Zu deren Regelungsbefugnis s. unten E.IV.

datenverarbeitung nach § 11 BDSG,[205] da Konzernunternehmen untereinander datenschutzrechtlich als Dritte gelten. Auch nach Inkrafttreten der DS-GVO wird sich das nicht prinzipiell ändern. Der Verordnungsentwurf der Kommission von 2012 enthielt nichts zum Thema. Die verabschiedete Verordnung definiert in Art. 4 Abs. 19, dass eine Unternehmensgruppe eine Gruppe[206] ist, die aus einem herrschenden und den von diesen abhängigen Unternehmen besteht. In Erwägungsgrund 48 wird die Formulierung des Erwägungsgrundes 38a der Trilog-Fassung vom Dezember 2015 aufgegriffen, wo es lediglich heißt, dass „Verantwortliche, die Teil einer Unternehmensgruppe oder Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, ein berechtigtes Interesse haben können, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln." Abgesehen davon, dass ein Erwägungsgrund keine Rechtswirkung hat und damit ohnehin kein Konzernprivileg postulieren könnte, ist die Formulierung als Hinweis darauf zu verstehen, dass es bei der Abwägung der Interessen des Datenverwenders und der geschützten Person nach Art. 6 Abs. 1 lit. f DS-GVO auch ein Unternehmensinteresse gibt, Daten im Konzern zu übermitteln.[207]

Auch Art. 88 Abs. 2 DS-GVO führt zu keiner anderen Bewertung. Dieser Absatz stellt besondere Schutzbedingungen für nationale Beschäftigtendatenschutzregelungen auf,[208] die insbesondere auch dann eingehalten werden müssen, wenn es um die Übermittlung personenbezogener Daten innerhalb eines Konzerns geht. Darin ist kein „verstecktes Konzernprivileg" zu sehen, denn Art. 88 Abs. 2 behandelt nur die „berechtigten Interessen und Grundrechte der betroffenen Person, insbesondere im Hinblick auf (…) die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe". Dies könnte zwar so verstanden werden, dass der nationale Gesetzgeber Konzerndatenverarbeitung personenbezogener Beschäftigtendaten regeln darf, dann aber jedenfalls deren Grundrechte und berechtigte Interessen wahren muss.

Jedoch ermöglicht Art. 47 DS-GVO Datenübermittlung im Konzern auf der Basis von Binding Corporate Rules. Die Vorschrift steht im Kapitel V über die Übermittlung personenbezogener Daten an Drittländer und sieht vor, dass die zuständige

---

205 *Seifert*, in: Simitis, BDSG-Kommentar, 2014, 8. Aufl., § 32 Rn. 116; *Wedde*, in: Däubler/Klebe/Wedde/Weichert, Kompaktkommentar zum BDSG, 2016, 5. Aufl., § 11 Rn. 10.

206 Der im Deutschen in diesem Zusammenhang unübliche Begriff geht auf das französische „le groupe" = Konzern zurück.

207 *Taeger/Rose*, BB 2016, 819, 822, Anm. 41.

208 Dazu näher oben E.II.2.

Aufsichtsbehörde konzerninterne rechtlich bindende Datenschutzvorschriften genehmigen kann, wenn diese die Anforderungen von Art. 47 Abs. 2 erfüllen und gemäß Art. 47 Abs. 1 lit. b den betroffenen Personen durchsetzbare Rechte einräumen.

III. Nationale Regelungsmöglichkeiten für Beschäftigtendatenschutz

1. EU-Rechtsgrundlage für Beschäftigtendatenschutz

Grundsätzlich können Mitgliedstaaten bei sekundärem Gemeinschaftsrecht geeignete Durchführungsmaßnahmen auch ohne Ermächtigung in einer EU-Verordnung erlassen. Nach Art. 291 Abs. 1 AEUV können sie dazu sogar verpflichtet sein, wenn diese erforderlich sind, um den Rechtsakt der Union durchzusetzen.[209] Für den Beschäftigtendatenschutz als Teil des Arbeitsrechts ergibt sich dabei noch eine weitere Besonderheit. Anders nämlich als beim allgemeinen Datenschutz, für den die Union nach Art. 16 AEUV Verordnungen mit unmittelbarer Bindungswirkung erlassen darf, hat die EU für das Arbeitsrecht nur eine Kompetenz nach Art. 153 i. V. m. Art. 114 Abs. 2 AEUV. In diesem Bereich dürfen nur Richtlinien erlassen werden, die national umgesetzt werden müssen. Der europäische Gesetzgeber ist also nicht dazu ermächtigt, den Beschäftigtendatenschutz in einer Verordnung mitzuregeln. Dieser Teil des Datenschutzes bleibt auf nationaler Ebene regelbar; eine Öffnungsklausel in diesem Bereich dient daher eher der Klarstellung als dass sie rechtlich erforderlich wäre, um Beschäftigtendatenschutz weiter national zu regeln. Eine Kompetenzüberschreitung des EU-Gesetzgebers würde zur Unwirksamkeit der Regelung führen.

Da allerdings eine bereichsspezifische Datenschutzregelung wie der Beschäftigtendatenschutz nicht losgelöst vom allgemeinen Datenschutz angewendet werden kann und der allgemeine Datenschutz in Zukunft europäisch geregelt ist, ist es nicht nur sinnvoll, sondern erforderlich, dass der deutsche Gesetzgeber die Materie vor dem Hintergrund der DS-GVO regelt.

2. (Erweiterte) Fortgeltung von § 32 BDSG

Die DS-GVO lässt große Regelungsspielräume gerade in Bereichen, in denen es in der Vergangenheit nicht gelungen ist, klare, umfassende und stimmige

---

209 *Streinz,* EUV-AEUV, 2012, 2. Aufl., Art. 291 Rn. 4 ff.; *Schwarze,* EU-Kommentar, 2012, 3. Aufl., Art. 291 AEUV Rn. 2.

Regelungen zu erlassen, insbesondere im Gesundheits- und Beschäftigtendatenschutz.[210]

Ausdrücklich gesetzlich geregelt ist der Beschäftigtendatenschutz in Deutschland nur rudimentär seit 2009 in § 32 BDSG. Da „spezifischere" Regelungen nicht unbedingt neue Regelungen sein müssen, könnte man im Rahmen des Art. 88 Abs. 1 auch eine einfache Fortschreibung dieser Norm erwägen. Kleinere Verbesserungen im Vergleich zur DS-GVO wären dann schon enthalten, denn § 32 Abs. 2 BDSG geht über die Verordnung hinaus, da nach dem BDSG auch nicht automatisiert verarbeitete personenbezogene Daten, etwa in Akten, vom Datenschutz umfasst sind. Auch der Inhalt von § 32 Abs. 1 Satz 2 BDSG, wo geregelt ist, wann Beschäftigtendaten zur Aufdeckung von Straftaten erhoben, verarbeitet oder genutzt werden dürfen, kann nicht unmittelbar aus der Verordnung entnommen werden. Ansonsten dürfte § 32 BDSG in seiner vagen Formulierung nicht „spezifisch" genug sein, um Art. 88 DS-GVO auszufüllen. Wenn also von Art. 88 Abs. 1 DS-GVO Gebrauch gemacht wird und zunächst nur eine „kleine Lösung" an nationaler Gesetzgebung im Beschäftigtendatenschutz realisiert werden soll, muss § 32 BDSG angepasst werden, um jedenfalls die Mindeststandards der DS-GVO einzuhalten. Das wirkt sich z. B. beim Transparenzgebot der DS-GVO (Art. 12) und den Betroffenenrechten (Art. 13 ff.) aus, die weiter gehen als bisher im nationalen Datenschutzrecht. Wird national nicht „spezifisch" genug geregelt, gelten die Vorschriften der DS-GVO. So verhält es sich auch in Mitgliedstaaten, die von der Regelungsoption in Art. 88 DS-GVO keinen Gebrauch machen.

Jedenfalls sollten zumindest lange überfällige Konkretisierungen vorgenommen werden, wie eine Beschränkung der Einwilligung des Beschäftigten als Rechtfertigungsgrund für Datenverarbeitung.[211] Auch Art. 88 Abs. 2 DS-GVO erfordert sofortige Regelungen zu den dort ausdrücklich genannten Verarbeitungszusammenhängen, d. h. vor allem zur Überwachung am Arbeitsplatz. Regelungen dazu sind auch deshalb erforderlich, weil es im deutschen Recht bislang nur eine Hilfskonstruktion über die Telekommunikationsgesetze TMG und TKG gibt. Auch für die Verarbeitung von sensiblen Daten im Beschäftigungsverhältnis, wie etwa genetische, biometrische oder Gesundheitsdaten, die in Art. 9 DS-GVO als

---

210 Das knapp 500 Seiten starke Gutachten von *Kühling/Martini* vom August 2016 widmet Art. 88 nur 13 Zeilen, stellt auf diesen aber fest, dass der Gesetzgeber völlig frei ist, „Arbeitnehmerdatenschutz" eigenständig zu regeln: *Kühling/Martini et al.*, Die Datenschutz-Grundverordnung und das nationale Recht, 2016, S. 298 (es dürfte ein redaktionelles Versehen sein, dass sowohl bei Art. 88 DS-GVO wie bei § 32 BDSG nicht der im Gesetz benutzte und viel weitere Beschäftigtenbegriff benutzt wird).

211 Zur Einwilligung s. näher unten E.III.4.

besonders schutzbedürftig hervorgehoben werden, bedürfte es auch bei einer zunächst „kleinen“ Lösung i. S. v. Art. 88 Abs. 1 DS-GVO einer klaren Regelung.

3. Beschäftigtendatenschutzgesetz

a) Erforderlichkeit einer gesetzlichen Regelung

Da der ursprüngliche Plan, die Fortentwicklung des Datenschutzes und bereichsspezifische Regelungen bei der Kommission durch delegierte Rechtsakte zu zentralisieren, gescheitert ist und daher die nähere Ausgestaltung und Weiterentwicklung des Beschäftigtendatenschutzes nur durch Arbeitsteilung zwischen der EU und den Mitgliedstaaten möglich ist, müssen diese ihrer Aufgabe auch gerecht werden und Regelungen treffen. Mit punktuellen Ergänzungen von § 32 BDSG wird man sich dabei nicht begnügen können. Dieser Weg wäre vielmehr eine konkludente Erklärung, nicht regeln zu wollen.

Schon das BDSG enthält keinen konsistenten Beschäftigtendatenschutz. § 32 BDSG ist nur eine Notlösung. Aus der Not geboren wurde diese Norm im Jahre 2009 als Reaktion auf gravierende Verstöße gegen den Beschäftigtendatenschutz bei mehreren Großunternehmen ins BDSG eingefügt. Schon zu diesem Zeitpunkt lagen mehrere Entwürfe für ein Beschäftigtendatenschutzgesetz vor, die aber zugunsten einer politisch rasch durchsetzbaren Variante fallen gelassen wurden. Die überfällige bereichsspezifische gesetzliche Regelung für den Schutz von Beschäftigtendaten wurde in einer einzigen Generalklausel vorläufig abgehakt. Auch nach dem Erlass von § 32 BDSG wurden weitere gesetzgeberische Initiativen mit Hinweis auf die in Arbeit befindliche europäische Datenschutzgrundverordnung vertagt. Im Koalitionsvertrag von 2013 heißt es:

„Die Verhandlungen zur Europäischen Datenschutzgrundverordnung verfolgen wir mit dem Ziel, unser nationales Datenschutzniveau – auch bei der grenzüberschreitenden Datenverarbeitung – zu erhalten und über das europäische Niveau hinausgehende Standards zu ermöglichen. Sollte mit einem Abschluss der Verhandlungen über die Europäische Datenschutzgrundverordnung nicht in angemessener Zeit gerechnet werden können, wollen wir hiernach eine nationale Regelung zum Beschäftigtendatenschutz schaffen“.[212]

Diese Planung basierte auf der Vorstellung, dass die Verabschiedung eines nationalen Beschäftigtendatenschutzgesetzes nicht sinnvoll sei, wenn es kurz darauf wegen einer die Materie auch regelnden unmittelbar und vorrangig geltenden europäischen Datenschutzverordnung nicht mehr hätte angewendet werden dürfen.

---

212 CDU/CSU/SPD, Koalitionsvertrag 18. Legislaturperiode, 2013, S. 70.

Die Lage stellt sich nun aber etwas anders dar als wohl erwartet. Die Grundverordnung ist zwar doch innerhalb des EU-Zeitplanes verabschiedet worden, regelt aber den Beschäftigtendatenschutz gerade nicht speziell, sondern überlässt ihn in Art. 88 DS-GVO ausdrücklich den Mitgliedstaaten. Daher ist eine umfassende nationale Regelung nicht nur rechtlich zulässig, sondern auch geboten, um ausreichenden Datenschutz im Beschäftigungsverhältnis zu gewährleisten. Der vage § 32 BDSG und die nur punktuelle Rechtsprechung dazu erlauben auch derzeit schon keinen rechtssicheren Umgang mit personenbezogenen Daten im Beschäftigungsverhältnis. Auch die zahlreichen Betriebsvereinbarungen zum Umgang mit Beschäftigtendaten erübrigen kein einheitliches Gesetz. Kollektivvereinbarungen und ausdrücklich auch Betriebsvereinbarungen können zwar gemäß Art. 88 Abs. 1 DS-GVO i. V. m. Erwägungsgrund 155 weiterhin Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten sein,[213] schützen aber nur Arbeitnehmer und nicht alle Beschäftigten im Sinne des weiten Beschäftigtenbegriffs der Verordnung und darüber hinaus nur die in Betrieben mit Betriebsrat, wo entsprechende Betriebsvereinbarungen bestehen.

Daher mahnt auch die Bundesbeauftragte für den Datenschutz an, dass sich die nationale Ausgestaltung nicht nur auf die Bereinigung des vorhandenen Rechts beschränken darf, sondern auch neue Impulse gegeben werden müssen. Gerade für den Beschäftigtendatenschutz ist in Art. 88 DS-GVO ein klarer Auftrag an den nationalen Gesetzgeber zu sehen, das längst überfällige Beschäftigtendatenschutzgesetz zu schaffen.[214] Eine „kleine Lösung" kann daher allenfalls eine Übergangsregelung sein, der auch wegen der Pflicht des Gesetzgebers, das informationelle Selbstbestimmungsrecht aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG zu gewährleisten,[215] eine umfassende Lösung folgen muss.

b) Bisherige Entwürfe

Schon im Volkszählungsurteil von 1983 hat das BVerfG für die Verarbeitung personenbezogener Daten möglichst bereichsspezifische Regelungen gefordert. Seitdem sah fast jede Koalitionsvereinbarung den Erlass eines Beschäftigtendatenschutzgesetzes vor,[216] so auch die o. a. der 18. Legislaturperiode. Da die 2009 in

---

213 Dazu näher unten E.IV.

214 *Voßhoff*, DuD 2016, 138. So auch in der Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 27. 3. 2014, 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Hamburg, 27./28. 3. 2014.

215 *Weichert*, in: Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 2016, 5. Aufl., Einleitung Rn.15.

216 *Schuler/Weichert*, Die EU-DSGVO und die Zukunft des Beschäftigtendatenschutzes, Gutachten v. 8. 4. 2016, *http://www.netzwerk-datenschutzexpertise.de/sites/default/files*.

Kraft getretene Generalklausel in § 32 BDSG fast alle Fragen des Beschäftigtendatenschutzes offen lässt und auch die Rechtsprechung nur punktuell zu Klarstellungen beitragen konnte, gab es mehrere konkrete Vorschläge für ein Beschäftigtendatenschutzgesetz. So legten die SPD,[217] aber auch Bündnis 90/Die Grünen einen Entwurf für ein eigenes Beschäftigtendatenschutzgesetz vor.[218] Der DGB entwickelte Leitlinien.[219] Die Bundesregierung legte 2010 einen umstrittenen Vorschlag vor,[220] der nur die Ergänzung des BDSG um einige weitere Paragraphen bedeutet hätte. Nicht nur, dass dieser Weg zu einer sehr unübersichtlichen Regelung geführt hätte und damit weit von der Erfüllung von Transparenzanforderungen an den Datenschutz entfernt war. Die Regelungen blieben auch zu punktuell, da nur einige Verarbeitungsformen erfasst wurden, andere, wichtige wie etwa die Biometrie nur am Rande eine Rolle spielten. Grundsätzliche Probleme, wie Beweiserleichterungen bei der Verwertung unzulässig im Internet recherchierter Daten oder Verwertungsverbote, wurden gar nicht angesprochen. Teilweise wurde die Arbeitnehmerüberwachung sogar ausgeweitet, z. B. durch die Einführung allgemeiner Gesundheitsuntersuchungen während des Beschäftigungsverhältnisses.[221] Entsprechend erreichte der Regierungsentwurf dann auch nicht das Gesetzgebungsverfahren und das Regelungserfordernis stellt sich nach dem Erlass der DS-GVO erneut.

c) Mindestinhalte einer nationalen Regelung zum Beschäftigtendatenschutz

Komplexe Lebenssachverhalte bedürfen differenzierter Regulierung, wenn der Schutzzweck erreicht werden soll. Wenige Generalklauseln sind zwar zunächst übersichtlicher, führen aber immer zu Rechtsunsicherheit und Regelungslücken, die in jahrelanger Detailarbeit von der Rechtsprechung gefüllt werden müssen, was gerade beim oft unpräzise justierenden EuGH problematisch ist. Rechtsgebiete werden auf diesem Wege schließlich viel unübersichtlicher[222] als bei einer systematischen gesetzlichen Regelung. Dabei ist Überregulierung zwar immer

---

217 BT-Drs. 17/69 v. 25. 11. 2009.

218 BT-Drs. 17/4853.

219 Abgedruckt in AuR 2010, 315.

220 BT-Drs. 17/4230 v. 15. 12. 2010.

221 Zu den Kritikpunkten im Einzelnen: *Körner*, Moderner Datenschutz für die Beschäftigten: Ein Ende der Skandale? – Gutachten für das HSI, 8. 11. 2010.

222 *Krause* weist zu Recht darauf hin, dass gerade im Beschäftigtendatenschutz die Rechtsprechung weniger als in anderen arbeitsrechtlichen Gebieten für klare Orientierung sorgen konnte: *Krause*, Verhandlungen des 71. Deutschen Juristentages, Band I: Gutachten/Teil B: Digitalisierung der Arbeitswelt – Herausforderungen und Regelungsbedarf, Essen 2016, S. 76.

eine Gefahr, aber eine „Verrechtlichungsfalle“[223] müsste man bei einem Beschäftigtendatenschutzgesetz nicht gleich befürchten, wenn ein Gleichgewicht zwischen konkreten Regelungen typischer Verarbeitungszusammenhänge im Beschäftigungsverhältnis und ausreichende Offenheit durch generelle Regelungen für weitere (technische) Entwicklungen gefunden werden kann. Jedenfalls sollte immer auf den aktuellen Stand der Technik abgestellt werden, der sich z. B. in DIN-Normen oder Empfehlungen von Fachgesellschaften niederschlagen könnte. Gerade wegen der rasanten Entwicklung der Informationstechnologie würde sich beim (Beschäftigen-)Datenschutz darüber hinaus ein regelmäßiger gesetzgeberischer Überprüfungsturnus anbieten. Derartiges ist dem deutschen (Arbeits-)Recht nicht fremd,[224] vom Gesetzgeber aber i. d. R. wenig geschätzt.

aa) Mindestrechte der DS-GVO

Ein Beschäftigtendatenschutzgesetz müsste jedenfalls die Mindestrechte der DS-GVO enthalten. Dazu gehören insbesondere:

- Die Betroffenenrechte aus Art. 12 ff. DS-GVO.[225]
- Besonderer Schutz sensibler Daten gemäß Art. 9 DS-GVO.[226]
- Die Berücksichtigung der Voraussetzungen in Art. 88 Abs. 2 DS-GVO, der im Wesentlichen der BVerfG-Rechtsprechung zum Allgemeinen Persönlichkeitsrecht entspricht.[227]
- Aus Gründen der Rechtsklarheit sollten auch die in der DS-GVO geregelten Grundsätze aufgenommen werden, die ohnehin als Auffangregeln gelten würden. In derartigen Fällen würde auch das Wiederholungsverbot nicht gelten.[228]

bb) Vorschriften für typische Verarbeitungsformen

Daneben sollten Vorschriften für typische Verarbeitungsformen aufgenommen werden. Dazu gehören bisher schon übliche Verarbeitungsformen, wie u. a. Videokontrolle, Ortungssysteme, IT-basierte Verfahren der Zugangskontrolle, etwa biometrische Verfahren, die Überwachung des Kommunikationsverhaltens von Beschäftigten sowohl bei der Nutzung betrieblicher IT-Infrastruktur wie bei der

---

223 So *Schuler/Weichert*, Die EU-DSGVO und die Zukunft des Beschäftigtendatenschutzes, Gutachten, 8. 4. 2016, S. 16.

224 S. etwa das Beschäftigungsförderungsgesetz aus den 1980er Jahren.

225 S. oben C.IV.

226 Dazu genauer oben E.II.2.d) und unten III.4.d)bb).

227 S. oben E.II.2.c).

228 S. oben D.

Nutzung privater Geräte („Bring your own device"). Auch das Screening von Bewerbern in sozialen Netzwerken ist regelungsbedürftig.

cc) Vorschriften für neue Verarbeitungsformen

Unter Datenschutzgesichtspunkten besonders problematisch sind neue Verarbeitungsformen, wie Big Data-Anwendungen oder Cloud Computing. Bei Big Data-Anwendungen geht es vor allem um die Zweckänderung von Datenverarbeitung, beim Cloud Computing besonders um Zugriffsrechte. Beides wäre regelbar, jedenfalls in einem abgrenzbaren Zusammenhang für Beschäftigtendaten eines Unternehmens. Die DS-GVO enthält dazu nichts Konkretes; versteckt werden in Art. 6 Abs. 4 i. V. m. Erwägungsgrund 50 Big Data-Anwendungen im Prinzip eher zugelassen. Im Beschäftigungsverhältnis können diese Verarbeitungsformen zunehmend Bedeutung erlangen. Cloud Computing ist in vielen Unternehmen bereits die Regel und auch Big Data-Auswertungen für die Voraussage zukünftigen Mitarbeiterverhaltens – und daran geknüpfte Rechtsfolgen – sind keine ferne Zukunftsvision.[229]

dd) Telekommunikation

Im Rahmen eines Beschäftigtendatenschutzgesetzes sollte auch endlich die bislang als Hilfskonstruktion herangezogene Fiktion, der Arbeitgeber sei Diensteanbieter i. S. der Telekommunikationsgesetze TKG und TMG, wenn Arbeitnehmer Telefon- und Internetverbindungen des Arbeitgebers erlaubt privat nutzen, auf ein rechtlich klares Fundament gestellt werden, das den arbeitsrechtlichen Besonderheiten Rechnung trägt.

ee) Auffang-Generalklausel

Auch wenn es wichtig ist, die typischen Verarbeitungsformen von Beschäftigtendaten zu regeln, macht es die rasante technische Entwicklung unumgänglich, zusätzlich eine Generalklausel vorzusehen.[230]

ff) Einschränkung der Einwilligung

Auch eine Einschränkung der Einwilligung als Rechtfertigung für die Verarbeitung personenbezogener Daten im Beschäftigungskontext muss gesetzlich

---

229 *Krause* verweist in diesem Zusammenhang auf US-amerikanische Beispiele: Verhandlungen des 71. Deutschen Juristentages, Band I: Gutachten/Teil B: Digitalisierung der Arbeitswelt – Herausforderungen und Regelungsbedarf, Essen, 2016, S. 74 f.

230 So auch *Krause*, a. a. O., S. 78.

geregelt werden. Das gilt besonders für die Einwilligung des Beschäftigten in die Verarbeitung sensibler Daten. Wegen der besonderen Bedeutung der Materie, wird sie im folgenden eigenen Kapitel behandelt.

gg) Verwertungsverbot

Schließlich sollte ein Verwertungsverbot für rechtswidrig erlangte personenbezogene Beschäftigtendaten normiert werden.

Rechtstechnisch gibt es zwei Umsetzungsmöglichkeiten für spezifische gesetzliche Beschäftigtendatenschutzregeln: sie können in ein auf der Basis der DS-GVO überarbeitetes BDSG integriert oder in einem eigenen Gesetz geregelt werden, wobei ein eigenständiges Gesetz aus Gründen der Rechtsklarheit und Transparenz zu bevorzugen wäre.[231]

4. Einwilligung als Erlaubnis, Art. 6 Abs. 1 lit. a, Art. 7 DS-GVO

a) Einwilligung als Ausdruck der informationellen Selbstbestimmung

In einer freiheitlichen Rechtsordnung ist die Verfügungsbefugnis des Einzelnen über seine eigenen Rechte eine grundlegende Gewährleistung.[232] Diese Verfügungsbefugnis wird i. d. R. durch die Einwilligung des Betroffenen in Eingriffe in seine Rechte ausgeübt. So ist es auch bei der Erhebung und Verarbeitung personenbezogener Daten. Auch hier ist die Einwilligung Ausdruck der verfassungsrechtlich garantierten informationellen Selbstbestimmung des Einzelnen.[233] Das BDSG sieht deshalb in der Einwilligung nach §§ 4, 4a einen für den öffentlichen wie den nicht-öffentlichen Bereich geltenden, der gesetzlichen Ermächtigung gleichwertigen Rechtfertigungsgrund für die informationstechnische Verwertung personenbezogener Daten. Dem trägt auch Art. 8 Abs. 2 der GR-Charta Rechnung,[234] wo die Einwilligungsmöglichkeit grundrechtlich gewährleistet ist und so ist es auch in Art. 2 lit. h und Art. 7 lit. a der DS-Richtlinie.[235] Die Hauptrolle spielt die Einwilligung allerdings im nicht-öffentlichen Bereich.[236]

---

231 Neben den o. a. (E.III.3.b) Entwürfen ist auch auf die Anforderungen in *Maas*/*Schmitz*/*Wedde*, Datenschutz 2014, S. 114 ff., zu verweisen.

232 *Gola*/*Schomerus*, BDSG, 2015, 12. Aufl., § 4 Rn. 5.

233 S. etwa BVerfG, JZ 2007, 576, 577.

234 Vgl. dazu NK-GA, Art. 8.

235 Zu deren Einwilligungskonzept und Verbesserungsmöglichkeiten hat noch 2011, kurz vor der Vorlage des ersten Entwurfs der DS-GVO die Art. 29-Datenschutzgruppe eine Stellungnahme vorgelegt: Stellungnahme 15/2011 zur Definition der Einwilligung, Dok. 01197/11/DE/WP187.

236 *Simitis,* in: Simitis (Hrsg.), BDSG, Kommentar, 2014, 8. Aufl., § 4a Rn. 14.

Schon gemäß dem BDSG ist die Einwilligung an Voraussetzungen gebunden, die zum Ausdruck bringen, dass sich der Einzelne bei der Verfügung über seine Rechte häufig in einer Situation befindet, in der er die Komplexität der Sachverhalte und Rechtsfolgen einer Einwilligung nicht immer vollständig überblickt. Ähnlich wie auch in anderen Lebenszusammenhängen, etwa bei der Einwilligung in medizinische Eingriffe, sind viele Betroffene mit den Hintergründen der hochkomplexen und sich ständig weiterentwickelnden Informations- und Kommunikationstechnologien nicht gut genug vertraut, um die, auch langfristigen Folgen einer Einwilligung richtig einschätzen zu können.[237] Das gilt übrigens für alle Altersstufen und auch für junge Menschen, die tendenziell zwar unbefangener und mit weniger Berührungsängsten neue Technik bedienen können, aber i. d. R. wenig Kenntnis über die „unsichtbaren" Abläufe haben. Die mit jeder IT-Gerätegeneration vereinfachte Bedienbarkeit bei gleichzeitiger Steigerung der technischen Datenverwertungsmöglichkeiten, verlangt sogar immer weniger Hintergrundwissen, um sich bequem im virtuellen Raum bewegen zu können.

b) Einwilligung als Fiktion

Entsprechend verlangt schon § 4a BDSG, dass eine Einwilligung zu ihrer Wirksamkeit freiwillig erteilt werden muss, nachdem der Betroffene über den Zweck der Datenverarbeitung informiert wurde. Die DS-GVO greift das auf und definiert in Art. 4 Nr. 11: „Einwilligung der betroffenen Person (ist) jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung."

Bereits für den allgemeinen Datenschutz ist zweifelhaft, ob eine Einwilligung in Datenerhebung und -verarbeitung tatsächlich immer ein Instrument zur selbstbestimmten Ausübung der informationellen Selbstbestimmung i. S. v. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ist. Mit einer Einwilligung lässt sich die Zweckbindung gesetzlicher Erlaubnistatbestände umgehen, da die Einwilligung nahezu jede Verwendung personenbezogener Daten legitimieren kann und sich gerade im nicht-öffentlichen Bereich daher mehr und mehr zu einem reinen Verwertungsrecht entwickelt.[238] Daher ist z. T. auch die Rede vom „Traumbild des mündigen Verbrauchers".[239]

---

237 Zur informierten Einwilligung vgl. *Körner*, Informierte Einwilligung als Schutzkonzept, in: Simon/Weiss (Hrsg.), Zur Autonomie des Individuums, Liber Amicorum Spiros Simitis, Baden-Baden 2000, S. 131.

238 *Simitis*, in: Simitis (Hrsg.), BDSG, Kommentar, 2014, 8. Aufl., § 4a Rn. 6 m. w. N.

239 *Buchner*, DuD 2010, 39, 42.

Besonders in Abhängigkeitsverhältnissen entpuppt sich die Legitimationswirkung der Einwilligung dann häufig als Fiktion.[240] Das gilt besonders für das Beschäftigungsverhältnis.[241] Auch hier wird die Einwilligung gerne als „wichtiger Baustein für einen rechtssicheren und praxistauglichen Datenschutz in Zeiten des zunehmenden Datenanfalls" gesehen, insbesondere von Unternehmensseite.[242] Es ist zwar richtig, dass das vom BVerfG definierte Recht auf informationelle Selbstbestimmung bedeutet, dass der Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten bestimmen können soll. Allerdings war das auch schon 1983, im Jahr des Urteils des BVerfG zur Volkszählung, als Grundsatz gemeint, der zum einen vor dem Hintergrund der damals im Vergleich zu heute sehr übersichtlichen automatisierten Datenverarbeitung zu sehen ist, die zudem überwiegend im öffentlichen Bereich stattfand, und zum anderen hinsichtlich der Einwilligung als Rechtfertigungsgrund schon immer an strenge Voraussetzungen gebunden war. Auch das BVerfG wusste bereits 1983, dass eine Einwilligung selbstverständlich nur dann als Ausübung des Selbstbestimmungsrechts des Einzelnen verstanden werden kann, wenn sie im Rahmen eines weitgehend ausgeglichenen (Vertrags-)Verhältnisses erteilt wird.

c) Einwilligung im Beschäftigungsverhältnis

Diese Gleichordnung besteht im Beschäftigungsverhältnis i. d. R. nicht. Der Arbeitnehmer ist abhängig, da er weisungsgebunden ist. Das macht seinen Status gerade aus, etwa im Unterschied zu einem Selbständigen. Die gesamte Entwicklung des Arbeitsrechts ist diesem Umstand geschuldet. Bei Entscheidungen im Rahmen eines Arbeitsvertrages ist der Einzelne rechtlich und faktisch nicht in gleichem Maße frei wie bei anderen Vertragstypen. Das ist eine Binsenweisheit, die auch der EU-Kommission klar war. Sie hatte daher in ihrem Entwurf der DS-GVO vom Januar 2012 eine Einwilligung als Rechtsgrundlage für Datenerhebung und -verarbeitung ausgeschlossen, wenn „ein erhebliches Ungleichgewicht zwischen Betroffenem und Datenverarbeiter besteht" (Art. 7 Abs. 4 DS-GVO-E). Diese Einschränkung sollte dem Umstand Rechnung tragen, dass in Abhängigkeitsverhältnissen die Gefahr für unfreiwillige Einwilligungen besonders groß ist. Das wurde in Erwägungsgrund 34 noch dahingehend konkretisiert, dass dieses Ungleichgewicht vor allem im Arbeitsverhältnis angenommen werden

---

240 *Simitis*, in: Simitis (Hrsg.), BDSG, Kommentar, 2014, 8. Aufl., § 4a Rn. 3 ff., 16 (für den öffentlichen Bereich).

241 *Tinnefeld/Petri/Brink*, MMR 2010, 727, 729.

242 *Wolf/Barlage-Melber*, AiB Extra 2015, 26, 27.

müsse. Darin „keine weitere Einschränkung der Einwilligungsmöglichkeit" zu sehen,[243] ist schwer nachvollziehbar.

Der Passus war in den Trilog-Verhandlungen besonders umstritten, allerdings nicht weil diese Gefahr abwegig wäre, sondern allein aus politischen Erwägungen und wegen der Mehrheitsverhältnisse bei den beteiligten EU-Organen. Daher wurde in der verabschiedeten Version der DS-GVO diese eindeutige Formulierung wieder gestrichen. Jetzt muss die Einwilligung nur noch aufgrund der freien Entscheidung des Beschäftigten erteilt werden. Nun gilt für alle Arten von Einwilligungen, dass es sich dabei gemäß Art. 4 Nr. 11 DS-GVO um freiwillige für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung handeln muss, die das Einverständnis der betroffenen Person mit der Verarbeitung ihrer personenbezogenen Daten zum Ausdruck bringt. Art. 7 spezifiziert dann die Bedingungen für eine rechtfertigende Einwilligung. So muss sie etwa bei schriftlicher Abgabe – Schriftform wird aber nicht gefordert – nach Abs. 2 in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache abgefasst sein und ist nach Abs. 3 frei widerruflich. Gemäß Art. 7 Abs. 1 DS-GVO muss der Verantwortliche nachweisen, dass eine Einwilligung vorgelegen hat. Das ist so zu verstehen, dass er eine rechtmäßige Einwilligung nachweisen muss, was deren Freiwilligkeit beinhaltet.

Aus Art. 7 Abs. 4 DS-GVO wird man ein Koppelungsverbot ablesen können. Danach ist die Freiwilligkeit einer Einwilligung zweifelhaft – und damit die Einwilligung unwirksam –, wenn die Erfüllung eines Vertrages von einer Einwilligung abhängig gemacht wird, ohne dass die Einwilligung für die Erfüllung des Vertrages erforderlich ist. Ob damit eine rechtfertigende Einwilligung des Bewerbers im Bewerbungsverfahren ausgeschlossen ist,[244] hängt davon ab, wie man die „Erfüllung des Vertrages" liest. Da es sich beim Bewerbungsverfahren um eine typische vorvertragliche Situation handelt, die bekanntlich bereits Rechtswirkungen entfaltet, und die Datenschutzbedürftigkeit gerade im Bewerbungsverfahren besonders hoch ist – hohes Informationsinteresse des potentiellen Arbeitgebers, Drucksituation des Bewerbers –, ist die Formulierung in Art. 7 Abs. 4 DS-GVO so zu verstehen, dass auch Einwilligungssituationen gemeint sind, die einen vor dem Abschluss stehenden Vertrag (hier den Arbeitsvertrag) betreffen.

---

243 So *Thüsing*, Beschäftigtendatenschutz und Compliance, § 5 Einwilligung, Rn. 35 f. zum Entwurf der DS-GVO Stand 2014.

244 So *Kort*, NZA 2016 (erscheint demnächst), II.1.k9, der aber nicht bezweifelt, dass die deutsche arbeitsgerichtliche Rechtsprechung zum Fragerecht im Bewerbungsverfahren auch unter der DS-GVO Bestand haben dürfte.

So sinnvoll ein Koppelungsverbot ist, es ist nicht ausreichend, um eine wirklich freie Entscheidung des Betroffenen zu gewährleisten.[245] Daher macht Art. 7 Abs. 4 DS-GVO eine weiter einschränkende nationale Regelung zur Einwilligung nicht überflüssig.

Entscheidend ist daher für die Bewertung der Einwilligung als Datenverarbeitungsrechtfertigung im Beschäftigungsverhältnis die typische Asymmetrie dieses Vertragsverhältnisses. Das ist auch nach wie vor die Sichtweise der DS-GVO, auch wenn die Formulierung in Art. 7 Abs. 4 abgeschwächt wurde. Erwägungsgrund 43 der verabschiedeten DS-GVO greift das „klare Ungleichgewicht" der Kommissionsversion wieder auf und macht deutlich, dass eine Einwilligung keine Rechtsgrundlage sein kann, wenn es im speziellen Fall unwahrscheinlich ist, dass sie freiwillig abgegeben wurde. Allerdings wird es durch diese Relativierung sehr schwierig, eine Einwilligung unter Zwang tatsächlich rechtssicher festzustellen.[246] Als Regelbeispiel für einen Verantwortlichen, zu dem das „klare Ungleichgewicht" typischerweise besteht, wird zwar nur eine Behörde genannt, die aber ausdrücklich („insbesondere") nur ein Beispiel sein soll. Das „klare Ungleichgewicht" besteht i. d. R. auch im Beschäftigungsverhältnis. So haben das bislang in Deutschland i. d. R. auch die Aufsichtsbehörden gesehen.[247]

Darüber hinaus sieht die DS-GVO auch noch weitere Einschränkungen für die Einwilligung vor. Neu ist die Absage an eine „opt-out"-Lösung, wie sie weithin üblich ist und noch im Kommissionsentwurf vorgesehen war: Die Einwilligung wird danach vorausgesetzt, wenn der Betroffene nicht ausdrücklich widerspricht. Von dieser Widerspruchsmöglichkeit macht er in der Praxis häufig keinen Gebrauch, sei es aus Unkenntnis oder Bequemlichkeit. In der DS-GVO ist es nun umgekehrt: Nach Art. 4 Nr. 11 muss eine „Erklärung oder eindeutig bestätigende Handlung" erfolgen, aus der zu erkennen ist, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Zwar ist keine Schriftform vorgeschrieben, aber aus Erwägungsgrund 32 ergibt sich, dass nicht alle konkludenten Handlungen Einwilligungen sein können. Die Einwilligung soll durch eine „eindeutige bestätigende Handlung" erfolgen, mit der „unmissverständlich", „etwa in Form einer schriftlichen Erklärung" deutlich gemacht wird, dass die betroffene Person mit der Verarbeitung ihrer personenbezogenen Daten einverstanden ist. Im selben Erwägungsgrund heißt es auch, dass „Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person keine Einwilligung darstellen" sollten.

---

245 *Simits*, in: Simitis (Hrsg.), BDSG, Kommentar, 2014, 8. Aufl., § a Rn. 65.
246 *Roßnagel/Nebel/Richter*, ZD 2015, 455, 457.
247 *Wybitul/Böhm*, BB 2015, 2102 f. m. w. N.

Im Vergleich zum bisherigen deutschen Recht[248] klarer ist auch die ausdrückliche Regelung eines jederzeitigen Widerrufs der Einwilligung nach Art. 7 Abs. 3 Satz 1 DS-GVO. Über das Widerrufsrecht muss bei Abgabe der Einwilligung informiert werden; außerdem muss der Widerruf so einfach sein wie die Erteilung der Einwilligung. Bislang war das so eindeutig im deutschen Recht nicht geregelt. Daher dürfte die neue BAG-Rechtsprechung, wonach der Widerruf einer Arbeitnehmereinwilligung nur möglich sein soll, wenn ein plausibler Grund vorliegt,[249] nicht aufrecht zu erhalten sein. Man muss bei dem entschiedenen Fall allerdings die konkreten Umstände berücksichtigen. Es ging um § 22 KunstUrhG – eine bereichsspezifische Datenschutznorm, die gemäß § 1 Abs. 3 Satz 1 BDSG Vorrang vor den allgemeinen Regeln hat – und einen Arbeitnehmer, der in einem kurzen Werbevideo seines ehemaligen Arbeitgebers für zwei Sekunden in einer Gruppe von 30 Personen (nach Ansicht des BAG nur schwer identifizierbar) zu sehen war, und die Abwägung, dass es für das Unternehmen einen unverhältnismäßigen Aufwand bedeutet hätte, das Video neu zu drehen. Die Einschränkung des Widerrufs der Einwilligung ist also diesem besonderen Sachverhalt geschuldet und kann nicht für alle Einwilligungen nach § 4a BDSG verallgemeinert werden.[250]

d) Handlungsmöglichkeiten des nationalen Gesetzgebers bei der Einwilligung

aa) Grundsätze

Die Öffnungsklausel für nationale Regelungen in Art. 6 Abs. 2 DS-GVO, der die Rechtmäßigkeitsgründe für Datensammlung aufzählt, erwähnt zwar nur die Buchstaben c) und e) und nicht a) über die Einwilligung. Das bedeutet aber nur, dass die Einwilligung allgemein als Rechtfertigung für Datenerhebung und -verarbeitung im gesamten öffentlichen und privaten Bereich zunächst nur den Voraussetzungen der Verordnung unterliegen soll.

Für Einwilligungen im Rahmen eines Beschäftigungsverhältnisses ist das aber gerade anders. Zwar ist Art. 82 Abs. 3 DS-GVO-E-Ratsversion, wonach die Mitgliedstaaten die Bedingungen festlegen können sollten, „unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung

---

248 Das BDSG regelt in § 28 Abs. 3a nur ein Widerrufsrecht beim Adresshandel oder bei Daten, die für Werbezwecke verwendet werden. Die Landesdatenschutzgesetze und § 13 Abs. 2 Nr. 4 TMG gehen weiter.

249 BAG 11. 12. 2014, NZA 2016, 604; Bespr. *Taeger*, jurisPR-DSR 1/2015, Anm. 4.

250 A. A. *Wybitul/Böhm*, BB 2015, 2101, 2104. Auf den zentralen Umstand, dass es sich um einen Spezialfall nach dem KunstUrhG handelte, wird dort nur in einer Fußnote (Fn. 45) hingewiesen.

des Arbeitnehmers verarbeitet werden dürfen", nicht in den verabschiedeten Verordnungstext übernommen worden. Allerdings überlässt nun Art. 88 Abs. 1 DS-GVO ausdrücklich dem nationalen Gesetzgeber die Kompetenz für Regelungen im Beschäftigtendatenschutz, wozu auch die Einwilligung im Beschäftigungsverhältnis gehört.

Aus der Formulierung des ersten Entwurfs der Kommission für eine Datenschutzgrundverordnung – nationale Regelungen nur „in den Grenzen der Verordnung" – wurde z. T. geschlossen, dass es dem nationalen Gesetzgeber verboten sei, für die Einwilligung strengere Maßstäbe festzulegen als die Verordnung.[251] Abgesehen davon, dass das für die Einwilligung im Beschäftigungsverhältnis keine Rolle gespielt hätte, da der erste Verordnungsentwurf noch ausdrücklich den Ausschluss der Einwilligung in Abhängigkeitsverhältnissen vorsah, ist nun Art. 88 Abs. 1 DS-GVO offen formuliert. Für eine freie nationale Regelbarkeit der Einwilligung im Beschäftigungsverhältnis spricht auch der Umstand, dass die Kommission nahezu alle ihre eigenen Regelungsbefugnisse im Wege delegierter Rechtsakte verloren hat. Eine Einschränkung der nationalen Regelungsrechte war zunächst insofern konsequent, als die vagen Bestimmungen der DS-GVO nach dem ursprünglichen Konzept der Verordnung vorwiegend von der Kommission selbst konkretisiert werden sollten. Schließlich haben sich aber die Mitgliedstaaten diese Konkretisierungsbefugnisse auf vielen Feldern doch selbst vorbehalten, so auch beim Beschäftigtendatenschutz und allen mit ihm zusammenhängenden Fragen, also auch und gerade bei der Einwilligung.

Auch wenn die Verordnung den nationalen Gesetzgeber nicht verpflichtet (nationale Vorschriften „können" vorgesehen werden), macht Erwägungsgrund 155 über Art. 88 DS-GVO hinaus deutlich, für wie zentral der EU-Gesetzgeber die Probleme um die Einwilligung im Beschäftigungsverhältnis und für wie wichtig er nationale Regelungen hält. Eine verbindlichere Regelung war im Kommissionsentwurf vorgesehen, aber unter den 28 Mitgliedstaaten schließlich politisch nicht durchsetzbar. Das hängt auch damit zusammen, dass für viele Mitgliedstaaten, die die DS-Richtlinie von 1995 nur rudimentär umgesetzt hatten, mit der DS-GVO nun erstmals Datenschutzregeln verbindlich werden, denen man nicht mehr so einfach ausweichen kann. Das löst Abwehrreaktionen gegen allzu eindeutige Regelungen aus, wie es das Verbot der Einwilligung als Rechtfertigung in Abhängigkeitsverhältnissen war.

Für Deutschland bedeutet das aber nicht, dass man sich hinter derartige Positionen zurückziehen kann. Hier gilt, dass bei „Privaten, zwischen denen rechtlich Gleichordnung herrscht, aber tatsächlich ein Machtgefälle auftreten kann, der

---

251 So *Gola*, EuZW 2012, 332, 336; *Schüßler/Zöll*, DuD 2013, 639, 640.

Ausgleich in der grundrechtlichen Schutzpflicht des Staates besteht, die durch Gesetzgebung erfüllt wird".[252]

Das BVerfG hat in ständiger Rechtsprechung festgestellt, dass sich „der einzelne Arbeitnehmer (…) beim Abschluss von Arbeitsverträgen typischerweise in einer Situation struktureller Unterlegenheit befindet" und sich diese Unterlegenheit auch während des Arbeitsverhältnisses fortsetze.[253] Aus derartigen asymmetrischen Vertragsverhältnissen – bereits entschieden in einem anderen Fall für den Abschluss eines Versicherungsvertrages[254] – folge zum Schutz des Selbstbestimmungsrechts der Betroffenen eine Regelungspflicht des Gesetzgebers, um „scheinbare Freiwilligkeit" auszuschließen.[255] Die Abhängigkeiten sind im Beschäftigungsverhältnis größer als beim Abschluss von Versicherungsverträgen, da der Arbeitnehmer i. d. R. existentiell auf sein Arbeitsverhältnis angewiesen ist. Wenn das BVerfG schon beim Versicherungsvertrag wegen des asymmetrischen Vertragsverhältnisses den Gesetzgeber in der Pflicht sieht, Regelungen zu treffen, um scheinbare Freiwilligkeit zu vermeiden, gilt diese gesetzgeberische Pflicht erst recht für das Beschäftigungsverhältnis.

Allerdings darf auch im Beschäftigungsverhältnis nicht außer Betracht bleiben, dass die Einwilligung grundsätzlich, wenn ihre Wirksamkeitsvoraussetzungen eingehalten werden, tatsächlich Ausdruck selbstbestimmter Entscheidung über die Verwendung der eigenen personenbezogenen Daten sein kann.[256] Ein soziales Abhängigkeitsverhältnis schließt nicht per se die Freiwilligkeit einer Einwilligung aus.[257] Der Schutz darf also nicht in Bevormundung umschlagen.[258] Daher gehen Forderungen an den Gesetzgeber, die Einwilligung als Rechtfertigung für Datenerhebung und -verarbeitung im Beschäftigungsverhältnis grundsätzlich auszuschließen,[259] zu weit. Auch wenn Art. 88 Abs. 1 DS-GVO strengeren Datenschutz im Beschäftigungsverhältnis erlaubt als es die allgemeinen Regeln der Verordnung vorsehen, würde ein völliger Ausschluss der Einwilligung gegen die

---

252 *Grimm*, JZ 2013, 585, 587; BVerfGE 98, 365, 395.

253 BVerfG, Beschl. v. 23. 11. 2006 – 1 BvR 1909/06, NJW 2007, 286, 287 m. w. N. der Rechtsprechung. So sieht das u. a. auch der Hamburgische Datenschutzbeauftragte, 18. Tätigkeitsbericht, 2002, S. 196 f. bei der Prüfung eines Falles der Konzerndatenverarbeitung.

254 BVerfG, MMR 2007, 93.

255 BVerfG, EuGRZ 2006, 695.

256 So auch das BAG 11. 12. 2014 – 8 AZR 1010/13, NZA 2015, 604, Rn. 32 (zu einer Einwilligung nach KunstUrhG). Vgl. auch *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 65.

257 *Däubler*, in: Däubler/Klebe/Wedde/Weichert, Kompaktkommentar zum BDSG, 2016, 5. Aufl., § 4a Rn. 23.

258 So auch *Buchner*, DuD 2010, 39, 43.

259 So *Hayen*, CuA 3/2016, 20, 22.

Grundprinzipien der DS-GVO verstoßen. Die Genese der DS-GVO bei der Einwilligung zeigt, dass ein vollständiger Ausschluss im Beschäftigungsverhältnis, der zunächst im Kommissionsentwurf von 2012 vorgesehen war, durch die Streichung dieses Passus gerade nicht gewollt ist.

Wo ausnahmsweise nicht von einem strukturellen Machtungleichgewicht ausgegangen werden muss, kann auch im Beschäftigungsverhältnis eine Einwilligung die Datenerhebung und -verarbeitung rechtfertigen. Auch die im Rahmen der DS-Richtlinie von 1995 etablierte Art. 29-Datenschutzgruppe hat sich in mehreren Stellungnahmen mit der Einwilligung befasst und betont, dass diese dann auch im Beschäftigungsverhältnis wirksam sein sollte, wenn für den Arbeitnehmer nachweislich aus der Verweigerung seiner Einwilligung kein Nachteil entstehen kann, sie also die Voraussetzung der Freiwilligkeit erfüllt.[260] Das ist besonders der Fall, wenn sich für den Arbeitnehmer überwiegend Vorteile ergeben.[261] Eine solche Einwilligung könne dann gültig sein, wenn die Person eine tatsächliche Wahlmöglichkeit habe und kein Risiko einer Täuschung, Einschüchterung, Nötigung oder beträchtlicher negativer Folgen bei Nichterteilen der Einwilligung bestehe.[262] Das ist aber eher die Ausnahme. Im Beschäftigungsverhältnis ist, wie erläutert, die allgemeine datenschutzrechtliche Rechtmäßigkeitsvoraussetzung der Freiwilligkeit häufig zweifelhaft und ihre Einhaltung schwer nachprüfbar – zumal der Beschäftigte im bestehenden Arbeitsverhältnis selten eine unfreiwillige Einwilligung (gerichtlich) geltend machen wird.

Daher bedarf es einer klaren gesetzgeberischen Einschränkung. Es müssen Bereiche definiert werden, wo eine Einwilligung die Datensammlung im Beschäftigungsverhältnis grundsätzlich nicht rechtfertigen kann. Dazu gehören insbesondere Datenerhebungen, die den Intimbereich berühren, etwa in Sanitäreinrichtungen, die Erstellung vollständiger Persönlichkeitsbilder, Totalüberwachung und vor allem die Erhebung von sensiblen Daten.[263]

Diese Perspektive hatte auch schon die Datenschutzrichtlinie von 1995 eingenommen, wo in Art. 8 Abs. 2 lit. a geregelt ist, dass die Mitgliedstaaten für besondere Kategorien von personenbezogenen Daten eine rechtfertigende Einwilligung

---

260 Art. 29-Datenschutzgruppe, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, 13.9.2001, 5062/01/DE/endg., WP 48, S. 27.

261 Vgl. *Taeger*, in: Taeger/Gabel, Kommentar zum BDSG, 2013, 2. Aufl., § 4a Rn. 62 mit Beispielen, wie etwa die Erteilung einer Magnetkarte für den Firmenparkplatz oder die Ausstellung einer Firmenkreditkarte.

262 Art. 29-Datenschutzgruppe, Stellungnahme 15/2011 zur Definition von Einwilligung, 13. 7. 2011, 01197/11/DE/WP 187, S. 15.

263 *Weichert*, in: Däubler/Klebe/Wedde/Weichert, Kompaktkommentar zum BDSG, 2016, 5. Aufl., § 3 Rn. 65.

ausschließen können. Deutschland hatte davon allerdings keinen Gebrauch gemacht.

bb) Sensible Daten, Art. 9 DS-GVO

Wie die §§ 3 Abs. 9, 4a Abs. 3, 28 Abs. 6–9 BDSG enthält auch Art. 9 DS-GVO Sonderregeln für sensible Daten.[264] Darunter sind im Wesentlichen die AGG-Merkmale sowie genetische und biometrische Daten zu verstehen. Die Erhebung und Verarbeitung derartiger besonderer Daten unterliegt strengeren Voraussetzungen als die Verarbeitung sonstiger Daten. Das gilt auch für das Beschäftigungsverhältnis, was bisher nach dem BDSG ähnlich geregelt ist. Dort gilt, wenn es um sensible Beschäftigtendaten geht, nicht § 32, sondern § 28 Abs. 6–9 BDSG. Nach Art. 9 Abs. 1 DS-GVO dürfen sensible Daten nicht verarbeitet werden. In Abs. 2 sind allerdings zehn Ausnahmen enthalten, so für das Arbeitsrecht Abs. 2 lit. b, wonach für die Erfüllung arbeits- und sozialrechtlicher Zwecke die Verarbeitung von sensiblen Daten gerechtfertigt sein kann, wenn die Mitgliedstaaten das entsprechend vorsehen.

Auch bei sensiblen Daten kann eine Einwilligung des Betroffenen die Erhebung und Verarbeitung rechtfertigen. An die Einwilligung werden aber gemäß Art. 9 Abs. 2 lit. a DS-GVO strengere Voraussetzungen gestellt als sonst. Die Einwilligung muss nicht nur eine „eindeutige bestätigende Handlung sein" (Erwägungsgrund 32), sondern „ausdrücklich" erfolgen. Schriftform wird aber auch hier nicht verlangt.

Gemäß Art. 9 Abs. 4 DS-GVO könnten die Mitgliedstaaten aber bei genetischen, biometrischen oder Gesundheitsdaten ausdrücklich Beschränkungen einführen. Zum Verhältnis von Art. 9 Abs. 4 zu Art. 88 Abs. 1 enthält die DS-GVO nichts. Der Zusammenhang legt aber nahe, dass die beiden Artikel zusammen zu lesen sind mit der Folge, dass die Mitgliedstaaten die Erhebung und Verarbeitung von genetischen, biometrischen und Gesundheitsdaten im Beschäftigungsverhältnis einschränken könnten und folglich auch die Einwilligung dazu. Das gilt im Übrigen auch ohne Rückgriff auf Art. 88 DS-GVO, da Art. 9 Abs. 4 bei genetischen, biometrischen und Gesundheitsdaten für alle Verarbeitungszusammenhänge eine mitgliedstaatliche Einschränkung erlaubt.

Wenn der deutsche Gesetzgeber die nationale Regelungsbefugnis aus Art. 88 Abs. 1 DS-GVO für eine Einschränkung der Einwilligungsbefugnis nicht aufgreift, bleibt es bei den Anforderungen der DS-GVO in Art. 6 Abs. 1 lit. a i. V. m. Art. 7 DS-GVO. Die entsprechen in materieller Hinsicht weitgehend denen in § 4a

---

[264] Zu den sensiblen Daten in Art. 9 DS-GVO s. schon oben E.II.2.d).

BDSG.[265] In formeller Hinsicht dagegen bleibt die DS-GVO z. T. hinter dem BDSG zurück, da keine Schriftform der Einwilligungserklärung verlangt wird.[266]

Bei der letzten, den Beschäftigtendatenschutz betreffenden Datenschutzreform, der Einfügung von § 32 ins BDSG im Jahr 2009, hatte der Gesetzgeber ausdrücklich eine freiwillig erteilte Einwilligung des Beschäftigten durch die Einführung von § 32 nicht ausschließen wollen.[267] Da § 32 BDSG nur eine – im Grunde aus sich heraus weitgehend nichtssagende – Generalklausel ist, muss für die Rechtmäßigkeitsvoraussetzungen einer Einwilligung auf §§ 4, 4a BDSG bzw. ab 2018 auf Art. 4, 6, 7 DS-GVO zurückgegriffen werden. Dem Problem der oft fehlenden Freiwilligkeit im Beschäftigungsverhältnis ist dort nicht ausreichend Rechnung getragen.

Daher sollte die nun wegen der Verabschiedung der DS-GVO erneut bestehende nationale Regelungsmöglichkeit für Beschäftigtendatenschutz dergestalt aufgegriffen werden, dass – endlich – dem Umstand der Asymmetrie im Beschäftigungsverhältnis Rechnung getragen wird und zumindest besonders kritische Kategorien von personenbezogenen Beschäftigtendaten der Einwilligungsbefugnis, die ja in der Praxis faktisch oft eine Einwilligungspflicht ist, entzogen werden.

IV. Handlungsspielraum der Betriebs- und Tarifvertragsparteien

1. Kollektivvereinbarungen als „spezifischere Vorschriften“

Neben Gesetzen, die die Mitgliedstaaten nach Art. 88 Abs. 1 DS-GVO zum Beschäftigtendatenschutz erlassen können, erlaubt die Vorschrift auch „spezifischere Vorschriften“ durch Kollektivvereinbarungen. Im Kommissionsvorschlag war nur nationaler Beschäftigtendatenschutz „per Gesetz“ vorgesehen. Das Europäische Parlament erweiterte auf die Formulierung „durch Rechtsvorschriften“ und ab der Fassung des Rates sind auch Kollektivvereinbarungen enthalten. Neben Tarifverträgen gehören dazu auch ausdrücklich Betriebsvereinbarungen, was Erwägungsgrund 155 klarstellt. Das war im Verhandlungsprozess vor allem ein deutsches Anliegen. Wie bisher können auch unter der DS-GVO kollektive Verträge weiter eine zentrale Rolle für den Beschäftigtendatenschutz spielen. Das bedeutet für Deutschland, dass vor allem Betriebsvereinbarungen ihre Bedeutung für den Beschäftigtendatenschutz behalten können.[268]

---

265 *Wybitul/Pötters*, RDV 2016, 10, 13.
266 *Wybitul/Pötters*, RDV 2016, 10, 12.
267 BT-Drs. 16/13657, S. 20.
268 Zu deren Bedeutung im deutschen Beschäftigtendatenschutz vgl. nur *Kort*, ZD 2016, 3.

Der Wortlaut von Art. 88 Abs. 1 DS-GVO und von Erwägungsgrund 155 sprechen dafür, dass Kollektivverträge ihre Konkretisierungsfunktion schon unmittelbar aus dem EU-Recht beziehen und nicht erst durch mitgliedstaatliche Zuweisung. Daher könnte Beschäftigtendatenschutz auch dann in Kollektivvereinbarungen geregelt werden, wenn der nationale Gesetzgeber von der Regelungsoption in Art. 88 DS-GVO keinen Gebrauch macht. Das ergibt sich insbesondere aus Art. 88 Abs. 3 DS-GVO. Danach muss jeder Mitgliedstaat innerhalb einer Zweijahresfrist der Kommission die „Rechtsvorschriften" melden, die „er" (der Mitgliedstaat) aufgrund von Abs. 1 des Art. 88 erlässt.[269] In Abs. 1 wiederum wird zwischen Rechtsvorschriften, die der Staat erlässt, und Kollektivvereinbarungen unterschieden. Die einzelnen Kollektivvereinbarungen sind also, wie sich aus dem Wortlaut von Art. 88 Abs. 3 ergibt, nicht der Kommission zu melden. Allenfalls wird der Mitgliedstaat der Kommission mitteilen, aufgrund welcher Normen die Kollektivparteien nach nationalem Recht Kompetenzen im Beschäftigtendatenschutz haben. Erforderlich ist das aber nach dem Wortlaut von Art. 88 Abs. 3 DS-GVO nicht.

In diesem Zusammenhang stellt sich die Frage, ob dem Betriebsrat ein Mitbestimmungsrecht für Beschäftigtendatenschutz eingeräumt werden sollte. Wenn weder Staat noch Unternehmen die Rolle des Betriebsrats bei der Regelung von Beschäftigtendatenschutz geschmälert sehen wollen, wäre es angemessen, diese Rolle auf ein klares rechtliches Fundament zu stellen. Nach §§ 75 und 80 BetrVG hat der Betriebsrat allgemein die Aufgabe, die Einhaltung von Datenschutzvorschriften zu überwachen. Ein ausdrückliches Mitbestimmungsrecht in Angelegenheiten des Datenschutzes gibt es dagegen nicht. Der bisher für erzwingbare Datenschutzbetriebsvereinbarungen von der Rechtsprechung herangezogene § 87 Abs. 1 Nr. 6 BetrVG ist nicht für Datenschutzzusammenhänge konzipiert – die Vorschrift stammt aus einer Zeit als es das Internet noch nicht gab – und deckt daher die Materie nur z. T. ab, da technische Überwachungseinrichtungen des Unternehmens Anknüpfungspunkt für die Mitbestimmung sind. Allerdings kann „Überwachung" weit verstanden werden.[270] Darüber hinaus können datenschutzrechtliche Betriebsvereinbarungen nur freiwillig nach § 88 BetrVG abgeschlossen werden. Es wäre also an eine Erweiterung von § 87 Abs. 1 Nr. 6 BetrVG zu denken, indem nicht nur an die Überwachung des Arbeitnehmers angeknüpft wird, sondern an die Nutzung von Daten, die sich einem Arbeitnehmer zuordnen lassen.[271] Eine moderne Formulierung bzw. Ergänzung von § 87 Abs. 1 Nr. 6

---

269 Dazu schon oben E.II.2.e).

270 Vgl. zum Mitbestimmungsrecht z. B. DKKW-*Klebe*, BetrVG, § 87 Rn. 175 ff., 194 ff., 201 f.

271 DKKW-*Klebe*, BetrVG, § 87 Rn. 187.

BetrVG wäre auch deshalb wünschenswert, weil es nicht Aufgabe des Betriebsrats sein kann, neue Technologien zu behindern, sondern nur deren Missbrauch zu verhindern. Ebenfalls angepasst werden müsste § 94 BetrVG.

Der Regelungsspielraum in den Katalogen des Art. 88 Abs. 1 DS-GVO und Erwägungsgrund 155 umfasst die Verarbeitung von Beschäftigtendaten bei der Einstellung, der Erfüllung und Beendigung des Arbeitsvertrages, der Gesundheit und Sicherheit am Arbeitsplatz oder Gleichheit und Diversität am Arbeitsplatz. Diese Aspekte dürften auch in Tarifverträgen geregelt werden, die aber für den Datenschutz in Deutschland bislang keine Rolle gespielt haben und das wohl auch in Zukunft nicht tun werden. Entsprechend hat Deutschland bei den Verhandlungen Wert auf die ausdrückliche Aufnahme von Betriebsvereinbarungen (im Erwägungsgrund 155) gelegt, die daher auch ab 2018, da es sich um ein eingespieltes Modell handelt, das kollektive Mittel der Wahl sein werden.

Alte Betriebsvereinbarungen zum Beschäftigtendatenschutz können ggf. nicht umstandslos weitergelten. Grundsätzlich gilt, dass Betriebsvereinbarungen als Erlaubnistatbestand für Datenverarbeitung jedenfalls die Anforderungen der DS-GVO als Mindestanforderung für den Beschäftigtendatenschutz einhalten müssen.[272] Genauer sind für den Beschäftigtendatenschutz die Voraussetzungen in Art. 88 Abs. 2 DS-GVO geregelt. Auch Betriebsvereinbarungen dürfen nicht gegen die Menschenrechte, die berechtigten Interessen und die Grundrechte der von der Datenverarbeitung betroffenen Personen verstoßen. Diese Vorgaben entsprechen im Wesentlichen § 75 Abs. 2 Satz 1 BetrVG. Art. 88 Abs. 2 erwähnt hier als besonders brisante Verarbeitungszusammenhänge die Beschäftigtendatenübermittlung im Konzern und Überwachungssysteme am Arbeitsplatz. Halten sich Betriebsvereinbarungen nicht an diesen Rahmen, können sie ab dem 25. 5. 2018 wegen der unmittelbaren Wirkung der Verordnung nicht mehr als Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten herangezogen werden.

In diesem Zusammenhang ist auch ein kritischer Blick auf die BAG-Rechtsprechung erforderlich, nach der Betriebsvereinbarungen zum Beschäftigtendatenschutz partiell vom BDSG auch „nach unten" abweichen dürfen. In der Literatur ist die Frage umstritten.[273] Das BAG hat zwar die Tendenz erkennen lassen, dass das möglich sein kann,[274] aber darauf hingewiesen, dass Betriebsrat und

---

272 So auch *Wybitul/Sörup/Pötters*, ZD 2015, 559, 561.

273 Zur Darstellung der widersprüchlichen Ansichten vgl. *Thüsing/Granetzny*, Beschäftigtendatenschutz und Compliance, 2014, 2. Aufl., § 4 Rn. 5 f. m. w. N.

274 Schon BAG, NZA 1986, 643, bestätigt in BAG 25. 9. 2013, NZA 2014, 41; kritisch *Seifert*, in Simitis (Hrsg.), BDSG, Kommentar, 2014, 8. Aufl., § 32 Rn. 167 m. w. N.

Arbeitgeber jedenfalls gemäß § 75 Abs. 2 BetrVG die Persönlichkeitsrechte der Arbeitnehmer und das Verhältnismäßigkeitsprinzip wahren müssen, so dass die negative Abweichung vom BDSG nicht sehr weitreichend sein kann. Aber was heißt das konkret für die Änderung von Verarbeitungszwecken, die Ausgestaltung der Auftragsdatenverarbeitung, die Umsetzung von Binding Corporate Rules oder die Festsetzung von Löschungsfristen?

Für die negative Abweichung von Betriebsvereinbarungen von der DS-GVO ist die Lage vordergründig klar: Von den strengen Prinzipien in Art. 88 Abs. 2 sowie sonstigen Prinzipien der DS-GVO darf nicht „nach unten" abgewichen werden.[275] Allerdings enthält die DS-GVO nicht in jedem Fall strenge Grundsätze. Beim Datentransfer in Drittländer etwa bietet die DS-GVO nicht viel mehr Schutz für die Betroffenen als nach geltendem Recht,[276] also sehr wenig. Zwar gibt es Beispiele für Datenschutzverträge, aber nicht selten sind Betriebsräte hier in der Defensive. Darüber hinaus ist grundsätzlich zu bedenken, dass Art. 88 DS-GVO bei aller Strenge in Abs. 2 keineswegs nur den Schutz der Betroffenen im Sinn hat, sondern auch eine Reihe von Kontrollmöglichkeiten abdeckt. Das ergibt sich aus der Formulierung wie der Systematik der DS-GVO. Die enthält nicht ausschließlich eine Grundrechtsgewährleistung, sondern gleichgewichtig das Prinzip des freien Datenverkehrs, wie bereits die Formulierung von Art. 1 Abs. 3 DS-GVO zeigt.[277] Auch Art. 88 DS-GVO ist nicht ausschließlich eine Schutzvorschrift für Beschäftigte. Schon Abs. 1 formuliert, dass spezifischere nationale Vorschriften zum Schutz von Rechten, aber auch zum Schutz von Freiheiten bei der Verarbeitung von Beschäftigtendaten erlassen werden können. Entsprechende Betriebsvereinbarungen würden sich dann durchaus noch im Rahmen der Verordnung bewegen. Auch deshalb ist eine Erweiterung der datenschutzrechtlichen Betriebsratsrechte im BetrVG erforderlich.

2. Verbandsklagerecht, Art. 80 DS-GVO

Grundsätzlich ist ein Verbandsklagerecht ein wichtiges Instrument für die Stärkung des Datenschutzes, das schon länger gefordert wird,[278] denn der Betroffene ist oft nicht selbst zur Informationsbeschaffung gegenüber Unternehmen in der

---

275 So auch in aller Deutlichkeit *Kort*, NZA 2016 (erscheint demnächst), I.8.c); *Wybitul*, BB 2/2016. Die erste Seite, sieht immerhin einigen Anpassungsbedarf bei der Transparenz von durch Betriebsvereinbarung gerechtfertigter Datenverarbeitung; vgl. auch DKKW-*Klebe*, BetrVG, § 87 Rn. 195f.

276 Dazu schon oben C.VIII.

277 Dazu auch schon oben E.II.2.b).

278 *Dieterich*, ZD 2016, 260, 265 m. w. N.

Lage und mit dem Prozessrisiko überfordert. Auch vor dem Hintergrund der begrenzten Kapazitäten der Aufsichtsbehörden ist ein solches Recht für die Durchsetzung datenschutzrechtlicher Vorschriften wichtig.[279]

Art. 80 Abs. 1 DS-GVO über die Vertretung von betroffenen Personen vor Aufsichtsbehörden und Gerichten ist für den allgemeinen Datenschutz konzipiert und hat weder Gewerkschaften noch Betriebsräte im Blick. Es geht bei Art. 80 Abs. 1 um eine Prozessführungsbefugnis, die Einrichtungen, Organisationen oder Vereinigungen ohne Gewinnerzielungsabsicht ausüben können, deren satzungsmäßige Ziele im öffentlichen Interesse liegen und die im Bereich Datenschutz tätig sind. Für jede einzelne Tätigkeit, die derartige Organisationen für Betroffene ausüben, müssen sie von diesen ausdrücklich beauftragt sein.

Der Betriebsrat kommt als Organisation i. S. v. Art. 80 Abs. 1 DS-GVO nicht in Betracht. Zwar hat er gemäß § 80 Abs. 1 Nr. 1 BetrVG auch die Aufgabe, die Einhaltung der Datenschutzbestimmungen im Betrieb zu überwachen. Der nicht rechtsfähige Betriebsrat ist aber erkennbar nicht als „Einrichtung, Organisation oder Vereinigung" i. S. v. Art. 80 Abs. 1 DS-GVO gemeint. Das Erfordernis einer Satzung, deren Ziel auf den Datenschutz gerichtet ist, wird auch nicht durch die allgemeinen Aufgaben aus dem BetrVG ersetzt.

Gewerkschaften könnten eher Organisationen i. S. v. Art. 80 Abs. 1 DS-GVO sein. I. d. R. ergibt sich aber aus ihrer Satzung nicht die Förderung von Datenschutz. Das lässt sich zwar ändern, macht aus ihnen aber dennoch nicht die in Art. 80 Abs. 1 anvisierten Organisationen. Es wäre aber denkbar, entsprechende „Einrichtungen, Organisationen oder Vereinigungen" mit dem Zweck Beschäftigtendatenschutz zu fördern, durch Gewerkschaften neu zu gründen.

Das wäre vor allem dann lohnend, wenn Deutschland von der Regelungsbefugnis in Art. 80 Abs. 2 DS-GVO Gebrauch machen und ein Verbandsklagerecht in Angelegenheiten des Beschäftigtendatenschutzes einführen würde. Art. 80 Abs. 2 DS-GVO ist auch, wie schon die Bußgeldregelungen in der DS-GVO, dem Kartellrecht entlehnt (vgl. § 33 Abs. 2 GWB) und ermöglicht nationale Regelungen für die in Art. 80 Abs. 1 DS-GVO genannten Einrichtungen, Organisationen oder Vereinigungen auch unabhängig von einem Auftrag der betroffenen Person tätig zu werden. Art. 80 Abs. 2 geht nicht zuletzt auf eine deutsche Initiative zurück, da der deutsche Gesetzgeber erst im Februar 2016 die Verbandsklage bei Datenschutzverstößen in § 2 Abs. 2 Satz 1 Nr. 11 UKlaG erweitert hat und wohl erhalten möchte.

---

279 A. a. O.

§ 2 Abs. 2 Satz 1 Nr. 11 UKlaG betrifft allerdings weder den Datenschutz allgemein noch den Beschäftigtendatenschutz im Besonderen. Das Unterlassungsklagengesetz wurde im Rahmen der Schuldrechtsreform von 2002 erlassen und dient vorwiegend dem Verbraucherschutz vor unzulässigen allgemeinen Geschäftsbedingungen. Zu diesem Zweck sieht das Gesetz ein Verbandsklagerecht auf Unterlassung, Widerruf und Beseitigung vor. Die nach § 4 i. V. m. § 3 UKlaG aktivlegitimierten Stellen kommen vor allem aus dem Mieter- und Verbraucherschutz und sind beim Bundesamt für Justiz registriert. Für das Arbeitsrecht gilt das UKlaG gemäß § 15 ausdrücklich nicht.

Seit 24. 2. 2016 ist die Verbandsklagebefugnis teilweise auch auf Datenschutzverstöße ausgedehnt worden, indem gemäß § 2 Abs. 2 Satz 1 Nr. 11 auch die Erlaubnisregelung für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten eines Verbrauchers den durch das UKlaG geschützten Verbraucherschutzgesetzen zugerechnet werden, d. h. die Vorschrift dient der besseren zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts.[280] Das ist für den formell-rechtlichen Datenschutz ein großer Fortschritt, da auch die Gerichte häufig entschieden hatten, Datenschutzrecht sei kein Verbraucherschutzrecht.[281] Das hing nicht zuletzt mit dem Ursprung des Datenschutzes im „Recht auf informationelle Selbstbestimmung" zusammen, das Teil des Persönlichkeitsrechts jedes Einzelnen ist und nicht mit dessen Funktion als Wirtschaftssubjekt zu tun hat.[282]

Eine vollständige Einbeziehung des Datenschutzrechts in das Verbandsklagerecht des UKlaG bedeutet die Neuregelung aber nicht, denn sie erkennt Datenschutzrecht als Verbraucherschutzrecht nur insoweit an als es um kommerzielles Handeln zwischen Unternehmern und Verbrauchern geht.[283] Allerdings könnte man hier erwägen, den Umstand zu akzeptieren, dass personenbezogene Daten in den meisten der nicht öffentlichen Verarbeitungszusammenhänge ohnehin längst zu Gütern geworden sind, um deren Verwertung es geht. Diese Position hatte schon die DS-Richtlinie eingenommen und nimmt auch die DS-GVO ein.[284] Datenschutz wäre dann jedenfalls auch Verbraucherschutz.

Um diese neue Regelung im UKlaG zu erhalten, hat Deutschland für die Öffnung in Art. 80 Abs. 2 DS-GVO plädiert. Sie schließt nicht aus, das nationale Verbands-

280 BGBl. I 2016, 233.
281 *Köpernik*, VuR 2014, 240.
282 *Halfmeier*, NJW 2016, 1126, 1127.
283 *Halfmeier*, a. a. O.
284 Zum hybridhaften Charakter des europäischen Datenschutzrechts ausführlich: *Lynskey*, The Foundations of EU Data Protection Law, Oxford 2015, insbes. S. 46 ff.

klagerecht nochmals zu erweitern und es auch zum Schutz von Beschäftigtendaten zu installieren. Dafür gilt die gleiche Diagnose wie für verbraucherbezogene Datenschutzprobleme: gerade aufgrund der zu erwartenden neuen Unklarheiten durch die über weite Strecken mit Generalklauseln arbeitende DS-GVO ist die Rechtsdurchsetzung und Rechtsfortbildung mit Hilfe der Verbandsklage notwendig[285] und sollte auch in einem Beschäftigtendatenschutzgesetz geregelt werden.

[285] *Halfmeier*, a. a. O., S. 1129.

F. Ergebnisse und Schlussfolgerungen

I. Allgemeine Ziele der DS-GVO

Die DS-GVO ist im materiellen Datenschutzrecht im Wesentlichen alter Wein in neuen Schläuchen, weshalb die Grundverordnung auch kein neues Datenschutzkonzept bereithält und schon gar kein Meilenstein in der Entwicklung des Datenschutzes ist,[286] wenn man von dem nicht zu unterschätzenden Umstand absieht, dass nach der DS-Richtlinie von 1995 überhaupt eine für alle EU-Staaten unmittelbar geltende Regelung zustande gekommen ist und ab dem 25. 5. 2018 jedenfalls im Prinzip in allen Mitgliedstaaten ein einheitliches Datenschutzrecht gelten wird. Wenn auch nicht aufgrund neuer Konzepte, so doch hinsichtlich der Regelungsebene stellt die DS-GVO also dennoch die wichtigste Rechtsänderung im Datenschutzrecht der letzten 20 Jahre dar.

Allerdings anders als ursprünglich von der Kommission geplant, schafft die DS-GVO nur teilweise einheitliches Datenschutzrecht innerhalb der EU. Durch die mehr als 30 Öffnungsklauseln erreicht die an sich unmittelbar geltende Verordnung möglicherweise sogar weniger Harmonisierungswirkung als die DS-Richtlinie von 1995, der der EuGH auch schon eine Harmonisierungspflicht entnommen hatte, insoweit Regelungen nach oben jedenfalls seit der jüngeren ASNEF-Entscheidung[287] nicht möglich sein sollen. Das ist bei den Öffnungsklauseln der DS-GVO z. T. anders, insbesondere beim Beschäftigtendatenschutz, wo in Art. 88 Abs. 1 gerade die im ursprünglichen Entwurf enthaltene Einschränkung, dass nur „im Rahmen der Verordnung" national geregelt werden durfte, in der verabschiedeten Fassung entfallen ist, was strengere nationale Regeln für den Beschäftigtendatenschutz ermöglicht.

Auch sehr viel „moderner", wie von der DS-GVO angestrebt, ist der Datenschutz durch die Verordnung nicht geworden, denn die seit über 45 Jahren auf der Basis ganz anderer Verarbeitungsbedingungen entwickelten Grundsätze, wie das Verbot mit Erlaubnisvorbehalt oder der Zweckbindungsgrundsatz werden beibehalten und nur punktuell ergänzt. Auch Technikneutralität kann ein Rechtsakt wie die DS-GVO angesichts der Ungewissheit der weiteren technischen Entwicklung

---

286 So aber *Dammann*, ZD 2016, 307, 314.

287 EuGH, Urt. v. 24. 11. 2011 – C-468/10, RDV 2012, 22 (ASNEF).

nicht gewährleisten. Neue Datenverarbeitungsformen und mit diesen verbundene neue wirtschaftliche Nutzungsmöglichkeiten personenbezogener Daten, wie etwa Big Data-Auswertungen, spricht die DS-GVO gar nicht erst an bzw. könnte sie sogar versteckt in der Zweckänderungsvorschrift des Art. 6 Abs. 4 DS-GVO i. V. m. Erwägungsgrund 50 erlauben.

Trotz der vertrauten Struktur im materiellen Datenschutzrecht kann nicht damit gerechnet werden, dass ab dem 25. 5. 2018 in den EU-Mitgliedstaaten tatsächlich einheitliches Datenschutzrecht praktiziert werden wird. Auch da, wo in der DS-GVO kein Raum für nationale Regelungen gelassen ist, arbeitet die Verordnung weitgehend mit Generalklauseln und unbestimmten Rechtsbegriffen, die in den, wenn auch längeren, so doch häufig ebenso vagen Erwägungsgründen nur bedingt rechtssicher erhellt werden. Daher wird es auf Jahre hinaus der nationalen Rechtsprechung überlassen bleiben, die Generalsklauseln der DS-GVO vor dem Hintergrund von 28 verschiedenen Rechtstraditionen und rechtsdogmatischen Auslegungssystemen zu interpretieren und nur in Einzelfällen wird der EuGH zu Klarstellungen Gelegenheit haben.

Darüber hinaus bleibt es bei der brisanten Übermittlung von personenbezogenen Daten an Drittstaaten im Wesentlichen beim geltenden – ineffizienten – Recht (C.VIII.).

Bleibt im materiellen allgemeinen Datenschutzrecht im Grundsatz also vieles beim alten, so enthält die DS-GVO auf der Verfahrensseite vor allem die Neuerung, dass durch das Marktortprinzip in Zukunft eine extraterritoriale Wirkung der EU-Regelung erzielt wird. Auch die Aufsicht ist so angelegt, dass sie durch den neu einzurichtenden Europäischen Datenschutzausschuss zu einer einheitlichen Anwendung der DS-GVO in allen Mitgliedstaaten führen soll. Hier ist allerdings fraglich, ob sich das von vielen gepriesene Kohärenzverfahren als effizient und nicht doch als bürokratischer Moloch entpuppen wird. Jedenfalls hat der deutsche Gesetzgeber die Mammutaufgabe, das sehr differenzierte deutsche Datenschutzrecht der Verordnung anzupassen.[288]

Grundsätzlich gilt, dass der Datenschutz umso mehr „dead letter law" bleibt als er generell-abstrakt für alle denkbaren Verarbeitungszusammenhänge geregelt wird und die Aufsicht schwerfällig ist.

---

[288] Vgl. dazu das im August 2016 erschienene umfangreiche Rechtsgutachten für das auf der Bundesebene für Datenschutz federführende Bundesministerium des Inneren von Prof. Kühling/Heberlein sowie einem Team um Prof. Martini im Programmbereich „Digitalisierung" am Deutschen Forschungsinstitut für öffentliche Verwaltung Speyer: *Kühlung/Martini et al.*, Die Datenschutz-Grundverordnung und das nationale Recht, 2016, als PDF-Dokument unter *http://www.foev-speyer.de* herunterladbar.

II. Beschäftigtendatenschutz

1. Für den Beschäftigtendatenschutz stellt sich die Lage besser dar als nach der Vorlage des ersten DS-GVO-Entwurfs der Kommission von 2012 zu erwarten war, da deutlich mehr nationale Regelungskompetenz auf diesem Gebiet erhalten wurde als im Kommissionsentwurf. Beschäftigtendatenschutz sollte zwar schon nach der Vorstellung der Kommission auch national geregelt werden dürfen, aber nur „im Rahmen der Verordnung". Nachdem dieser Passus entfallen ist, ist der nationale Regelungsspielraum viel weiter, wenn sich auch die Mitgliedstaaten nicht vollständig von den Grundprinzipien der Verordnung entfernen dürfen. Nationale Abweichungen „nach unten" sind also nicht möglich, „nach oben" dagegen erlaubt, wobei aber dem Hybridcharakter der DS-GVO – sie enthält den Schutz personenbezogener Daten des Einzelnen und will den freien Verkehr dieser Daten gewährleisten – Rechnung getragen werden muss (E.II.2.b und c).

2. Die vermeintlichen Einschränkungen in Art. 88 Abs. 2 DS-GVO – Menschenwürde, weitere Grundrechte der betroffenen Personen, Transparenz – ergeben sich ohnehin schon aus nationalem Verfassungsrecht und bedeuten keine darüber hinausgehende Einengung des nationalen Gesetzgebers.

3. Art. 88 Abs. 3 DS-GVO enthält eine Mitteilungspflicht, jedoch keine Ausschlussfrist. Auch bei einer zunächst nur reinen Fortschreibung von § 32 BDSG könnte später noch eine detaillierte Regelung zum Beschäftigtendatenschutz erlassen werden (E.II.2.e).

4. Der in der DS-GVO verwendete Beschäftigtenbegriff ist europäisch zu interpretieren (E.II.2.a).

5. Eine nationale Regelung des Beschäftigtendatenschutzes ist nicht nur möglich, sondern erforderlich, da die DS-GVO diesen Bereich nahezu vollständig den Mitgliedstaaten überlässt und die allgemeinen Regeln der DS-GVO im Wesentlichen nicht einmal den Standard von § 32 BDSG gewährleisten würden.

6. Eine nationale Regelung des Beschäftigtendatenschutzes muss die Mindeststandards der DS-GVO einhalten, ist aber „nach oben" offen. Das ergibt sich u. a. aus der Genese von Art. 88 DS-GVO. Die ursprünglich vorgesehene Einschränkung, dass mitgliedstaatliche Regelungen zum Beschäftigtendatenschutz nur „im Rahmen der Verordnung" erfolgen dürfen, ist ausdrücklich nicht in die verabschiedete Version übernommen worden.

7. Eine (erweiterte) Fortgeltung von § 32 BDSG wäre nur eine „kleine Lösung" i. S. v. Art. 88 DS-GVO und wäre als Erklärung aufzufassen, die vielfältigen

Besonderheiten des Beschäftigtendatenschutzes gerade nicht regeln zu wollen.

Eine reine Fortgeltung des derzeitigen § 32 BDSG würde den Vorgaben von Art. 88 DS-GVO nicht entsprechen, da die Regelungen nach Art. 88 Abs. 1 DS-GVO „spezifisch", d. h. nicht generalklauselartig sein müssen und Art. 88 Abs. 1 dafür ausdrücklich beispielhaft Bereiche nennt, die jedenfalls geregelt werden sollen.

Diesen (einfachsten) Weg hat allerdings ein erster, noch nicht abgestimmter – und vom BMJV scharf kritisierter[289] – Entwurf des Bundesministeriums des Inneren (BMI)[290] zunächst gewählt. Er schöpft den Spielraum, den die DS-GVO im Beschäftigtendatenschutz einräumt, nicht ansatzweise aus, sondern begnügt sich im Wesentlichen mit der Fortschreibung des Status quo des § 32 BDSG.[291] Das würde aber eine Verschlechterung bedeuten, da etliche bereichsspezifische Einzelregelungen im deutschen Recht, die auch das Beschäftigungsverhältnis betreffen, ab 2018 nicht mehr gelten werden, da für diese Bereiche die DS-GVO keine Öffnungsklauseln für nationale Regelungen enthält. An ihre Stelle treten dann (nur) die allgemeinen Regeln der DS-GVO.

8. Wünschenswert und europarechtlich möglich ist eine längst überfällige, umfassende gesetzliche Regelung des Beschäftigtendatenschutzes in einem eigenen Gesetz, da die DS-GVO als ein allgemeines Datenschutzinstrument für alle denkbaren Verarbeitungsformen den Besonderheiten der Datenverarbeitung im Beschäftigungskontext nicht gerecht werden kann. Hier besteht auch eine Schutzpflicht des Staates, das verfassungsrechtlich

---

289 40-seitige BMJV Stellungnahme vom 31. 8. 2016 zu einem Datenschutzanpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU, abrufbar unter: *https://netzpolitik.org//wp-upload/2016/09/BMJV_Stellungnahme_DSAnpUG_EU.pdf*.

290 Der Entwurf wurde nicht offiziell veröffentlicht, kursiert aber so breit gestreut im Netz, dass er hier zitiert werden kann: Referentenentwurf des Bundesministeriums des Inneren – Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Datenschutz-Grundverordnung und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU), Vorschlag des BMI für die 1. Ressortabstimmung vom 5. 8. 2016: *https://netzpolitik.org//wp-upload/2016/09/Referentenentwurf_DSAnpUG_EU.pdf*.

291 In dieser Richtung auch kurz *Thüsing*, BB 2016, 2165 f., der immerhin die handwerkliche Qualität des BMI-Vorschlags lobt. Auch die bestreitet das BMJV allerdings vehement („nicht verständlich"; „widersprüchliche Formulierungen"; „sollte grundlegend überarbeitet werden" u. Ä.). Auch die Bundesbeauftragte für den Datenschutz hält den Entwurf für „verfehlt und weitgehend misslungen", abrufbar unter: *https://netzpolitik.org//wp-upload/2016/09/BfDI_Stellungnahme_DSAnpUG_EU.pdf*, S. 4.

gewährleistete Recht auf informationelle Selbstbestimmung effizient in Gesetzgebung umzusetzen.

9. Sensible Daten sind in Art. 9 DS-GVO besonders geschützt. Art. 9 Abs. 4 weist darauf hin, dass sich eine nationale Regelung i. S. v. Art. 88 DS-GVO an Art. 9 orientieren muss. Allerdings enthält Art. 9 eine Ausnahme für die Verarbeitung sensibler Daten für arbeits- und sozialrechtliche Zwecke. Ausdrücklich sind aber nationale Regelungen für die Einschränkung der Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten zulässig (E.II.2.d und E.II.4.d)bb).

10. Auch die Reichweite der Einwilligung kann im Beschäftigungskontext national geregelt, also auch eingeschränkt werden. Das ist angesichts der Asymmetrie im Beschäftigungsverhältnis erforderlich, da häufig nicht von der Freiwilligkeit einer Einwilligung ausgegangen werden kann. Jedenfalls kann schon aus der DS-GVO selbst ein Koppelungsverbot abgelesen werden (E.III.4.c). Ein solches Verbot ist aber nicht ausreichend, um die freie Entscheidung der Betroffenen zu gewährleisten.

11. Die deutsche Regelung zum betrieblichen Datenschutzbeauftragten kann aufrechterhalten werden und sollte ergänzt werden (E.II.3.).

12. Datenschutz durch Technik ist ein wichtiger Grundsatz, der in der DS-GVO nur vage geregelt ist. Er sollte in einer nationalen Regelung stärker betont und konkretisiert werden. Gleichzeitig darf Datenschutz durch Technik den materiellen Datenschutz nicht ersetzen, sondern sollte ihn ergänzen (E.II.4.).

13. Ein Konzernprivileg enthält die DS-GVO nicht (E.II.5.).

14. Die Rolle der Kollektivparteien, insbesondere des Betriebsrats bleibt für den Beschäftigtendatenschutz weiterhin zentral. Ggf. wäre an die Einführung eines Mitbestimmungsrechts für Beschäftigtendatenschutz zu denken (E.IV.1.).

15. Ein Verbandsklagerecht im Beschäftigtendatenschutz könnte eingeführt werden (E.IV.2.).

Literaturverzeichnis

Albrecht, Jan Philipp, Die EU-Datenschutzgrundverordnung rettet die informationelle Selbstbestimmung! Ein Zwischenruf für einen einheitlichen Datenschutz durch die EU, ZD 2013, 587–590.

Albrecht, Jan Philipp, Das neue EU-Datenschutzrecht, CR 2016, 88–98.

Ashkar, Daniel, Durchsetzung und Sanktionierung des Datenschutzrechts nach den Entwürfen der Datenschutz-Grundverordnung, DuD 2015, 796–800.

Benner, Christiane, Crowdwork – zurück in die Zukunft? Perspektiven digitaler Arbeit, Frankfurt a.M., 2015.

Bittner, Timo, Der Datenschutzbeauftragte gemäß EU-Datenschutz-Grundverordnungs-Entwurf, RDV 2014, 183–189.

Boeken, Winfried/Düwell, Franz Josef/Diller, Martin/Hanau, Hans (Hrsg.), Gesamtes Arbeitsrecht, 2016 (NomosKommentar: NK-GA).

Buchner, Benedikt, Informationelle Selbstbestimmung im Privatrecht, Tübingen, 2006.

Buchner, Benedikt, Die Einwilligung im Datenschutzrecht, DuD 2010, 39–43.

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

Bundesministerium für Arbeit und Soziales (Hrsg.), Grünbuch – Arbeiten 4.0, Berlin, 2015.

Calliess, Christian/Ruffert, Matthias, EUV/AEUV, Kommentar, 5. Aufl., München, 2016.

Cate, Fred, The Failure of Fair Information Practice Principals, in: Winn, Jane (Hrsg.), Consumer Protection in the Age of the "Information Economy", Ashgate, 2006.

Dammann, Ulrich, Erfolge und Defizite der EU-Datenschutzgrundverordnung, ZD 2016, 307–314.

Däubler, Wolfgang, Internet und Arbeitnehmerdatenschutz, AiB extra 2015, 29 – 32.

Däubler, Wolfgang, Gläserne Belegschaften, 6. Aufl., Frankfurt am Main, 2015.

Däubler, Wolfgang, Digitalisierung und Arbeitsrecht, SR Sonderausgabe Juli 2016.

Däubler, Wolfgang/Klebe, Thomas, Crowdwork: Die neue Form der Arbeit - Arbeitgeber auf der Flucht?, NZA 2015, 1032–1041.

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo, Kompaktkommentar zum BDSG, 5. Aufl., Frankfurt a.M., 2016.

Däubler, Wolfgang/Kittner, Michael/Klebe, Thomas/Wedde, Peter, Betriebsverfassungsgesetz, 15. Aufl. 2016 („DKKW").

Dederer, Hans-Georg, Die Grenzen des Vorrangs des Unionsrechts – Zur Vereinheitlichung von Grundrechts-, Ultra-vires- und Identitätskontrolle, JZ 2014, 313.

Diedrich, Kay, Vollharmonisierung des EU-Datenschutzrechts – bereits geltende Vorgaben für deutsche Datenschutzgesetze. Maßstäbe für richtlinienkonforme Auslegung und Anwendbarkeit nach EuGH ASNEF/FECEMD vom 24.11.2011, CR 2013, 408–412.

Dieterich, Thomas, Rechtsdurchsetzungsmöglichkeiten der DS-GVO, ZD 2016, 260–266.

Dix, Alexander, Datenschutzaufsicht im Bundesstaat – ein Vorbild für Europa, DuD 2012, 318–321.

Düwell, Franz Josef/Brink, Stefan, Die EU-Datenschutz-Grundverordnung und der Beschäftigtendatenschutz, NZA 2016, 665–668.

Faust, Sebastian/Spittka, Jan/Wybitul, Tim, Milliardenbußgelder nach der DS-GVO? Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz, ZD 2016, 120–125.

Forst, Gerrit, Wer ist „Beschäftigter" i. S. d. § 3 Abs. 11 BDSG?, RDV 2014, 128–136.

Franck, Lorenz, System der Betroffenenrechte nach der Datenschutz-Grundverordnung (DS-GVO), RDV 2016, 111–119.

Franzen, Martin/Gallner, Inken/Oetker, Hartmut, Kommentar zum europäischen Arbeitsrecht, München, 2016.

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

Giesen, Richard/Junker, Abbo/Rieble, Volker, Industrie 4.0 als Herausforderung des Arbeitsrechts, ZAAR Schriftenreihe, Band 39, München, 2016.

Gola, Peter, Beschäftigtendatenschutz und EU-Datenschutz-Grundverordnung, EuZW 2012, 332–336.

Gola, Peter/Pötters, Stephan/Thüsing, Gregor, Art. 82 DSGVO, Öffnungsklausel für nationale Regelungen zum Beschäftigtendatenschutz – Warum der deutsche Gesetzgeber jetzt handeln muss, RDV 2016, 57–61.

Gola, Peter/Schomerus, Rudolf, Bundesdatenschutzgesetz. BDSG, Kommentar, 12. Aufl., München, 2015.

Gola, Peter/Schulz, Sebastian, Der Entwurf für eine EU-Datenschutz-Grundverordnung – eine Zwischenbilanz, RDV 2013, 1–7.

Grabitz, Eberhard/Hilf, Meinhard/Nettersheim, Martin, Das Recht der Europäischen Union, München, 58. Ergl., Stand: Januar 2016.

Grau, Timon/Grantzny, Thomas, EU-US-Privacy Shield – Wie sieht die Zukunft des transatlantischen Datenverkehrs aus?, NZA 2016, 405–410.

Grimm, Dieter, Der Datenschutz vor einer Neuorientierung, JZ 2013, 585–592.

Groeben von der, Hans/Schwarze, Jürgen/Hatje, Armin, Europäisches Unionsrecht, 7. Aufl., Baden-Baden, 2015.

Härting, Niko/Schneider, Jochen, Das Ende des Datenschutzes – es lebe die Privatsphäre, CR 2015, 819–827.

Halfmeier, Axel, Die neue Datenschutzverbandsklage, NJW 2016, 1126–1129.

Hayen, Ralf-Peter, „Der Kampf wird sich lohnen", Interview in: CuA 3/2016, 20–23.

Heuschmid, Johannes, Anm. zu EuGH, Urt. v. 17. 3. 2015 – C-533/13, HSI-Newsletter 1/2015, II.

Hirsch, Nadja, Stellungnahme vom 4. 3. 2013 zum Kommissionsentwurf, C7-0025/2012 – 2012/0011 (COD).
Hirsch, Nadja, Eine Datenschutz-Grundverordnung für Europa? Licht und Schatten im Kommissionsentwurf vom 25. 1. 2012, ZD 2012, 99–106.
Jaspers, Andreas/Reif, Yvette, Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung: Bestellpflicht, Rechtsstellung und Aufgaben, RDV 2016, 61–68.
Keppeler, Lutz, Was bleibt vom TMG-Datenschutz nach der DS-GVO? Lösung und Schaffung von Abgrenzungsproblemen im Multimedia-Datenschutz, MMR 2015, 779.
Kingreen, Thorsten, Die Grundrechte des Grundgesetzes im europäischen Grundrechtsföderalismus, JZ 2013, 801–811.
Kingreen, Thorsten/Kühling, Jürgen, Weniger Schutz durch mehr Recht: Der überspannte Parlamentsvorbehalt im Datenschutzrecht – Eine Problemskizze am Beispiel des Gesundheitsdatenschutzrechts –, JZ 2015, 213–221.
Klebe, Thomas, Crowdwork: Faire Arbeit im Netz?, AuR 2016, 277–281.
Klein, Florian/Roos, Philipp, Videoüberwachung: Kostspielige Folgen für den Arbeitgeber?, ZD 2016, 65–72.
Klug, Christoph, Der Datenschutzbeauftragte in der EU – Maßgaben der Datenschutzgrundverordnung, ZD 2016, 315–319.
Köpernik, Kristin, Zur Notwendigkeit einer Verbandsklage bei Datenschutzverstößen, VuR 2014, 240–242.
Körner, Marita, Informierte Einwilligung als Schutzkonzept, in: Simon, Dieter/Weiss, Manfred (Hrsg.), Zur Autonomie des Individuums, Liber Amicorum Spiros Simitis, Baden-Baden, 2000, S. 131–150.
Körner, Marita, Moderner Datenschutz für die Beschäftigten: Ein Ende der Skandale? Gutachten zum Regierungsentwurf zur Regelung des Beschäftigtendatenschutzes im Auftrag des Hugo Sinzheimer Instituts für Arbeitsrecht, Frankfurt a.M., 2010 (*http://www.hugo-sinzheimer-institut.de/veroeffentlichungen/hsi-working-paper.html*).
Körner, Marita, Regierungsentwurf zum Arbeitnehmerdatenschutz, AuR 2010, 416–421.
Körner, Marita, Die Reform des EU-Datenschutzes - Der Entwurf einer EU-Datenschutz-Grundverordnung (DS-GVO) – Teil I, ZESAR 2013, 99–107.
Körner, Marita, Die Reform des EU-Datenschutzes – Der Entwurf einer EU-Datenschutz-Grundverordnung (DS-GVO) – Teil II, ZESAR 2013, 153–159.
Kort, Michael, Das Dreiecksverhältnis von Betriebsrat, betrieblichem Datenschutzbeauftragten und Aufsichtsbehörde beim Arbeitnehmer-Datenschutz, NZA 2015, 1345–1352.
Kort, Michael, Arbeitnehmerdatenschutz gemäß der EU-Datenschutz-Grundverordnung, DB 2016, 711–716.
Kort, Michael, Betriebsrat und Arbeitnehmerdatenschutz – Rechte der Interessenvertretung bei datenschutzrechtlich relevanten Maßnahmen des Arbeitgebers, ZD 2016, 3–9.
Kort, Michael, Eignungsdiagnose von Bewerbern unter der Datenschutzgrundverordnung (DS-GVO), NZA 2016 (erscheint demnächst).

Kraska, Sebastian, Auswirkungen der EU-Datenschutzgrundverordnung, ZD-Aktuell 2016, 04173.
Krause, Rüdiger, Verhandlungen des 71. Deutschen Juristentages, Band I: Gutachten/Teil B: Digitalisierung der Arbeitswelt – Herausforderungen und Regelungsbedarf, Essen, 2016.
Kühling, Jürgen, Rückkehr des Rechts: Verpflichtung von „Google & Co." zu Datenschutz, EuZW 2014, 527–532.
Kühling, Jürgen/Heberlein, Johanna, EuGH „reloaded": „unsafe harbor" USA vs. „Datenfestung" EU, NVwZ 2016, 7–12.
Kühling, Jürgen/Martini, Mario, Die Datenschutzgrundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, 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/Seidel, Christian/Sivridis, Anastasios, Datenschutzrecht, Kommentar, 3. Aufl., Heidelberg, 2015.
Lynsky, Orla, The Foundations of EU Data Protection Law, Oxford, 2015.
Maas, Heiko, EU-Datenschutz-Grundverordnung: Datensouveränität in der digitalen Gesellschaft, DuD 2015, 579–580.
Maas, Ingrid/Schmitz, Karl/Wedde, Peter, Datenschutz 2014 – Probleme und Lösungsmöglichkeiten, Frankfurt a.M., 2014.
Masing, Johannes, Einheit und Vielfalt des Europäischen Grundrechtsschutzes, JZ 2015, 477–487.
Mayer-Schönberger, Viktor, Delete – Die Tugend des Vergessens in digitalen Zeiten, 3. Aufl., Wiesbaden, 2015.
Mayer-Schönberger, Viktor/Cukier, Kenneth, Big Data – Die Revolution die unser Leben verändern wird, 2. Aufl., München, 2013.
Nguyen, Alexander, Die zukünftige Datenschutzaufsicht in Europa, ZD 2015, 265–270.
Oppermann, Thomas/Classon, Claus Dieter/Nettesheim, Martin, Europarecht, 7. Aufl., München, 2016.
Pötters, Stephan, Grundrechte und Beschäftigtendatenschutz, Baden-Baden, 2013.
Polzin, Monika, Das Rangverhältnis von Verfassungs- und Unionsrecht nach der neuesten Rechtsprechung des BVerfG, JuS 2012, 1–6.
Preis, Ulrich/Sagan, Adam, Europäisches Arbeitsrecht, Köln, 2015.
Reding, Viviane, Sieben Grundbausteine der europäischen Datenschutzreform, ZD 2012, 195–198.
Richter, Philipp, Datenschutz zwecklos? – Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO, DuD 2015, 735–740.
Roßnagel, Alexander, Handbuch Datenschutzrecht, München, 2003.
Roßnagel, Alexander, Datenschutz in einem informatisierten Alltag, Gutachten im Auftrag der Friedrich-Ebert-Stiftung, Berlin, 2007.

Roßnagel, Alexander, Schriftliche Stellungnahme zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung am 24. Februar 2016 im Ausschuss Digitale Agenda des Deutschen Bundestags, 24. 2. 2016.

Roßnagel, Alexander/Kroschwald, Steffen, Was wird aus der Datenschutzgrundverordnung? Die Entschließung des Europäischen Parlaments über ein Verhandlungsdokument, ZD 2014, 495–500.

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

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

Schild, Hans-Hermann/Tinnefeld, Marie-Theres, Datenschutz in der Union – Gelungene oder missglückte Gesetzentwürfe?, DuD 2012, 312–317.

Schüßler, Lennart/Zöll, Oliver, EU-Datenschutz-Grundverordnung und Beschäftigtendatenschutz, DuD 2013, 639–643.

Schuler, Karin/Weichert, Thilo, Die EU-DSGVO und die Zukunft des Beschäftigtendatenschutzes, Gutachten 8.4.2016, *http://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_dsgvo_beschds.pdf* (letzter Abruf am: 10. 8. 2016).

Schulze, Reiner/Zuleeg, Manfred/Kadelbach, Stefan, Europarecht – Handbuch für die Rechtspraxis, 3. Aufl., Baden-Baden, 2015.

Schwarze, Jürgen, EU-Kommentar, 3. Aufl., Baden-Baden, 2012.

Simitis, Spiros, Die EG-Datenschutzrichtlinie: eine überfällige Reformaufgabe, in: Herzog, Felix/Neumann, Ulfried (Hrsg.), Festschrift für Winfried Hassemer, Heidelberg, 2010, S. 1235 – 1248.

Simitis, Spiros, Bundesdatenschutzgesetz, 8. Aufl., Baden-Baden, 2014.

Simon, Dieter/Weiss, Manfred (Hrsg.), Zur Autonomie des Individuums, Liber Amicorum Spiros Simitis, Baden-Baden, 2000.

Spindler, Gerald, Die neue EU-Datenschutz-Grundverordnung, DB 2016, 937 – 947.

Streintz, Rudolf, EUV-AEUV, Vertrag über die Europäische Union und Vertrag über die Arbeitsweise der Europäischen Union, 2. Aufl., München, 2012.

Sydow, Gernot/Kring, Markus, Die Datenschutzgrundverordnung zwischen Technikneutralität und Technikbezug, ZD 2014, 271–276.

Taeger, Jürger, Einwilligung im Arbeitsverhältnis in die Veröffentlichung eines Werbevideos und ihre Widerrufbarkeit – KunstUrhG als lex specialis gegenüber dem BDSG, Anmerkung zu BAG, Urt. v. 11. 12. 2014 – 8 AZR 1010/13, jurisPR-DSR 1/2015, Anm. 4.

Taeger, Jürgen/Gabel, Detlev (Hrsg.), Kommentar zum BDSG und Datenschutzvorschriften des TKG und TMG, 2. Aufl., Frankfurt a.M., 2013.

Taeger, Jürgen/Rose, Edgar, Zum Stand des deutschen und europäischen Beschäftigtendatenschutzes, BB 2016, 819–831.

Thüsing, Gregor, Beschäftigtendatenschutz und Compliance, 2. Aufl., München, 2014.

Thüsing, Gregor, Datenschutz im Arbeitsverhältnis – Kritische Gedanken zum neuen § 32 BDSG, NZA 2009, 865–870.

Thüsing, Gregor, Umsetzung der Datenschutz-Grundverordnung im Beschäftigungsverhältnis: Mehr Mut zur Rechtssicherheit!, BB 2016, 2165.
Tinnefeld, Marie-Theres/Petri, Thomas/Brink, Stefan, Aktuelle Fragen um ein Beschäftigtendatenschutzgesetz – Eine erste Analyse und Bewertung, MMR 2010, 727–735.
Venetis, Frank/Oberwetter, Christian, Videoüberwachung von Arbeitnehmern, NJW 2016, 1051–1057.
Voßhoff, Andrea, Update BfDI 2.0 – Ausblick 2016, DuD 2016, 138.
Wedde, Peter, Die unterschätzte Macht der Mitbestimmung, CuA 2016, 8–13.
Wedde, Peter, EU-Datenschutz-Grundverordnung – Kurzkommentar mit Synopse BDSG/EU-DS GVO, Frankfurt 2016.
Weichert, Thilo, EU-US-Privacy Shield – ist der transatlantische Datentransfer nun grundrechtskonform?, ZD 2016, 209–217.
Weichert, Thilo/Schuler, Karin, Die EU-DSGVO und die Zukunft des Beschäftigtendatenschutzes – Gutachten v. 8. 4. 2016.
Will, Michael, Schlussrunde bei der Datenschutz-Grundverordnung?, ZD 2015, 345–346.
Wolf, Roland/Barlage-Melber, Eva, Datenschutz in Zeiten der Digitalisierung, AiB 2015, 26–28.
Wybitul, Tim, Was bringt die neue EU-Datenschutzgrundverordnung?, BB 2016, Die Erste Seite, Heft 2.
Wybitul, Tim, Was ändert sich mit dem neuen EU-Datenschutzrecht für Arbeitgeber und Betriebsräte, ZD 2016, 203–208.
Wybitul, Tim/Böhm, Wolf-Tassilo, Freier Wille auch im Arbeitsverhältnis?, BB 2015, 2101–2105.
Wybitul, Tim/Pötters, Stephan, Der neue Datenschutz am Arbeitsplatz, RDV 2016, 10–16.
Wybitul, Tim/Sörup, Thorsten/Pötters, Stephan, Betriebsvereinbarungen und § 32 BDSG – Wie geht es nach der DS-GVO weiter?, ZD 2015, 559–564.
Ziegler, Katharina, Arbeitnehmerbegriffe im europäischen Arbeitsrecht, Baden-Baden, 2011.
Zürn, Andreas/Maron, Christian, Der Koalitionsvertrag der 18. Legislaturperiode aus arbeitsrechtlicher Sicht, BB 2014, 629–633.

Schriftenreihe des Hugo Sinzheimer Instituts für Arbeitsrecht

Band 17 Matthias Jacobs / Matthias Münder / Barbara Richter
Spezialisierung der Unionsgerichtsbarkeit im Arbeitsrecht – Fachkammer für Arbeitsrecht am EuGH
ISBN 978-3-7663-6585-9

Band 16 Wolfgang Däubler
Tarifverträge zur Unternehmenspolitik? Rechtliche Zulässigkeit und faktische Bedeutung
ISBN 978-3-7663-6465-4

Band 15 Raimund Waltermann
Differenzierungsklauseln im Tarifvertrag in der auf Mitgliedschaft aufbauenden Tarifautonomie
ISBN 978-3-7663-6469-2

Band 14 Olaf Deinert
Beschäftigung ausländischer Arbeitnehmer in Inlandsbetrieben
ISBN 978-3-7663-6468-5

Band 13 Florian Rödl / Raphaël Callsen
Kollektive soziale Rechte unter dem Druck der Währungsunion
ISBN 978-3-7663-6467-8

Band 12 Ulrich Preis / Daniel Ulber
Ausschlussfristen und Mindestlohngesetz – Der Mindestlohn als unabdingbarer Sockelanspruch
ISBN 978-3-7663-6413-5

Band 11 Ulrike Wendeling-Schröder (Hrsg)
Die Arbeitsbedingungen des Betriebsrats
ISBN 978-3-7663-6329-9

Band 10 Monika Schlachter
Das Verbot der Altersdiskriminierung und der Gestaltungsspielraum der Tarifvertragsparteien
ISBN 978-3-7663-6389-3

Band 9 Ingrid Maas / Karl Schmitz / Peter Wedde
Datenschutz 2014 Probleme und Lösungsmöglichkeiten
ISBN 978-3-7663-6386-2

Band 8 Thorsten Kingreen
Soziales Fortschrittsprotokoll – Potenzial und Alternativen
ISBN 978-3-7663-6326-8

Band 7 Ulrike Wendeling-Schröder
Kritik der Lehre vom fehlerhaften Tarifvertrag unter besonderer Berücksichtigung der Tarifverträge tarifunfähiger Gewerkschaften in der Leiharbeit
ISBN 978-3-7663-6282-7

Band 6 Jens Schubert
Der Vorschlag der EU-Kommission für eine Monti-II-Verordnung – eine kritische Analyse unter Einbeziehung der Überlegungen zu der Enforcement-Richtlinie
ISBN 978-3-86194-115-6

Band 5 Wolfgang Däubler
Die Unternehmerfreiheit im Arbeitsrecht – eine unantastbare Größe?
ISBN 978-3-86194-110-1

Band 4 Bernd Waas
Betriebsrat und Arbeitszeit – Pauschale Abgeltung und Freistellungen über das Gesetz hinaus
ISBN 978-3-86194-092-0

Band 3 Bernd Waas
Geschlechterquoten für die Besetzung der Leitungsgremien von Unternehmen – Bewertung der aktuellen Entwürfe aus unionsrechtlicher und rechtsvergleichender Sicht
ISBN 978-3-86194-080-7

Band 2 Rüdiger Krause
Tarifverträge zur Begrenzung der Leiharbeit und zur Durchsetzung von Equal Pay
ISBN 978-3-86194-071-5

Band 1 Britta Rehder / Olaf Deinert / Raphaël Callsen
Arbeitskampfmittelfreiheit und atypische Arbeitskampfformen – Rechtliche Bewertung atypischer Arbeitskampfformen und Grenzen der Rechtsfortbildung
ISBN 978-3-86194-056-2