www.betriebs-berater.de

Betriebs Berater

70 Jahre

14|2016

Recht | Wirtschaft | Steuern

4.4.2016 | 71. Jg.
Seiten 769–832

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Prof. Dr. Jürgen Taeger und Dr. Edgar Rose

Zum Stand des deutschen und europäischen Beschäftigtendatenschutzes

Seit mehr als 30 Jahren wird ein Gesetz zum Arbeitnehmerdatenschutz von allen Seiten gefordert, von den politischen Parteien, Gewerkschaften, Datenschutzaufsichtsbehörden und der Wissenschaft. In diesem Zeitraum hat sich die betriebliche Praxis der Datenverarbeitung mehrfach dramatisch verändert, wodurch immer neue Herausforderungen für den Datenschutz der Beschäftigten aufgetreten sind. Videoüberwachung, Dokumentenmanagementsysteme mit Leistungsdaten über Arbeitnehmer, private Nutzung betrieblicher Kommunikationsmittel (BYOD-Bring-Your-Own-Device), genetische Untersuchungen, biometrische Zugangssysteme, GPS-Ortung der Dienstwagen, soziale Medien – das alles gab es früher nicht, bestimmt heute aber die Realität im Unternehmen. Es liegt auf der Hand, dass die Wahrung der Persönlichkeitsrechte von Arbeitnehmern besonders vor dem Hintergrund der digitalen Erfassung von Daten ein wichtiges Thema ist. Im digitalen Zeitalter sind das berechtigte Informationsinteresse des Arbeitgebers und die Wahrung der Persönlichkeitsrechte der Beschäftigten mit einem Beschäftigtendatenschutzgesetz auszubalancieren. In diesem Zusammenhang gilt es auch, die Stellung des Betriebs- bzw. Personalrats zu regeln.

I. Ausgangslage

Am 15.12.2015 einigten sich die Institutionen der EU im so genannten Trilog[1] über eine künftige EU-Datenschutzgrundverordnung (DSGVO),[2] die voraussichtlich Mitte 2018 mit Anwendungsvorrang gegenüber nationalen Datenschutzvorschriften anzuwenden sein wird.[3] Trotz der zwischen den am Trilog Beteiligten und insbesondere zwischen den Mitgliedstaaten weiter bestehenden kontroversen Ansichten wurde letztlich ein mit zahlreichen Öffnungsklauseln erkaufter Kompromiss erzielt, der das ursprüngliche Ziel einer EU-weiten Harmonisierung des Datenschutzrechts aus den Augen verlor. Inzwischen hat Österreich auch formal Bedenken geäußert,[4] was aber zu keiner Verzögerung der Beschlussfassung führen wird, weil letztlich die politisch gewollte Datenschutzgrundverordnung angesichts der erforderlichen – und erreichbaren – qualifizierten Mehrheit (Art. 16 Abs. 3 und 4 EUV) vom Rat für Justiz und Inneres bei einer erster Lesung am 21.4.2016 behandelt, vom Plenum des Europäischen Parlaments im Mai 2016 beschlossen und im EU-Amtsblatt bis Juli veröffentlicht werden kann. Die DSGVO würde dann gem. Art. 91 DSGVO 20 Tage nach der Veröffentlichung in Kraft treten und zwei Jahre später im Jahr 2018 Geltung erlangen. Dann wäre sie gem. Art. 288 Abs. 2 S. 2 AEUV für die Mitgliedstaaten verbindlich. Damit wird auch das Thema einer gesetzlichen Regelung des Arbeitnehmerdatenschutzes in Deutschland erneut auf die Tagesordnung gesetzt, denn in Art. 82 DSGVO ist eine Öffnungsklausel vorgesehen, wonach die Mitgliedstaaten für den Datenschutz im Beschäftigungskontext spezifische Regelungen per Gesetz oder Kollektivvereinbarung treffen können.

Im Mittelpunkt des Beitrags steht eine Bestandsaufnahme des bisherigen Beschäftigtendatenschutzes, wie er jedenfalls bis zum Inkrafttreten der DSGVO Bestand haben dürfte. Es wird erörtert, ob diese Rechtslage auch nach Geltung der DSGVO bestehen bleiben kann oder ob der nationale Gesetzgeber wegen der DSGVO beim Beschäftigtendatenschutz tätig werden muss und welche Handlungsoptionen ihm dabei zur Verfügung stehen.

II. Mangel an klaren gesetzlichen Regelungen zum Beschäftigtendatenschutz

Bis heute existiert kein umfassendes gesetzliches Arbeitnehmerdatenschutzrecht. Seit 2009 gibt es mit § 32 BDSG eine rudimentäre, ausdrücklich vorläufige Regelung.

Zuletzt wurde im Jahre 2010 ein Entwurf eines Beschäftigtendatenschutzgesetzes vorgelegt.[5] Der Entwurf sah die Integration des Beschäftigtendatenschutzes in das BDSG mit den §§ 32–32l BDSG vor. Er schaffte es bis in die 1. Lesung im Bundestag. Dann wurde er in der folgenden Ausschussberatung von der Regierung zurückgezogen.

Kritik gab es von allen Seiten, vom Bundesrat,[6] von Arbeitgeberseite,[7] von den Gewerkschaften[8] und aus der Wissenschaft.[9] Die umständliche Sprache und die unübersichtliche Struktur waren wenig anwenderfreundlich. Die große Zahl an unbestimmten Rechtsbegriffen war nicht geeignet, die noch immer bestehende Rechtsunsicherheit zu beseitigen. Und im Übrigen gab es neue Erlaubnistatbestände und Ausnahmeregelungen, die aus der Perspektive der Arbeitnehmer zu deutlich weniger Datenschutz geführt hätten. Erlaubt werden sollten die präventive Videoüberwachung und das Datenscreening mit anonymisierten Daten ohne konkreten Tatverdacht. Einwilligungen sollten nur möglich sein, wenn das Gesetz es ausdrücklich vorsieht: es sah dann

1 Trilog bezeichnet Verhandlungen zwischen der Europäischen Kommission, dem Rat der Europäischen Union und dem Europäischen Parlament zur Streitbeilegung im Rahmen europäischer Gesetzgebung.

2 Soweit hier Normen der DSGVO zitiert werden, bezieht sich dies auf die am 28.1.2016 als Ratsdok. 5455/16 veröffentlichte deutsche Übersetzung des im Trilog gefundenen Kompromisses der insbesondere bezüglich der Nummerierung der redaktionellen Bearbeitung bedarf. Es kann also sein, dass in der zu beschließenden und in die Sprachen der Mitgliedstaaten zu übersetzenden Fassung noch sprachliche Anpassungen an die Rechtssprache der Mitgliedstaaten erfolgen und die Nummerierung der Vorschriften angepasst werden wird.

3 S. zur Entstehungsgeschichte und zu den Regelungsinhalten im Überblick *Albrecht*, CR 2016, 88.

4 S. die zu Protokoll der Ratstagung vom 12.2.2016 gegebene Erklärung der österreichischen Delegation, http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/de/pdf (Abruf: 17.3.2016).

5 Am 3.9.2010 im Bundesrat (BR-Drs. 535/10) und nachfolgend im Bundestag (BT-Drs. 17/4230).

6 Stellungnahme des Bundesrates vom 5.11.2010, BR-Drs. 535/10(B).

7 BDA, Innenausschuss Drs. 17(4)252 C.

8 DGB Bundesvorstand Abt. Recht Stellungnahme vom 3.9.2010. http://www.dgb.de/themen/++co++3a87cbec-b9d1-11df-6fd9-00188b4dc422 (Abruf: 17.3.2016).

9 *Beckschulze/Natzel*, BB 2010, 2368; *Forst*, NZA 2010, 1043; *Heinson/Sörup/Wybitul*, CR 2010, 751; *Körner*, AuR 2010, 416; *Kort*, DB 2011, 651; *Tinnefeld/Petri/Brink*, MMR 2010, 727, und 2011, 427; *Thüsing*, NZA 2011, 16.

aber Einwilligungen in Datenverarbeitungen vor, bei denen man nach geltendem Recht wegen der fehlenden Freiwilligkeit gerade keine Einwilligung zulassen würde, beispielsweise beim Umgang mit Gesundheitsdaten.

Der 2009 kurzfristig in das Gesetz eingefügte § 32 BDSG sollte nur ein erster Schritt zu einem einheitlichen Beschäftigtendatenschutzrecht sein und später mit einem Arbeitnehmerdatenschutzgesetz präzisiert werden.[10] Dafür enthielt auch der Koalitionsvertrag der Großen Koalition von 2013 bereits Eckdaten.[11] Gegen Status quo gibt es weiter anhaltende Kritik.[12] Die Forderung nach einer umfassenden Regulierung ist nicht verstummt. Richtig ist, dass § 32 BDSG zahlreiche Rechtsfragen offen lässt.

Nach der Gesetzesbegründung sollte der Datenschutz der Arbeitnehmer zunächst in allgemeiner Form im BDSG verankert werden, ohne eine abschließende Regelung zu treffen.[13] Laut Beschlussempfehlung des Innenausschusses enthält § 32 BDSG eine allgemeine Regelung zum Schutz personenbezogener Daten von Beschäftigten, die die von der Rechtsprechung erarbeiteten Grundsätze nicht ändern, sondern lediglich zusammenfassen und ein Arbeitnehmerdatenschutzgesetz weder entbehrlich machen, noch inhaltlich präjudizieren soll.[14]

Nach dem Scheitern einer umfassenden Regelung des Arbeitnehmerdatenschutzes in der 17. Wahlperiode hat die aktuelle Bundesregierung im Koalitionsvertrag der 18. Wahlperiode Ende 2013 lediglich festgehalten: Falls mit dem Abschluss der Verhandlungen über die Europäische Datenschutzgrundverordnung (DSGVO) nicht in angemessener Zeit gerechnet werden könne, solle eine nationale Regelung zum Beschäftigtendatenschutz geschaffen werden.[15]

Ende 2015 ist mit Abschluss des Trilogs der europäischen Gesetzgebungsorgane das Inkrafttreten der DSGVO in greifbare Nähe gerückt. Das am 15.12.2015 erzielte Verhandlungsergebnis eines künftigen Verordnungstextes[16] ist am 17. und 18.12.2016 bereits vom federführenden Innen- und Justizausschuss (LIBE) des Europäischen Parlaments und vom Ausschuss der ständigen Vertreter der Mitgliedstaaten jeweils fast einstimmig angenommen worden.[17] Bei der Verabschiedung 2016 würde die DSGVO dann nach einer zweijährigen Frist wohl Mitte 2018 geltendes Recht.

Allerdings enthält der nunmehr beschlossene Text der DSGVO gerade keine dezidierte Regelung zum Beschäftigtendatenschutz. Vielmehr gibt es in Art. 82 DSGVO eine Öffnungsklausel, die auf dem gesamten Feld des Beschäftigtendatenschutzes spezifische nationale Regelungen zulässt. Damit wäre auch im Sinne des Koalitionsvertrages der Weg frei für eine umfassende gesetzliche Regelung des betreffenden Rechts in Deutschland. Allerdings finden sich in der Öffnungsklausel in Art. 82 DSGVO hierfür auch Vorgaben. Welche Handlungsoptionen sich daraus für den Gesetzgeber und auch für die Kollektivvertragsparteien künftig im Beschäftigtendatenschutz ergeben, soll Gegenstand des Schlussabschnitts dieses Beitrags sein.

III. Zulässigkeit der Erhebung und Verwendung von Beschäftigtendaten

Das zentrale Strukturelement des gegenwärtigen Datenschutzes, das in § 4 Abs. 1 BDSG geregelt ist, wird als „Verbot mit Erlaubnisvorbehalt" bezeichnet und gilt auch für Datenschutzfragen im Arbeitsverhältnis. Die Formulierung hat sich eingebürgert, auch wenn wir es nicht mit einem ausdrücklichen förmlichen Verbot durch Gesetz zu tun haben.[18] § 4 BDSG enthält also kein gesetzliches Verbot im verwaltungsrechtlichen Sinn, das durch einen Verwaltungsakt bei einem Vorliegen von Erlaubnisgründen aufzuheben wäre. Vielmehr ist die Erhebung und Verwendung einerseits zulässig, wenn das BDSG oder ein anderes Gesetz dies erlaubt. Neben dem BDSG gibt es eine außerordentlich große Zahl an Bundes- und Landesgesetzen im formellen Sinn, die bereichsspezifischen Datenschutz enthalten und für bestimmte Zwecke eine Erlaubnis oder gar eine Pflicht enthalten, personenbezogene Daten zu erheben und zu verarbeiten. Zu denken ist auch an die personalaktenrechtlichen Vorschriften in §§ 106 ff. BBG und in den personalaktenrechtlichen Vorschriften in den Landesbeamtengesetzen sowie die Datenschutzvorschriften für die Bediensteten auf Landesebene in den jeweiligen Landesdatenschutzgesetzen und in § 83 BetrVG. Auch im Arbeits- und Sozialrecht gibt es zahlreiche Meldepflichten des Arbeitgebers, nach denen personenbezogene Daten über Arbeitnehmer zu erheben und zu übermitteln sind (Beispiel: Anzeige eines Arbeitsunfalls gemäß § 193 Abs. 1 SGB VII).

Die Erhebung und Verwendung ist laut § 4 Abs. 1 BDSG ebenfalls zulässig, wenn der Betroffene wirksam eingewilligt hat. Das Recht auf informationelle Selbstbestimmung impliziert auch das Recht, Daten über die eigene Person zur Speicherung und Nutzung zur Verfügung zu stellen. § 106 Abs. 3 BBG erkennt das beispielsweise für die Einwilligung der Beamten in die zweckändernde Verwendung der Personaldaten ausdrücklich an. Das BDSG stellt allerdings in §§ 4a und 28 Abs. 3 ff. BDSG Anforderungen an die Wirksamkeit einer Einwilligung in die Erhebung und Verwendung personenbezogener Daten durch eine verantwortliche Stelle. Die wichtigste Anforderung – und bereits Bestandteil des Tatbestandsmerkmals ‚Einwilligung' – ist gemäß § 4a BDSG, dass sie auf der freien Entscheidung des Betroffenen beruht und nicht unter Zwang oder Druck abgegeben wird. In diesem Sinne darf auch der Abschluss eines Rechtsgeschäfts nicht von einer Einwilligung abhängig gemacht werden, wonach der Erhebung von Daten zugestimmt wird, die für dieses Rechtsgeschäft nicht erforderlich sind (sog. Kopplungsverbot).[19] Insbesondere darf der Abschluss eines Arbeitsvertrags nicht von einer derartigen Einwilligung abhängig gemacht werden.

Vom Grundsatz des Verbots mit Erlaubnisvorbehalt geht auch die Datenschutzgrundverordnung aus (Art. 6 DSGVO; Rechtmäßigkeit der Verarbeitung). Art. 6 DSGVO konkretisiert Art. 8 Abs. 2 Grundrechte-Charta, wonach personenbezogene Daten „nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden" dürfen. Der Erlaubnistatbestand der

10 BT-Drs. 16/13657, 34; s. dazu auch *Zöll*, in: Taeger/Gabel, BDSG, 2013, § 32, Rn. 2.
11 Koalitionsvertrag zwischen CDU, CSU und SPD, 18. Legislaturperiode, S. 70; *Wank*, ErfK, 2012, Rn. 1 zu § 32 BDSG, bezeichnet die Norm als gesetzgeberischen Schnellschuss, der wohlwollend auszulegen sei (https://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf (Abruf: 17.3.2016).
12 Zuletzt *Franzen*, RDV 2014, 200; *Thüsing*, RDV 2014, 196.
13 BT-Drs. 16/12011, 53 zu Nr. 33.
14 BT-Drs. 16/13657, 20.
15 Koalitionsvertrag zwischen CDU, CSU und SPD (Fn. 11).
16 Dokument des Rates 15039/15.
17 Newsdienst ZD-Aktuell 2016, 04946.
18 Überzeugend argumentiert *Buchner*, DuD 2016, 155. S. auch *Taeger*, in: Taeger/Gabel, BDSG, 2013, § 4, Rn. 1; *Gola/Schomerus*, BDSG, 2015, Rn. 3 zu § 4; Franzen, ErfK, 2016, Rn. 1 zu § 4 BDSG. Für die Beibehaltung des Verbotsprinzips. *Karg*, DuD 2013, 75; *Weichert*, DuD 2013, 246; *Bäcker*, in: Wolff/Brink, Beck'scher Online-Kommentar Datenschutzrecht, § 4, Rn. 3; *Spindler*, Persönlichkeitsschutz im Internet, Gutachten F zum 69. DJT, S. 102; *Taeger*, Datenschutzrecht, 2014, Kap. I, Rn. 51. Den Grundsatz des Verbots mit Erlaubnisvorbehalt ablehnend *Bull*, Netzpolitik, 2013, S. 136; *Nettesheim*, VVDStRL Bd. 170 (2011), 7, und – bezogen auf den Beschäftigtendatenschutz – *Franzen*, ZfA 2012, 172, 180 ff.
19 Generell auch *Simitis*, in: Simitis, BDSG, 2014, Rn. 63 zu § 4a; einschränkend *Plath*, in: Plath, BDSG, 2013, Rn. 30 zu § 4a, der nur dort das Kopplungsverbot gelten lassen will, wo es der Gesetzgeber ausdrücklich vorsieht (§ 28 Abs. 3a BDSG, § 12 Abs. 3 TMG).

Einwilligung findet sich in Art. 6 Abs. 1 Buchst. a DSGVO. Danach ist die Verarbeitung personenbezogener Daten auch zulässig, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere festgelegte Zwecke gegeben hat. Art. 4 Abs. 8 DSGVO definiert die Einwilligung wie folgt: „‚Einwilligung der betroffenen Person' jede ohne Zwang, für den konkreten Fall, in Kenntnis der Sachlage und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist."

1. Betriebsvereinbarung als Erlaubnis

Eine viel gestellte Frage ist, ob Tarifverträge und Betriebsvereinbarungen Gesetze im Sinne des § 4 BDSG sind, die materielles Datenschutzrecht insofern enthalten können, als sie eine Erhebung und Verarbeitung personenbezogener Daten von Arbeitnehmern durch den Arbeitgeber erlauben.

Für Unternehmen als nicht-öffentliche Stellen sind der normative Teil der Tarifverträge und Betriebsvereinbarungen, für die der § 77 Abs. 4 S. 1 BetrVG die normative Außenwirkung anordnet, sowie der eine Betriebsvereinbarung ersetzende Spruch einer Einigungsstelle als Rechtsvorschriften (Gesetz im materiellen Sinne) im Sinne des § 4 Abs. 1 BDSG seit langem grundsätzlich anerkannt.[20] Eine Betriebsvereinbarung darf daher datenschutzrechtliche Regelungen über die Erhebung und Verwendung von Arbeitnehmerdaten enthalten, wenn sich die Erlaubnisvorschrift im Rahmen der Regelungsautonomie der Betriebsparteien bewegt und die den Betriebsparteien etwa aus § 75 Abs. 2 BetrVG gezogenen Regelungsschranken nicht überschreitet.[21]

Das bedeutet nichts anderes als die Pflicht dieser Betriebsparteien, bei der Betriebsvereinbarung die Wahrung der Arbeitnehmerpersönlichkeitsrechte zu beachten. Es ist also von den Vertragsparteien der Betriebsvereinbarung stets der Schutzauftrag des § 75 Abs. 2 BetrVG zu berücksichtigen; auch in dieser Hinsicht ist das vom „Gesetzgeber" zu beachtende Verhältnismäßigkeitsprinzip streng zu wahren,[22] sonst wäre eine vom Arbeitgeber aus der Betriebsvereinbarung abgeleitete Erlaubnis schon deswegen unwirksam.[23]

Das wäre beispielsweise der Fall, wenn eine Betriebsvereinbarung vorsehen würde, dass besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) für ein Genom-Screening der Arbeitnehmer übermittelt werden dürfen. Eine solche Regelung der Betriebsparteien wäre wegen eines schwerwiegenden Eingriffs in das Selbstbestimmungsrecht des einzelnen Arbeitnehmers, dessen Gesundheitsdaten zu dem besonders geschützten innersten Kern seiner Persönlichkeitssphäre gehören, unzulässig. Hier müsste der Gesetzgeber selbst regulierend tätig werden und erforderlichenfalls durch ein Gesetz – wie das Arbeitsschutzgesetz – regeln, ob und unter welchen materiellen und formellen Schutzvoraussetzungen im Interesse des Arbeitnehmers ausnahmsweise eine Datenerhebung und -verwendung der Arbeitnehmerdaten für eine Genomanalyse erlaubt sein sollte. Abgesehen davon kann eine Betriebsvereinbarung zum Gesundheitsmanagement im Betrieb aber zulässig sein.

Wenn der Arbeitgeber die private Nutzung dienstlicher Kommunikationseinrichtungen in einem bestimmten Rahmen erlauben will, kann durch eine Betriebsvereinbarung geregelt werden, dass er trotz der dann auch privaten Kommunikation unter der betrieblichen E-Mail-Adresse die Einhaltung des angemessenen Nutzungsumfangs privater Kommunikation kontrollieren darf.

Das BAG[24] hat kürzlich festgestellt, dass eine Betriebsvereinbarung auch die Persönlichkeitsrechte von Beschäftigten beschränken darf. Die Betriebsvereinbarung muss nur verhältnismäßig sein. Konkret ging es in der Entscheidung um die stichprobenartigen Taschenkontrollen am Werkstor, nachdem es zu Diebstählen in hohem Ausmaß (> 250 000 Euro p. a.) im Werk gekommen war. Die Betriebsvereinbarung hatte hier die Einzelheiten geregelt.

Es ist also abwegig, wenn von manchen Autoren[25] aus der Pflicht, die Persönlichkeitsrechte der Arbeitnehmer zu wahren, stereotyp der Schluss gezogen wird, dass „daher kaum ein Fall denkbar" ist, in dem eine nach dem BDSG an sich unzulässige Datenverarbeitung durch Betriebsvereinbarung ermöglicht wird. Auch in aktuellen Veröffentlichungen heißt es weiterhin, dass Betriebsvereinbarungen den gesetzlichen Schutz nur nachzeichnen und konkretisieren, nicht aber absenken könnten[26] bzw. nicht wesentlich, aber geringfügig vom Datenschutzniveau des BDSG zu Ungunsten der Arbeitnehmer abweichen könnten.[27] Darum geht es jedoch gar nicht. Es werden durch Betriebsvereinbarungen ja nicht Rechte der Arbeitnehmer – etwa auf Auskunft oder Löschung – kassiert, die Zweckbindung außer Kraft gesetzt oder die Kontrollbefugnisse durch den betrieblichen Datenschutzbeauftragten eingeschränkt. Sondern es wird das geschaffen, was das BDSG vorsieht: ein Erlaubnistatbestand für die Datenverarbeitung, und das eben unter abwägender Beachtung der Persönlichkeitsrechte der Arbeitnehmer. Gerade auch im Interesse der Persönlichkeitsrechte der Beschäftigten sind zahlreiche Fälle der Datenverarbeitung vorstellbar, die gesetzlich problematisch wären, weil sie nicht zur Durchführung des Arbeitsverhältnisses erforderlich sind, aber z. B. personenbezogen Vergünstigungen einräumen.[28]

Angeführt wird für die enge Bindung der Betriebspartner an das BDSG, dass sowohl die Betriebsvereinbarung als auch das Gesetz die gleichen Vorgaben der europäischen Datenschutzrichtlinie 95/46/EG umzusetzen haben.[29] Doch sind die Interpretations- und Ermessensspielräume in Art. 7 b) und f) dieser Richtlinie so groß, dass im Einzelfall unterschiedliche Ergebnisse der Umsetzung weithin gedeckt sind. Ein eng formulierter gesetzlicher Erlaubnistatbestand in § 32 Abs. 1 BDSG und eine erweiterte Zulässigkeit von Eingriffen auf Grundlage einer Betriebsvereinbarung können nebeneinander bestehen.

Auch die Datenschutzgrundverordnung geht davon aus, dass neben den Gesetzen im formellen Sinn auch Tarifverträge, die Gesetzeskraft haben, und Kollektivvereinbarungen den Beschäftigtendatenschutz spezifisch regeln dürfen. Art. 82 Abs. 1 DSGVO erwähnt die Kollektivvereinbarungen ausdrücklich neben dem Gesetz. In einer nicht abschließenden Liste werden die Zwecke aufgeführt, für die derartige Kollektivvereinbarungen „insbesondere" abgeschlossen werden können. Der Erwägungs-

20 BAG, 27.5.1986 – 1 ABR 48/84, NZA 1986, 643, 646 f., BAG, 30.8.1995 – 1 ABR 4/95, BB 1996, 643, NZA 1996, 218, 221; *Thüsing/Granetzny*, in: Thüsing, Beschäftigtendatenschutz und Compliance, 2014, § 4, Rn. 4-6; *Wybitul*, NZA 2014, 225, *Franzen*, ErfK, 2016, Rn. 2 zu § 4 BDSG.
21 *Taeger*, Datenschutzrecht, 2014, Kap. III, Rn. 205.
22 Z. B. BAG, 26.8.2008 – 1 ABR 16/07, BB 2008, 2743 m. BB-Komm. Domke, NZA 2008, 1187, Rn. 14–18.
23 *Kania*, ErfK, 2016, Rn. 12 zu § 75 BetrVG; *Körner*, AuR 2015, 394.
24 BAG, 15.4.2014 – 1 ABR 2/13, NZA 2014, 551, Rn. 38 ff.
25 *Bausewein*, Legitimationswirkung von Einwilligung und Betriebsvereinbarung im Beschäftigtendatenschutz, 2012, S. 105; *Franzen*, ErfK 2016, Rn. 3 zu § 4 BDSG; *Gola/Schomerus*, BDSG, 2015, Rn. 10a zu § 4; *Kock/Francke*, NZA 2009, 646, 647.
26 *Wybitul/Sörup/Pötters*, ZD 2015, 559, 560.
27 *Kort*, ZD 2016, 3, 7.
28 Beispiele können sich u. a. ergeben aus der privaten Internetnutzung am Arbeitsplatz, der Durchführung von Betriebsfeiern, der elektronischen Kantinenabrechnung, der individuellen Präsentation auf Internetseiten des Unternehmens, des Kritik- und Vorschlagswesens, der Publikation einer Betriebszeitung, des Parkplatzzugangs.
29 *Pötters*, Grundrechte und Beschäftigtendatenschutz, 2013, S. 245.

grund 124 erhellt, dass zu den Kollektivvereinbarungen auch die Betriebs- und Dienstvereinbarungen zu zählen sind.

Im Ergebnis können wir also festhalten, dass eine Betriebsvereinbarung eine Rechtsvorschrift im Sinne des § 4 Abs. 1 BDSG und im Sinne des Art. 82 DSGVO sein kann.[30] In der Praxis lassen sich zahlreiche Betriebs- und Personalvereinbarungen finden, die im Rahmen des § 75 Abs. 2 BetrVG bzw. des § 67 BPersVG durchaus (auch) im Interesse der Beschäftigten Regelungen mit Erlaubnisvorschriften im Sinne des Datenschutzrechts enthalten.

2. Einwilligung als Erlaubnis

Wichtig ist festzustellen, dass die Erteilung einer Einwilligung eine Grundrechtsausübung[31] und nicht etwa einen Grundrechtsverzicht darstellt. Als Norm des objektiven Rechts entfaltet dieses Grundrecht auf Informationelle Selbstbestimmung seinen Rechtsgehalt auch im Privatrecht und insbesondere auch im Beschäftigungsverhältnis. Das besondere Gewaltverhältnis, die Subordination unter das Weisungsrecht des Arbeitgebers, ändert an diesem Selbstbestimmungsrecht zunächst grundsätzlich nichts.[32]

Die Einwilligung sollte aber nicht eingeholt werden, wenn eine gesetzliche Erlaubnis vorliegt,[33] von denen es einige gibt. Umstritten ist, wie die Rechtslage zu beurteilen ist, wenn doch eine Einwilligung eingeholt wird, obwohl bereits eine gesetzliche Erlaubnis vorliegt, und wenn diese Einwilligung dann widerrufen wird. Es wird die Ansicht vertreten, dass nach Treu und Glauben (§ 242 BGB) der Arbeitgeber dann von der gesetzlichen Erlaubnis keinen Gebrauch machen darf.[34] Es werde ein Vertrauenstatbestand geschaffen. Das überzeugt nicht. Der Widerruf einer Einwilligung führt nicht zur Derogation einer gesetzlichen Erlaubnisnorm. Der Arbeitgeber ist aber gut beraten, zunächst zu prüfen, ob eine gesetzliche Erlaubnis vorliegt, um die angestrebte Datenerhebung und -verarbeitung vorzunehmen, bevor eine Einwilligung eingeholt wird.

In § 4a BDSG finden sich Anforderungen an die Wirksamkeit einer Einwilligungserklärung. Nach Absatz 1 S. 1 ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Die Wirksamkeit der Einwilligung setzt weiter eine umfassende Information über die verantwortliche Stelle, die Art der Daten und den Zweck der Verarbeitung voraus (informierte Einwilligung). Die Informationen müssen leicht erkennbar sein und besonders hervorgehoben werden, wenn sie im Zusammenhang mit anderen Erklärungen erfolgt. Die Einwilligung muss vor der Erhebung erfolgt und widerruflich sein. Die Schriftform ist bei elektronischer Kommunikation nicht erforderlich.

Auch die Art. 29-Gruppe, in der sich die europäischen Datenschutzaufsichtsbehörden zusammengeschlossen haben, hat sich mit der Einwilligungsmöglichkeit in Beschäftigungsverhältnissen befasst. Sie hat darauf hingewiesen, dass ein Arbeitgeber sich in bestimmten Fällen auf eine Einwilligung seiner Beschäftigten stützen können muss und diese auch wirksam ist, wenn für den Arbeitnehmer nachweislich aus der Verweigerung der Einwilligung oder aus dem Widerruf der Einwilligung kein Nachteil entsteht.[35] Sie stellt weiter fest, dass eine Einwilligung aber nur dann gültig sein könne, wenn die betroffene Person eine tatsächliche Wahlmöglichkeit habe und kein Risiko einer Täuschung, Einschüchterung, Nötigung oder beträchtlicher negativer Folgen bestehe, wenn sie die Einwilligung nicht erteile.[36]

Die umstrittene Frage ist, ob es im Beschäftigungsverhältnis überhaupt Freiwilligkeit geben kann. Nicht selten wird vertreten, dass das wegen der Angewiesenheit des Arbeitnehmers auf den Erhalt seines Arbeitsplatzes nicht oder nur ganz ausnahmsweise der Fall sei.[37] Allerdings heißt es im Bericht des Innenausschusses des Deutschen Bundestages bei der Begründung des 2009 eingefügten § 32 BDSG, dass nach dem Willen des Gesetzgebers „eine Datenerhebung oder -verwendung auf der Grundlage einer freiwillig erteilten Einwilligung des Beschäftigten … durch § 32 nicht ausgeschlossen“ ist.[38]

Auch „im Falle eines Machtungleichgewichts zwischen Datenverarbeiter und Betroffenem (ist) die Freiheit des Einzelnen zur Selbstbestimmung nicht notwendigerweise ausgeschlossen“.[39] Sicherlich: In einer Bewerbungssituation wird ein Arbeitnehmer, der im Wettbewerb mit anderen Arbeitsuchenden steht, in der Entscheidung nicht frei sein können, über die gesetzlich zulässige Verarbeitung seiner Daten hinaus seinem möglichen künftigen Arbeitgeber die Nutzung seiner Daten für andere als die gesetzlich erlaubten Zwecke zu gestatten oder ihm gar qua Einwilligung zu erlauben, Fragen zu stellen, die ohne Einwilligung nicht gestellt werden dürften. Von einer freien Willensbildung wird man in dieser Lage nicht ausgehen können.[40] Es bleibt daher dabei, dass eine Einstellung nicht von einer Einwilligung in eine Datenerhebung und -verarbeitung von Beschäftigtendaten abhängig gemacht werden darf, die für die Erfüllung der Pflichten aus dem Vertrag nicht erforderlich ist. Dies betont auch § 7 Abs. 4 DSGVO als Bedingung für die Einwilligung ausdrücklich.

Gleichwohl: Das BDSG enthält hinsichtlich der Möglichkeit zur Einwilligung „keine Bereichsausnahme für das Arbeitsrecht“. Die Freiwilligkeit ist etwa gegeben, wenn Daten erfasst werden, um eine personalisierte Magnetkarte zu erhalten, mit der die Schranke zum Mitarbeiterparkplatz geöffnet werden kann; selbstverständlich dürfen diese Daten dann nicht zu einer Anwesenheitskontrolle genutzt werden. Zulässig wäre auch die Datenübermittlung auf der Grundlage einer Einwilligung, wenn der Arbeitnehmer an einem Personalentwicklungsprogramm des Konzerns teilnehmen will und deshalb wegen des (derzeit noch) fehlenden Konzernprivilegs[41] einer Personaldatenübermittlung an das konzernverbundene Unternehmen für den Zweck der Personalentwicklung einwilligen muss. Der Arbeitnehmer kann einwilligen, dass sein Name und (elektronische) Adresse an den Arbeitgeberverband – oder an eine Gewerkschaft – übermittelt wird, um über den Stand von Tarifverhandlungen informiert zu werden. Die Konzernbetriebsvereinbarung (KBV)

30 S. zur DSGVO insofern auch *Gola/Pötters/Thüsing*, RDV 2016, 55.
31 *Simitis*, in: Simitis, BDSG, 2014, Rn. 2 zu § 4a.
32 So jetzt auch ausdrücklich das BAG in einer Entscheidung zur Einwilligung nach § 22 KUG (BAG, 11.12.2014 – 8 AZR 1010/13, K&R 2015, 433, NZA 2015, 604, Rn. 32, m. Anm. *Taeger*, jurisPR-DSR 1/2015 Anm 4).
33 *Gola/Schomerus*, BDSG, 2015, Rn. 16 zu § 4.
34 Vgl. *Gola/Wronka*, Handbuch Arbeitnehmerdatenschutz, 2013, Rn. 386; *Simitis*, in: Simitis, BDSG, 2014, Rn. 93 zu § 4a.
35 Art. 29-Datenschutzgruppe, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, 13. September 2001, 5062/01/DE/endg., WP 48, S. 27.
36 Art. 29-Datenschutzgruppe, Stellungnahme 15/2011 zur Definition von Einwilligung, 13.7.2011, 01197/11/DE, WP 187, S. 15.
37 Z. B. *Tinnefeld/Petri/Brink*, MMR 2010, 727, 729.
38 BT-Drs. 16/13657, 20; darauf verweisen auch *Thüsing/Traut*, in: Thüsing, Beschäftigtendatenschutz und Compliance, 2014, § 5, Rn. 11.
39 *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 65.
40 So auch Art. 29-Datenschutzgruppe, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, 13.9.2001, 5062/01/DE/endg., WP 48, S. 27.
41 In Erwägungsgrund 38a der DSGVO heißt es: „Für die Verarbeitung Verantwortliche, die Teil einer Unternehmensgruppe oder einer Einrichtung sind, die einer zentralen Stelle zugeordnet ist, können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln.“ Eine Unternehmensgruppe ist nach der Definition in Art. 4 Nr. 16 „eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht“. Mit diesem als ‚kleines Konzernprivileg‘ bezeichneten Erwägungsgrund wird lediglich anerkannt, dass es bei der Abwägung nach Art. 6 Abs. 1 Buchst. f DSGVO ein Unternehmensinteresse gibt, Daten innerhalb des Konzerns zu übermitteln. S. dazu auch *Lachenmann*, Datenübermittlung im Konzern, 2016.

zwischen der Deutschen Bahn AG sowie der Mobility Logistics AG und dem Konzernbetriebsrat vom 21.1.2016 über die Nutzung des konzerninternen Social Media-Angebots ‚DB Planet' sieht in § 3 vor, dass die Beschäftigten das Angebot freiwillig auf der Grundlage einer im Anhang zur KBV enthaltenen Einwilligungserklärung nutzen, soweit nicht aus dienstlichen Gründen die Nutzung der dienstlichen Elemente von DB Planet als vertraglich geschuldete Arbeitsleistung verlangt wird. Sicher lassen sich weitere Beispiele finden, in denen davon ausgegangen werden kann, dass keine Zwangslage vorliegt und damit die Einwilligung wirksam ist.[42]

Anders als im ersten Kommissionsentwurf zu einer DSGVO ist die Einwilligung im Beschäftigungsverhältnis als Erlaubnis für die Verarbeitung von Beschäftigtendaten in der jetzigen Fassung des Trilog-Ergebnisses – sowie in den früheren Entwürfen von Parlament und Rat – nicht mehr ausgeschlossen, so dass sie unter den genannten Bedingungen auch künftig für Beschäftigungszwecke und für beschäftigungsfremde Zwecke zulässig sein wird.

Die Anforderungen an die Einwilligung nach Art. 6 Abs. 1 Buchst. a i. V. m. Art. 7 DSGVO entsprechen weitgehend denen des BDSG; nur wird künftig eine ausdrückliche Erklärung (opt in) erforderlich und eine opt out-Lösung nicht mehr zulässig sein. Aufgrund in Art. 7 DSGVO enthaltenen Einwilligungsbedingungen wird eine Einwilligung auch zu dokumentieren sein, um den Nachweis der erfolgten Einwilligung erbringen zu können (Art. 7 Abs. 1 DSGVO). *Hayen*, CuA 3/2016, 20, 22, fordert, dass der Gesetzgeber tätig wird und die Unzulässigkeit der Einwilligung im Beschäftigungsverhältnis festschreibt oder sie wenigstens auf die Fälle reduziert, die dem Beschäftigten einen rechtlichen oder wirtschaftlichen Vorteil verschafft. Die Erwägungsgründe 32 und 34 der DSGVO geben weitere Auslegungshilfen. So sollen Minderjährige unter 16 Jahren keine Einwilligung ohne Zustimmung der Sorgeberechtigten geben können, wenn dem Kind ‚Dienste der Informationsgesellschaft' angeboten werden. Das BDSG setzte hier die Einsichtsfähigkeit des Einwilligenden voraus.

IV. Regelungsgehalt des § 32 BDSG

Die 2009 eingefügte Vorschrift zum Beschäftigtendatenschutz, mit der der Gesetzgeber die bisherigen Grundsätze zum Beschäftigtendatenschutz nicht ändern, sondern lediglich zusammenfassen wollte,[43] verdient nähere Betrachtung.

1. Reichweite

§ 32 BDSG gilt für Beschäftigte, womit auf die Definition in § 3 Abs. 11 BDSG verwiesen wird. Der dort definierte Beschäftigtenbegriff ist deutlich weiter als der gleichlautende Begriff im Sozialversicherungs- oder Gleichstellungsrecht. Er umfasst nicht nur Arbeitnehmer, sondern unter anderem auch Richter und Beamte, zur Berufsbildung beschäftigte Personen, arbeitnehmerähnliche Personen (z. B. viele freie Mitarbeiter, Heimarbeitnehmer), nach dem Jugendfreiwilligendienstegesetz Beschäftigte. Ausdrücklich werden gemäß § 3 Abs. 11 Ziff. 7 BDSG auch Bewerberinnen und Bewerber sowie Personen, deren Beschäftigungsverhältnis beendet ist, einbezogen. Also auch Personen, zu denen nie ein Arbeitsverhältnis bestanden hat, deren Daten aber wegen einer Bewerbung erfasst worden sind, unterfallen § 32 BDSG. Ebenso können sich Ehemalige wegen noch vorhandener Beschäftigtendaten auf § 32 BDSG berufen. Auch unter der DSGVO wird dieser weite Personenkreis erfasst sein, obwohl sich der Wortlaut des Art. 82 Abs. 1 DSGVO auf ‚Arbeitnehmerdaten', und nicht auf ‚Beschäftigtendaten' bezieht.[44] Zu bedenken ist aber, dass der europäische Arbeitnehmerbegriff per se weiter ist und etwa auch Beamte einschließt und in der Norm selbst die Verarbeitung „im Beschäftigtenkontext" adressiert wird, so dass sich insoweit auch künftig an dem durch § 3 Nr. 11 BDSG festgelegten personellen Anwendungsbereich nichts ändern wird.

Organmitglieder, mit denen ein Geschäftsbesorgungsvertrag geschlossen wurde, werden nicht erfasst; auf sie ist § 28 Abs. 1 BDSG anzuwenden.

§ 32 BDSG gilt für das Erheben, Verarbeiten und Nutzen von Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses. Verarbeiten ist laut § 3 Abs. 4 BDSG das Speichern, Verändern, Übermitteln, Sperren und Löschen. Eine Besonderheit ergibt sich aus § 32 Abs. 2 BDSG, wonach für die Anwendung der Bestimmung keine automatisierte Verarbeitung vorausgesetzt wird. Jedwede personenbezogene Notiz wird dadurch in den Anwendungsbereich des § 32 einbezogen. Das mag zum Schutz der Beschäftigten vernünftig sein. Doch stellt sich die Frage, ob die Vorschrift dem EU-Recht genügt; denn die EU-Datenschutzrichtlinie (DSRL) sieht diese Erstreckung auf analoge Daten nicht vor. Der EuGH hatte seit 2003 mehrfach entschieden,[45] dass die DSRL 95/46/EG keine Mindeststandards setze, sondern eine grundsätzlich umfassende Harmonisierung vornehme, so dass ein Abweichen auch zugunsten der Beschäftigten europarechtswidrig wäre. Auch die DSGVO regelt nicht die Verarbeitung analoger Daten etwa in den klassischen Personalakten in Papierform, sondern nur die elektronische Verarbeitung. Die Öffnungsklausel in Art. 82 Abs. 1 DSGVO sieht aber anders als andere Öffnungsklauseln der DSGVO nicht vor, dass sich nationale Regelungen an die ‚Grenzen der Verordnung' halten müssten. Aus Art. 153 i. V. m. Art. 114 Abs. 2 AEUV folgt eine Regelungskompetenz der Mitgliedstaaten für das Arbeitsrecht, so dass nicht daran gezweifelt werden kann, dass auch nach Inkrafttreten der DSGVO § 32 BDSG oder eine Nachfolgevorschrift sich auch auf analoge Beschäftigtendaten erstrecken darf.

Damit § 32 BDSG zur Anwendung kommt, muss die Erhebung, Verarbeitung oder Nutzung der Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses erfolgen. Darunter sind alle Zwecke zu verstehen, die mit dem Arbeitsverhältnis in einem ursächlichen Zusammenhang stehen – keineswegs nur Zwecke des arbeitsvertraglich vereinbarten Leistungsaustausches. Erst wenn der Arbeitgeber dem Beschäftigten wie ein beliebiger Dritter gegenüber steht, greift § 32 BDSG nicht mehr.[46] Dieses weite Verständnis ergibt sich aus der Absicht des Gesetzgebers, eine allgemeine Regelung zum Schutz personenbezogener Daten von Beschäftigten zu schaffen.[47] Die Grenze ist z. B. überschritten, wenn der Arbeitnehmer beim Arbeitgeber wie ein beliebiger Kunde (ohne besondere Vergünstigung) einkauft. Geht es hingegen um die Gewährung eines Beschäftigtenrabatts, unterfällt auch die Datenverarbeitung für diesen Zweck dem § 32 BDSG.

§ 32 BDSG soll für „besondere Arten personenbezogene Daten" gemäß § 3 Abs. 9 BDSG (Angaben über u. a. Herkunft, Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) laut Begründung des zuständigen Ausschusses nicht gelten, da insoweit § 28

42 *Taeger*, Datenschutzrecht, 2014, Kap. III, Rn. 206 f.
43 BT-Drs. 16/13657, 20.
44 S. auch *Gola/Pötters/Thüsing*, RDV 2016, 55.
45 EuGH, 6.11.2003 – C-101/01, EWS 2003, 559 und EuGH, 24.11.2011 – C-468/10, C-469/10, K&R 2012, 40, NZA 2011, 1409.
46 *Schmidt*, DuD 2010, 207, 209; ähnlich *Traut*, RDV 2014, 119, 121.
47 BT-Drs. 16/13657, 20.

Abs. 6–8 BDSG mit strengeren Regelungen durchgreift.[48] Da tut sich dann aber eine große Lücke auf. Woraus soll der Arbeitgeber dann seine Befugnis nehmen, im Einstellungsgespräch nach der Gesundheit des Arbeitnehmers fragen zu dürfen, wenn sich aus dem Fragerecht des Arbeitgebers dagegen keine Bedenken ergeben, etwa weil der zu besetzende Arbeitsplatz bestimmte gesundheitliche Anforderungen stellt?

Der Vollständigkeit halber weist der Gesetzgeber in § 32 Abs. 3 BDSG darauf hin, dass die Beteiligungsrechte der Arbeitnehmervertretungen (Betriebsräte, Personalräte, Sprecherausschüsse, kirchliche Mitarbeitervertretung) unberührt bleiben. Sie beruhen auf anderen Vorschriften und sollen durch das BDSG weder erweitert noch beschnitten werden.

2. Erlaubnistatbestände gemäß § 32 BDSG

§ 32 Abs. 1 S. 1 BDSG erlaubt die Erhebung, Verarbeitung oder Nutzung von Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses. In die Privatsphäre des Arbeitnehmers darf nicht tiefer eingegriffen werden, als es zur Erfüllung der Zwecke des Beschäftigungsverhältnisses – im Hinblick auf die Entscheidung über die Begründung, Durchführung oder Beendigung – erforderlich ist.

Es ist verbreitete Ansicht,[49] dass mit „Erforderlichkeit" eine Interessenabwägung nach den Grundsätzen der Verhältnismäßigkeit vorzunehmen ist. Es müsse eine Abwägung der Interessen des Arbeitnehmers mit den schutzwürdigen Belangen des Arbeitgebers vorgenommen werden. Nach anderer Ansicht ist bei der Anwendung von S. 1 keine gesonderte Interessenabwägung vorzunehmen.[50]

Der Gesetzestext ist insoweit unmissverständlich. Allein den Maßstab der Erforderlichkeit stellt der Gesetzgeber heraus. Während andere Erlaubnisnormen eine Interessenabwägung explizit anordnen – wie § 32 Abs. 1 S. 2, § 28 Abs. 1 S. 1 Nr. 2 und 3 BDSG – fehlt diese in § 32 Abs. 1 S. 1 BDSG. Die Datenverarbeitung hat demnach einen akzessorischen Charakter. Sie ist ein Hilfsmittel zur Zweckerreichung. Sie dient dem rechtsgeschäftlichen Schuldverhältnis mit dem Arbeitnehmer, so dass die sich daraus ergebenden Verpflichtungen zu erfüllen sind. Ergeben sich aus Gesetzen, z. B. Arbeitsschutzgesetzen, Arbeitnehmerschutzgesetzen, aus fiskalischen und sozialrechtlichen Regelungen, Pflichten des Arbeitgebers, Daten bereit zu halten oder zu übermitteln, dann ist ihre Erhebung gesetzlich zwingend – also erforderlich. Für die Durchführung des Arbeitsverhältnisses sind z. B. auch alle Daten erforderlich, die in die Entgeltabrechnung eingehen. Das betrifft auch Leistungsdaten, wenn ein Leistungsentgelt vereinbart ist. Feststellungen über die Zielerreichung oder Beurteilungen, die keine Auswirkungen auf das Entgelt haben, können ebenfalls als erforderliche Daten gelten, da sie z. B. für Auswahlentscheidungen (Beförderung oder Weiterbildung) maßgeblich sein können. Auch Maßnahmen, die die Vertragstreue der Beschäftigten kontrollieren (z. B. Torkontrollen), können erforderlich sein.

Es ist nach objektiven Kriterien festzustellen, ob die Daten benötigt werden, sie also notwendig sind, so dass nur bei ihrer Kenntnis die sich aus dem Vertragsverhältnis ergebenden Rechte geltend gemacht und Pflichten erfüllt werden können. Eine Prüfung der Erforderlichkeit ist keineswegs blind gegenüber Belangen der Beschäftigten, denn sie verlangt den mildesten Eingriff in ihre informationelle Selbstbestimmung, der für den jeweiligen Zweck geeignet ist. Jeder Eingriff, der darüber hinausgeht, ist nicht mehr erforderlich. Im Anschluss findet aber keine zusätzliche Verhältnismäßigkeitsprüfung mehr statt, wie explizit von manchen Autoren vorgeschlagen.[51] Dies würde den Maßstab der Erforderlichkeit übrigens auch aufweichen. Denn was für die Durchführung des Arbeitsverhältnisses aufgrund des Vertrages oder aufgrund zwingender gesetzlicher Pflichten bezüglich der Erhebung, Speicherung und Übermittlung notwendig ist, kann nicht von einer darüber hinausgehenden Interessenabwägung abhängig gemacht werden. § 32 Abs. 1 S. 1 BDSG ist daher im Hinblick auf das Merkmal ‚erforderlich' so zu lesen wie in § 28 Abs. 1 S. 1 Nr. 1 BDSG.

a) Erforderlichkeit bei der Begründung des Beschäftigungsverhältnisses

Nun ist aber bekannt, dass der Arbeitgeber in der Bewerbungssituation ein hohes Informationsinteresse hat, viel über Bewerber zu erfahren. Es ist nicht eindeutig eingrenzbar, was für die Einstellungsentscheidung zwingend erforderlich ist. Es ist eine Abwägung vorzunehmen, soweit nicht offensichtlich schon aufgrund gesetzlicher Pflichten bestimmte Daten erforderlich sind, die z. B. eine bestimmte Qualifikation nachweisen. Bei der Überlegung, wie weit das Fragerecht des Arbeitgebers bei Anbahnung des Beschäftigungsverhältnisses geht, wird also in der Regel intensiver geprüft werden müssen, ob ein berechtigtes, billigenswertes und schutzwürdiges Interesse des Arbeitgebers besteht,[52] demgegenüber die schutzwürdigen Belange des Beschäftigten zurücktreten müssen.

Gemäß einer Verhältnismäßigkeitsprüfung wird dann festzustellen sein, ob die Datenerhebung und -verwendung erforderlich ist, um den angestrebten Zweck zu erreichen. Dabei kann auch die alte Sphärentheorie wieder belebt werden, wonach der Schutz der Privatsphäre des Arbeitnehmers schwerer wiegt, je näher die Informationen sich über den sozialen Bereich dem innersten Kern, der Intimsphäre nähern.

Fragen zum Gesundheitszustand wären damit nur erlaubt, wenn bestimmte gesundheitliche Dispositionen eine entscheidende berufliche Anforderung darstellen, etwa bei Piloten und LKW-Fahrern. Bluttests sind und bleiben unzulässig; sie greifen unverhältnismäßig in die Privatsphäre von Bewerbern ein.[53]

Diskutiert wird weiter, ob nach einer Schwerbehinderung gefragt werden darf. Das könnte für den Arbeitgeber wichtig sein, weil er nach § 78 SGB IX verpflichtet ist, eine bestimmte Quote von Schwerbehinderten oder Gleichgestellten einzustellen. Wenn er nicht danach fragen darf, dann kann es ihm auch passieren, dass er nach einer Kündigung eines Arbeitnehmers innerhalb von drei Wochen nach der Kündigung einen Hinweis auf eine Schwerbehinderung erhält und damit ein Kündigungsschutz entsteht. Es bleibt bei der Rechtsprechung des BAG im Zeitalter des Antidiskriminierungsgesetzes: Ist ein bestimmter Gesundheitszustand oder das Nicht-Vorhandensein bestimmter Einschränkungen für einen Arbeitsplatz wesentlich, darf danach gefragt werden.[54] Ist das nicht der Fall, darf nach keiner Form

48 BT-Drs. 16/13657, 20; *Franzen*, ErfK, 2015, Rn. 3 zu § 32 BDSG; *Thüsing*, in: Thüsing, Beschäftigtendatenschutz und Compliance, 2014, § 3, Rn. 19.

49 *Pötters/Traut*, RDV 2013, 132, 133; *Schmidt*, DuD 2010, 207, 212; *Stamer/Kuhnke*, in: Plath, BDSG, 2013, Rn. 17 f. zu § 32; *Thüsing*, NZA 2009, 865, 868; *Thüsing*, in: Thüsing, Beschäftigtendatenschutz und Compliance, 2014, § 3, Rn. 16 f.; *Zöll*, in: Taeger/Gabel, BDSG, 2013, Rn. 18 zu § 32.

50 *Vogel/Glas*, DB 2009, 1747, 1751; in der Tendenz auch *Seifert*, in: Simitis, BDSG, 2014, Rn. 10 zu § 32, der die Belange der Arbeitnehmer bereits in einer strengen Durchführung des Maßstabes der Erforderlichkeit berücksichtigt sieht.

51 Z. B. *Pötters/Traut*, RDV 2013, 132, 134 ff.; *Zöll*, in: Taeger/Gabel, BDSG, 2013, Rn. 18 zu § 32.

52 So die Standardformel des BAG, vgl. *Däubler*, Gläserne Belegschaften?, 6. Aufl. 2015, Rn. 209; *Gola/Wronka*, Handbuch Arbeitnehmerdatenschutz, 6. Aufl. 2013, Rn. 474; *Thüsing/Forst*, in: Thüsing, Beschäftigtendatenschutz und Compliance, 2. Aufl. 2014, § 7, Rn. 18.

53 *Däubler*, Gläserne Belegschaften?, 2015, Rn. 219; *Thüsing/Forst*, in: Thüsing, Beschäftigtendatenschutz und Compliance, 2014, § 7, Rn. 29.

54 *Thüsing/Forst*, in: Thüsing, Beschäftigtendatenschutz und Compliance, 2014, § 7, Rn. 25; eingehend zum grundsätzlichen Verbot der Frage im Anbahnungs- und in den ersten sechs Monaten des Beschäftigungsverhältnisses *Husemann*, RdA 2014, 16, 24 f.

oder Schwere der Behinderung gefragt werden. Möchte der Arbeitgeber den Arbeitsplatz wegen besagter Quote mit einem Schwerbehinderten besetzen, kann er dies in der Ausschreibung deutlich machen und es dem Bewerber überlassen, freiwillig darauf hinzuweisen.
Fragen nach Fähigkeiten, Kenntnissen und Erfahrungen dienen der Beurteilung, ob der Bewerber für eine Stelle geeignet ist. Fachkundenachweise, die für bestimmte Tätigkeiten gesetzlich vorgeschrieben sind, müssen dokumentiert werden. Auch Angaben über private Vermögensverhältnisse des Bewerbers dürfen erhoben werden, wenn eine Tätigkeit angestrebt wird, die die Vornahme von Vermögensverfügungen vorsieht oder bei der eine erhöhte Gefahr der Bestechlichkeit oder Veruntreuung besteht.[55] Hier ist die umfangreiche Rechtsprechung der Arbeitsgerichte zum Fragerecht des Arbeitgebers von Bedeutung.
Es bleibt insoweit datenschutzrechtlich wie arbeitsrechtlich bei der Feststellung, dass der Arbeitgeber ein Fragerecht hat, wenn „der Arbeitgeber ein berechtigtes, billigenswertes und schutzwürdiges Interesse an der Beantwortung seiner Frage hat. Hinsichtlich sensibler Daten (Gesundheit, sexuelle Identität, Vorstrafen unter Beachtung von § 53 BZRG) gilt, dass die Antwort wegen der Art der auszuübenden Tätigkeit wesentlich sein muss.
Bei der Datenerhebung ist das Direkterhebungsprinzip des § 4 Abs. 2 BDSG zu beachten. Das schließt nicht aus, in Ausnahmefällen Daten auch bei Dritten erheben zu dürfen. Eine allgemeine Internetrecherche zu den Bewerbern ist allerdings unzulässig, denn auch hier gelten die inhaltlichen Grenzen des Fragerechts.[56] Nach überwiegender Auffassung dürfen aber im Bewerbungsverfahren Daten aus sozialen Netzwerken erhoben werden, soweit sie berufsbezogen sind.[57] Umstritten ist, ob dies auf § 28 Abs. 1 S. 1 Nr. 3 BDSG[58] oder § 32 Abs. 1 S. 1 BDSG[59] zu stützen ist. Die Einsichtnahme in berufliche soziale Netzwerke ist nur bei der Anbahnung eines Beschäftigungsverhältnisses zulässig, danach soll die Abwägung in der Regel ein ‚nein' ergeben.[60]
Generell gilt für Bewerberdaten, dass sie zu löschen sind, soweit sie für den Zweck der Einstellung nicht mehr benötigt werden. Es wird auch aus datenschutzrechtlicher Perspektive allerdings ein Aufbewahrungsrecht eingeräumt, solange Konkurrentenklagen nach dem Allgemeinen Gleichstellungsgesetz (AGG) möglich sind.[61]

b) Erforderlichkeit bei der Durchführung des Beschäftigungsverhältnisses

Stammdaten und alle Informationen, die aufgrund gesetzlicher Informations- und Dokumentationspflichten und zur Erfüllung von Arbeitgeberpflichten aus Gesetz, Tarifvertrag oder Betriebsvereinbarung benötigt werden, dürfen gespeichert und genutzt werden. Umstritten ist, ob Daten für Personalentwicklungsmaßnahmen und Qualifizierungsprogramme in sog. skill-Datenbanken verarbeitet werden dürfen. Die allgemeine Ansicht[62] ist, dass dies nur mit Einwilligung der betroffenen Arbeitnehmer zulässig ist.
Mitarbeiterdaten dürfen im Internet öffentlich gemacht werden, wenn Außenkontakte bestehen. ‚Öffentlich zugänglich machen' ist eine Form der Verarbeitung, für die eine Erlaubnis vorliegen muss. Name, Funktion und Kontaktdaten dürfen für eine Kontaktaufnahme angegeben werden. Das Einstellen eines Beschäftigtenfotos auf der Internetseite des Arbeitgebers ist nach einem BAG-Urteil allerdings nicht nach § 32 BDSG, sondern nach den §§ 22, 23 KUG zu beurteilen.[63] Eine in der Regel schriftliche Einwilligung des Beschäftigten ist hierzu erforderlich, soweit nicht die Ausnahmen des § 23 Abs. 1 KUG (v. a. Person nur Beiwerk) greifen.

c) Erforderlichkeit bei der Beendigung des Beschäftigungsverhältnisses

Im Zusammenhang mit der Beendigung des Beschäftigungsverhältnisses fallen eine Reihe spezifischer personenbezogener Daten an, insbesondere wenn die Beendigung nicht einvernehmlich erfolgt.
Gemäß § 32 Abs. 1 S. 1 BDSG dürfen Beschäftigtendaten erhoben, verarbeitet oder genutzt werden, soweit dies für die Beendigung erforderlich ist. Das können einerseits Daten sein, die die rechtlichen Schritte der Beendigung bzw. der Abwicklung des Beschäftigungsverhältnisses betreffen (z. B. Kündigungserklärungen, Aufhebungsvereinbarungen). Nicht selten müssen auch Daten speziell für die Abwicklung erhoben werden, z. B. für die Berechnung einer Abfindung. Andererseits geht es um Daten, die der Arbeitgeber im Zuge eines Beendigungskonflikts benötigt (z. B. Abmahnungen, Überwachungsprotokolle, Fehlzeiten, Kriterien der sozialen Auswahl).
Bei Beendigung des Beschäftigungsverhältnisses stellt sich zudem die Frage der Löschung von personenbezogenen Daten, die nicht mehr benötigt werden. Personenbezogene Daten sind gemäß § 35 Abs. 2 S. 2 Nr. 3 BDSG zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Grundsätzlich werden nach dem Beschäftigungsende Durchführungsdaten nicht mehr benötigt. Allerdings gibt es vielfältige Aufbewahrungspflichten des Arbeitgebers, die einer Löschung entgegenstehen.[64] So sehen z. B. § 16 Abs. 2 ArbZG und § 17 Abs. 1 MiLoG eine zweijährige Aufbewahrungspflicht für personenbezogene Arbeitszeitdaten vor. Beendigungsdaten werden nicht mehr benötigt, wenn daraus keine Rechte mehr abgeleitet werden können. So verjährt der Anspruch auf ein Arbeitszeugnis gemäß § 195 BGB nach drei Jahren, so dass dafür erforderliche Daten danach zu löschen sind. Tarifliche Ausschlussfristen können für viele Daten schon nach einigen Monaten die Aufbewahrung entbehrlich machen.

d) Erforderlichkeit bei der Datenerhebung zur Aufdeckung von Straftaten

Anders sieht dies bei § 32 Abs. 1 S. 2 BDSG aus, der die Datenerhebung zur Aufdeckung von Straftaten betrifft. Hier ist die abschließende Abwägung mit den schutzwürdigen Interessen der Arbeitnehmer ausdrücklich vorgesehen. Danach unterbleibt selbst das zur Aufdeckung Erforderliche, wenn es unverhältnismäßig ist. Entsprechend hat das BAG am 20.6.2013[65] klargestellt, dass § 32 Abs. 1 S. 2 BDSG „eine am Verhältnismäßigkeitsprinzip orientierte, die Interessen des Arbeitgebers und des Beschäftigten berücksichtigende Abwägung im

55 *Däubler*, Gläserne Belegschaften?, 2015, Rn. 220c, unterscheidet, dass das Fragerecht bei einem Finanzdirektor, nicht aber bei einem Kassierer gegeben sei.
56 *Kania/Sansone*, NZA 2012, 360, 363; *Stamer/Kuhnke*, in: Plath, BDSG, 2013, Rn. 27 zu § 32; *Zöll*, in: Taeger/Gabel, BDSG, 2013, Rn. 21 zu § 32.
57 *Bissels/Lützeler/Wisskirchen*, BB 2010, 2433, 2436 f.; *Kania/Sansone*, NZA 2012, 360, 364; *Stamer/Kuhnke*, in: Plath, BDSG, 2013, Rn. 27 zu § 32; *Zöll*, in: Taeger/Gabel, BDSG, 2013, Rn. 22 zu § 32; gegen diese Einschränkung *Ernst*, NJOZ 2011, 953, 955.
58 *Bissels/Lützeler/Wisskirchen*, BB 2010, 2433, 2436 f.; *Stamer/Kuhnke*, in: Plath, BDSG, 2013, Rn. 27 zu § 32.
59 Die Bundesregierung teilte in ihrer Antwort auf eine Kleine Anfrage am 10.4.2014 mit, dass auch für die Erhebung von Daten in sozialen Netzwerken und Internetforen die allgemeinen Grundsätze aus § 32 Abs. 1 S. 1 BDSG anzuwenden seien (BT-Drs. 18/1122, 2).
60 Jedenfalls die routinemäßige, anlasslose Überprüfung der Äußerungen sämtlicher Beschäftigter in Social Media und der von ihnen eingestellten Angebote auf Internetverkaufsplattformen sowie ganz allgemein das Googeln ihrer Namen ist laut *Thüsing/Traut*, in: Thüsing, Beschäftigtendatenschutz und Compliance, 2014, § 14, Rn. 37) unzulässig.
61 *Gola/Schomerus*, BDSG, 2015, Rn. 15 zu § 32.
62 Z. B. *Däubler*, Gläserne Belegschaft?, 2015, Rn. 262.
63 BAG, 11.12.2014 – 8 AZR 1010/13, BB 2015, 1276, K&R 2015, 433, NZA 2015, 604, Rn. 11, 12.
64 *Gola/Schomerus*, BDSG, 2015, Rn. 36 zu § 32.
65 BAG, 20.6.2013 – 8 AZR 1010/13, BB 2014, 890, NZA 2014, 143, Rn. 26.

Einzelfall" voraussetze. Eine heimliche Spindöffnung zur Aufklärung eines Diebstahls sei zwar geeignet, aber nicht erforderlich, um den Fall aufzuklären. Die Öffnung bei Anwesenheit des Arbeitnehmers wäre das mildere Mittel gewesen. Daher sei die Öffnung ein Eingriff in den Kernbereich privater Lebensgestaltung gewesen und damit rechtswidrig. Die bei der Spindöffnung festgestellten Tatsachen unterlägen daher dem Beweisverwertungsverbot. Das BAG hat eine Abwägung mit den grundrechtlich geschützten Interessen des Arbeitgebers – dem grundrechtlich geschützten Schutz seiner unternehmerischen Freiheit und seines Eigentumsrechts – nicht vorgenommen.

Besonders brisant war bei der Formulierung des § 32 BDSG im Jahre 2009 die Frage, welche Überwachungsmaßnahmen dem Arbeitgeber erlaubt werden sollen, um sich gegen Straftaten der Beschäftigten zu schützen. Denn vorausgegangen waren vielbeachtete „Datenschutzskandale" u. a. im Einzelhandel, in deren Verlauf insbesondere der Einsatz von Detektiven, die Verhaltensprotokolle von Mitarbeitern bis hinein in das Privatleben sowie Fotos erstellten, und das Installieren von Videokameras zur Überwachung der Beschäftigten thematisiert wurden. In § 32 Abs. 1 BDSG wurde daher in S. 2 ein weiterer spezieller Erlaubnistatbestand mit besonderen Grenzen für die Aufdeckung von Straftaten formuliert. Danach dürfen Beschäftigtendaten zur Aufdeckung von Straftaten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt. Insbesondere dürfen Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sein.

Diese Regelung erfordert also eine bereits begangene Straftat, die Maßnahmen nur gegenüber dem konkret Verdächtigen zulässt. § 32 Abs. 1 S. 2 BDSG ist dem klaren Wortlaut nach also keine Erlaubnisgrundlage, wenn nach begangener Straftat mehrere Beschäftigte ohne konkretisierende Hinweise als Täter in Betracht kommen. Die Vorschrift scheidet schon im Ansatz aus, wenn noch gar keine Straftaten vorliegen und lediglich präventiv die Entdeckungsgefahr erhöht werden soll.[66]

Unter Verweis auf seine ständige Rechtsprechung sieht es das BAG[67] auch unter Berücksichtigung des neuen § 32 Abs. 1 S. 2 BDSG bei Vorliegen einer Straftat grundsätzlich als zulässig an, zur Aufklärung, wer aus einer Beschäftigtengruppe der Täter ist, die gesamte Gruppe z. B. per Video zu überwachen. Weitere Voraussetzung ist allerdings, dass weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft sind.

Das BAG[68] hatte noch 2012 ein Beweisverwertungsverbot im Kündigungsschutzprozess abgelehnt, wenn eine – im Übrigen gegenüber den betroffenen Arbeitnehmern verhältnismäßige – Videoüberwachung öffentlich zugänglicher Räume durchgeführt wurde, ohne dass die gemäß § 6b BDSG gebotene Kennzeichnung einer solchen Videoüberwachung vorgenommen wurde. Der damals zu entscheidende Sachverhalt fand vor Einführung des § 32 BDSG statt. In zwei neueren Entscheidungen hat das BAG[69] die Maßnahmen des Arbeitgebers (Videoüberwachung, Spindkontrolle) jeweils als unverhältnismäßig eingestuft und entschieden, dass Kündigungsgründe, die durch eine nicht von § 32 BDSG gedeckte Datenerhebung festgestellt wurden, nach § 286 Abs. 1 ZPO nicht verwertet werden dürfen.

Rein präventiven Maßnahmen zur Verhinderung von Rechtsverstößen, also z. B. eine Videoüberwachung oder ein Datenscreening ohne konkret vorliegende Straftaten lassen sich nicht unter § 32 Abs. 1 S. 2 BDSG subsumieren. Eine verdachtsunabhängige Erforschung von Rechtsverletzungen im Rahmen etwa von Compliance-Maßnahmen muss aber möglich sein. Der Gesetzgeber hat daher klargestellt, dass verdachtsunabhängige Ermittlungen unter § 32 Abs. 1 S. 1 BDSG fallen,[70] während die Weiterverfolgung von in dieser Weise ermittelten Verdachtsfällen, also die tatsächliche Aufdeckung der Straftat, am strengeren Maßstab des § 32 Abs. 1 S. 2 BDSG zu messen ist. Bei Kontrollen im Rahmen von Compliance-Maßnahmen sind flächendeckende Vollkontrollen nicht erlaubt, sondern eher Stichproben. Eine verdachtsunabhängige dauernde – verdeckte oder offene – Videoüberwachung zur Kontrolle von Beschäftigten wäre danach nicht zulässig.[71]

V. Festlegung des Nutzungszwecks

Die grundlegende Erlaubnisnorm der Datenerhebung und -verwendung im geschäftlichen Verkehr findet sich in § 28 BDSG. Für Vertragszwecke ist insbesondere § 28 Abs. 1 S. 1 Nr. 1 BDSG maßgeblich, der bis zur Inkraftsetzung von § 32 BDSG im Jahre 2009 auch für den Arbeitsvertrag galt. Seitdem mit § 32 BDSG eine Spezialregelung existiert, stellt sich die Frage, inwieweit Erlaubnistatbestände des § 28 BDSG neben § 32 BDSG bei der Verarbeitung von Beschäftigtendaten noch Geltung beanspruchen können.[72] So ist umstritten, ob § 28 Abs. 1 S. 2 BDSG von § 32 BDSG verdrängt wird oder ergänzend zur Anwendung kommen kann. Wenn personenbezogene Daten von Beschäftigten zulässigerweise erhoben werden, ist zu klären, ob für die Erhebung und die anschließende Speicherung sowie alle weiteren Verarbeitungen der Zweck festzulegen und zu dokumentieren ist. Im Bericht des Innenausschusses des Deutschen Bundestages[73] heißt es dazu, dass § 32 auch den § 28 Abs. 1 S. 2 BDSG verdränge, der bestimmt, dass bei der Erhebung die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen sind. Der Zweck werde in § 32 BDSG umfassend festgelegt, nämlich Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses. Eines Rückgriffs auf § 28 Abs. 1 S. 2 BDSG bedürfe es daher nicht. Es bräuchten die Zwecke der für das Beschäftigungsverhältnis erhobenen Daten nicht detaillierter als in § 32 BDSG normativ vorgesehen angegeben zu werden.

Diese Ansicht überzeugt nicht.[74] Die Zweckbindung der Datenerhebung ist ein wichtiges Prinzip des Datenschutzrechts. Im Interesse der Datensparsamkeit muss ein unmittelbarer Zusammenhang zwischen Speicherung und konkretem Verwendungszweck bestehen.[75] Entfällt daher der Zweck oder sind die Daten für die Erfüllung des Zwecks nicht mehr erforderlich, sind sie nach § 35 Abs. 2 S. 2 Ziff. 3 BDSG zu löschen. Der gesetzliche Zwang, den Erhebungszweck konkret festzulegen, soll helfen, die Erforderlichkeit der Speicherung präzise zu ermitteln und im Blick zu behalten. Wenn die Norm, § 32 Abs. 1 BDSG, nur geltendes Recht festschreiben soll, wie der Gesetzgeber zu-

66 Zur Abgrenzung im Detail *Zöll*, in: Taeger/Gabel, BDSG, 2013, Rn. 48 zu § 32.
67 BAG, 21.11.2013 – 2 AZR 797/11, NZA 2014, 243, Rn. 50.
68 BAG, 21.6.2012 – 2 AZR 153/11, BB 2013, 125, NZA 2012, 1025, Rn. 21 ff.
69 BAG, 20.6.2013 – 2 AZR 546/12, BB 2014, 890, NZA 2014, 143, Rn. 18 ff. (Spindkontrolle); BAG, 21.11.2013 – 2 AZR 797/11, NZA 2014, 243, Rn. 42 ff. (Videoüberwachung).
70 BT-Drs. 16/13657, 21; *Zöll*, in: Taeger/Gabel, BDSG, 2013, Rn. 48 zu § 32.
71 *Däubler*, Gläserne Belegschaft?, 2015, Rn. 312b; a. A. *Pötters/Traut*, RDV 2013, 132, 138, die auch ständigen Überwachungsdruck u. U. für zulässig halten.
72 Eingehend *Zöll*, in: Taeger/Gabel, BDSG, 2013, Rn. 6 ff. zu § 32.
73 BT-Drs. 16/13657, 20 f.
74 *Stamer/Kuhnke*, in: Plath, BDSG, 2013, Rn. 10 zu § 32; *Thüsing*, NZA 2009, 865, 869.
75 *Meents/Hinzpeter*, in: Taeger/Gabel, BDSG, 2013, Rn. 25 zu § 35,

vor im selben Dokument schreibt,[76] dann müssen die einzelnen Zwecke auch weiterhin im Arbeitsverhältnis detailliert bestimmt werden.
Es deutet nichts darauf hin, dass mit § 32 BDSG der Beschäftigtendatenschutz entschärft werden sollte. Insoweit scheint die Formulierung in der Begründung des Innenausschusses, dass § 28 Abs. 1 S. 2 verdrängt werde, wohl tatsächlich „unbedacht gewählt" zu sein.[77] Die Gesetzessystematik spricht jedenfalls für die Anwendung der Zweckbestimmungspflicht auch im Arbeitsverhältnis. Wenn in § 32 Abs. 1 S. 1 BDSG formuliert wird, dass die Daten für Beschäftigungszwecke verwendet werden, dann ist damit nur sehr weit der sachliche Anwendungsbereich beschrieben worden. Auch in § 28 Abs. 1 S. 1 BDSG heißt es ähnlich, dass die Verarbeitung „als Mittel für die Erfüllung eigener Geschäftszwecke" erfolgt. Auch hier wird allein der Anwendungsbereich festgelegt. Bei § 28 BDSG genügt es dann ausdrücklich nicht, festzuhalten, dass die Daten von Kunden für Geschäftszwecke benötigt werden, sondern es muss eben nach § 28 Abs. 1 S. 2 BDSG der Zweck genauer angegeben werden. In Bezug auf § 32 BDSG besteht genau dasselbe systematische Bedürfnis, dass auch hier der Zweck konkretisiert wird: Angaben zu Fehlzeiten werden für das betriebliche Wiedereingliederungsmanagement verwendet; Mitgliedschaft in der Gewerkschaft wird für das Abführen von Mitgliedsbeiträgen verwendet; Daten zu den Unterhaltsverpflichtungen der Beschäftigten dienen der Durchführung der sozialen Auswahl bei einem Stellenabbau. Im Übrigen sind die Angaben zur Zweckbestimmung auch Gegenstand der Verarbeitungsübersichten nach § 4e BDSG.

VI. Kontrolle des Arbeitnehmerdatenschutzes

Die Einhaltung der Vorschriften zum Beschäftigtendatenschutz wird auf verschiedenen Wegen sichergestellt. Für den Fall, dass ein Durchsetzungsinstrument versagt, besteht so die Möglichkeit, dass ein anderes greift.

1. Persönliche Kontrolle durch den Arbeitnehmer

Zunächst hat der Beschäftigte selbst einen Anspruch darauf, zu erfahren, welche Daten über ihn erhoben und verarbeitet werden. Er hat nach den §§ 34, 35 BDSG ein Recht auf Auskunft, Berichtigung, Sperrung, Löschung. Er kann sich zudem an den Betriebsrat gemäß § 85 BetrVG und an den betrieblichen Datenschutzbeauftragten gemäß § 4f Abs. 5 BDSG wenden. Dieser muss die Meldung des Betroffenen gemäß § 4f Abs. 4 BDSG vertraulich behandeln, bewerten, gegebenenfalls aktiv werden und den Betroffenen hierüber unterrichten.[78] Auch an die Aufsichtsbehörde für den Datenschutz kann sich ein betroffener Arbeitnehmer wenden; jedoch sind hierbei Rücksichtnahmepflichten auf den Arbeitgeber zu beachten.[79] Bei einer sorgfaltswidrigen Verletzung der Persönlichkeit stehen einem Betroffenen auch Schadensersatzansprüche aus § 7 BDSG und aus §§ 823 Abs. 1 und Abs. 2 BGB – hier i.V.m. mit dem Datenschutzgesetz als Schutzgesetz – zu.
Diese Rechte werden auch bei Geltung der DSGVO erhalten bleiben, insbesondere die Rechte der Betroffenen nach Kapitel III der DSGVO. Allerdings werden beim Recht auf Auskunft dann Grenzen gesetzt, wenn die Auskunft Betriebs- und Geschäftsgeheimnisse bei dem für die Verarbeitung Verantwortlichen berührt, was zuletzt bei der Frage nach dem Auskunftsanspruch gegenüber einer Auskunftei hinsichtlich der einen Score berechnenden Algorithmen diskutiert wurde.[80] Erwägungsgrund 51 S. 5 bestätigt, dass Auskunftsrechte ihre Grenze u. a. bei Betriebsgeheimnissen finden.

2. Betrieblicher Datenschutzbeauftragter

Daneben nimmt der betriebliche Datenschutzbeauftragte seine Kontrollfunktion im Rahmen der Selbstkontrolle der verantwortlichen Stelle wahr. Ein betrieblicher Datenschutzbeauftragter ist gem. § 4f BDSG zu bestellen, wenn regelmäßig mehr als neun Personen beschäftigt werden, die Zugang zu personenbezogenen Daten im Unternehmen haben.
Bemerkenswert ist, dass auch schon dann ein betrieblicher Datenschutzbeauftragter zu bestellen ist, wenn von diesem eine Vorabkontrolle durchzuführen ist. In einem Verfahren, das bis zum OVG Lüneburg[81] ging, hatte eine Oldenburger Ein-Personen-GmbH als Eigentümerin eines Bürohauses aufgrund von Diebstahls von Notebooks mit sensiblen Daten aus einem Büro eine Videoüberwachungsanlage im Treppenhaus installiert. Die Aufsichtsbehörde hielt hier wegen der besondere Risiken für die Verletzung von Persönlichkeitsrechten eine Vorabkontrolle für erforderlich, so dass die GmbH, die keine Angestellten hat, einen betrieblichen Datenschutzbeauftragten bestellen musste, damit von diesem die gutachtliche Stellungnahme im Rahmen der Vorabkontrolle erstellt werden konnte. Schon deswegen erscheint es bei Kleinen und Mittleren Unternehmen häufig sinnvoll, dass mit der Aufgabe des betrieblichen Datenschutzbeauftragten auch eine externe Person beauftragt werden kann.
Neben den Aufsichtsbehörden, an den sich Betroffene auch weiterhin wenden können, bleiben die betrieblichen Datenschutzbeauftragten ein wichtiges Kontrollinstrument. Die DSGVO sieht hinsichtlich einer umfassenden Bestellpflicht bedauerlicherweise keine Vollharmonisierung vor, sondern überlässt es mit einer weiteren Öffnungsklausel den Mitgliedstaaten, über die in Art. 35 Abs. 1 DSGVO vorgesehenen Fälle hinaus vor, eine Pflicht zur Bestellung von betrieblichen Datenschutzbeauftragten zu regeln. Nach Art. 35 Abs. 1 DSGVO besteht eine Bestellpflicht nur für öffentliche Stellen (a) und dann, wenn die Verarbeitungsvorgänge „aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen" (b) oder wenn die Kerntätigkeit der verarbeitenden Stelle „in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 9a besteht" (c). Art. 35 Abs. 8 SGVO stellt es frei, ob zum Datenschutzbeauftragten ein Beschäftigter (interner) oder ein externer Dienstleister bestellt wird. Beide müssen die erforderliche berufliche Qualifikation und das Fachwissen besitzen (Art. 35 Abs. 5 DSGVO).[82] Dass der Datenschutzbeauftragte weiterhin unabhängig und weisungsfrei arbeitet und nicht wegen der Erfüllung seiner Aufgaben abberufen oder benachteiligt wird, stellt Art. 36 Abs. 3 DSGVO sicher.
Es ist davon auszugehen, dass Deutschland von der Option des Art. 35 Abs. 4 DSGVO Gebrauch machen wird, um mit § 4f BDSG oder mit einer entsprechenden Nachfolgeregelung die Bestellpflicht in bisherigem Umfang beizubehalten. Es gibt derzeit keine Hinweise, dass der deutsche Gesetzgeber die Bestellpflicht an die Unternehmensgröße koppeln wird.

76 BT-Drs. 16/13657, 20.
77 *Stamer/Kuhnke*, in: Plath, BDSG, 2013, Rn. 10 zu § 32 unter Verweis auf *Thüsing*, NZA 865, 869.
78 *Simitis*, in: Simitis, BDSG, 2014, Rn. 163 und 166 zu § 4f.
79 *Rudkowski*, CCZ 2013, 204, 205 f.
80 S. dazu *Taeger*, K&R 2014, Heft 10, Beihefter 4, S. 4, und *ders.*, Anmerkung zu einer Entscheidung des BGH vom 28.1.2014 (VI ZR 156/13; MMR 2014, 489) – Zum Umfang einer von der SCHUFA zu erteilenden Auskunft, MMR 2014, 492.
81 OVG Lüneburg, 29.9.2014 – 11 LC 114/13, NJW 2015, 502.
82 S. hierzu und zum Folgenden auch den Erwägungsgrund 75.

3. Betriebsrat

Der Betriebsrat hat gemäß § 80 Abs. 1 Ziff. 1 BetrVG darüber zu wachen, dass die zu Gunsten der Arbeitnehmer geltenden Gesetze und andere Vorschriften beachtet werden. Hierzu gehören auch das Bundesdatenschutzgesetz und andere den Datenschutz regelnde Vorschriften.[83] Daher ist der Arbeitgeber verpflichtet, den Betriebsrat umfassend über alle Formen der Verarbeitung personenbezogener Daten der Arbeitnehmer zu unterrichten. Der Betriebsrat hat nicht nur darüber zu wachen, dass – soweit gesetzlich erforderlich – ein betrieblicher Datenschutzbeauftragter bestellt wird. Er hat darüber hinaus selbst eine Kontrolle über die Einhaltung des Datenschutzrechts durchzuführen, soweit Beschäftigte betroffen sind.[84]

Zur Erfüllung seiner Pflichten nimmt der Betriebsrat Anregungen und Beschwerden der Beschäftigten im Bereich des Datenschutzes gemäß §§ 80 Abs. 1 Ziff. 3 und 85 BetrVG entgegen, um sie, falls sie berechtigt erscheinen, gegenüber dem Arbeitgeber zu vertreten. Weiter nimmt der Betriebsrat sein Mitbestimmungsrecht aus § 87 Abs. 1 Ziff. 6 BetrVG wahr, das sich allerdings nur auf jenen Teil des Datenschutzes erstreckt, der technische Überwachungseinrichtungen betrifft. Weitere Fragen des Datenschutzes kann der Betriebsrat in freiwilligen Betriebsvereinbarungen gemäß § 88 BetrVG mit dem Arbeitgeber regeln, soweit dieser dazu bereit ist.[85]

Arbeitnehmervertretungen werden prüfen, ob sie nach Inkrafttreten der Datenschutzgrundverordnung Einrichtungen, Organisationen und Vereinigungen nach Art. 76 DSGVO sind und im Auftrag einer betroffenen Person Beschwerde einlegen sowie deren Rechte wahrnehmen und einen Schadensersatzanspruch geltend machen dürfen. Der deutsche Gesetzgeber darf aufgrund der Öffnungsklausel in Art. 76 DSGVO auch vorsehen, dass auch ohne eine Beschwerde des Betroffenen den angesprochenen Einrichtungen, Organisationen und Vereinigungen ein ‚Verbandsklagerecht' eingeräumt wird, das bei einer Durchsetzung entsprechender politischer Forderungen auch Betriebsräten und Gewerkschaften eingeräumt werden könnte.

4. Verhältnis Betriebsrat – Datenschutzbeauftragter

Zunächst stellt sich die Frage, ob ein Mitglied des Betriebsrats zugleich betrieblicher Datenschutzbeauftragter sein kann. Der Gesetzeswortlaut verbietet es nicht. Das BDSG kennt den Betriebsrat überhaupt nicht. Wir müssen uns also mit den allgemeinen Anforderungen an den betrieblichen Datenschutzbeauftragten näher befassen. Das Gesetz verlangt gemäß § 4f Abs. 2 S. 1 BDSG, dass er die für das Amt erforderliche Fachkunde und Zuverlässigkeit besitzen muss. Hier steht die Frage im Raum, ob sich aus der Zuverlässigkeitsanforderung Argumente ergeben können, die gegen eine Bestellung eines Datenschutzbeauftragten sprechen, der Mitglied des Betriebsrates ist. Oder ob gar ein wichtiger Grund nach § 626 BGB vorliegt, einen bereits bestellten Datenschutzbeauftragten abzurufen, wenn er zum Mitglied des Betriebsrates gewählt wird.

Bei den subjektiven Zuverlässigkeitskriterien geht es um die persönliche und charakterliche Eignung, um Verfehlungen, Vorstrafen oder andere persönliche Verhaltensweisen, die Zweifel an der gebotenen Zuverlässigkeit aufkommen lassen.[86] Die Tatsache, Mitglied des Betriebsrats zu sein, gibt selbstredend keinen Anlass, an der persönlichen Integrität zu zweifeln.

Bei den objektiven Kriterien geht es um mögliche Interessenkollisionen.[87] Übt der betriebliche Datenschutzbeauftragte das Amt neben einem anderen Amt aus, kann die Situation eintreten, dass er sich selbst kontrolliert und dabei naturgemäß Interessenkonflikte auftreten können. Deshalb gilt es als ausgeschlossen, dass Mitglieder der Geschäftsleitung, die Leitung der IT oder der Systemadministration, Leiter Personal oder Mitarbeiter aus der Revision betriebliche Datenschutzbeauftragte sein können.[88]

Hoch umstritten ist es, ob es eine Interessenkollision auch im Verhältnis Betriebsrat – betrieblicher Datenschutzbeauftragter geben kann.[89] Zunächst einmal verfolgen beide Institutionen die Einhaltung der Datenschutzvorschriften, der Betriebsrat aus §§ 75 und 80 BetrVG und der betriebliche Datenschutzbeauftragte aufgrund seiner Aufgaben und Befugnisse nach dem BDSG.

Es kann aber auch gut zu Konflikten zwischen den Rollen des Datenschutzbeauftragten und des Betriebsrats kommen, u. a. wegen der Möglichkeit des Datenschutzbeauftragten, auch die Datenverarbeitung des Betriebsrats zu kontrollieren.[90] Problematisch ist insoweit auch, dass der betriebliche Datenschutzbeauftragte aufgrund seiner umfassenden Kontrollfunktion auch Zugang zu Dateien haben kann, in die der Betriebsrat kein Einsichtsrecht hat.

Schließlich muss sich ein Betriebsrat klar und unter Umständen auch streitig gegenüber der Unternehmensleitung positionieren. Der betriebliche Datenschutzbeauftragte hat bei Defiziten im Datenschutz die Unternehmensleitung darauf hinzuweisen und kann sich bei unterschiedlichen Auffassungen auch an die Aufsichtsbehörde wenden. Er wird sich aber nicht öffentlich gegenüber der Geschäftsleitung positionieren.

Aus diesen Gründen ist es entgegen einer Entscheidung des Bundesarbeitsgerichts[91] eher problematisch, dass ein Betriebsrat zugleich das Amt des betrieblichen Datenschutzbeauftragten einnimmt.[92]

Die Datenschutzgrundverordnung bringt in dieser Frage keine Klarheit. Art. 36 Abs. 4a DSGVO sieht insofern auch nur vor, dass der betriebliche Datenschutzbeauftragte auch andere Aufgaben und Pflichten wahrnehmen kann, dass derartige Aufgaben und Pflichten aber nicht zu einem Interessenkonflikt führen dürfen.

In diesem Zusammenhang wurde ein weiteres kontroverses Thema angesprochen. Es fragt sich, ob der Datenschutzbeauftragte überhaupt die Datenverarbeitung des Betriebsrats kontrollieren darf. Das BAG entschied 1997, dass keine Kontrollbefugnis des Datenschutzbeauftragten gegenüber dem Betriebsrat bestehe; denn er sei ‚verlängerter Arm des Arbeitgebers' und nicht neutral.[93] Dieses Urteil kann keinen Bestand mehr haben.[94] Gab es schon damals gute Argumente, die gegen diese Entscheidung sprachen, so ist nach der Änderung des BDSG von 2009 anzuerkennen, dass die Unabhängigkeit des betrieblichen Datenschutzbeauftragten weiter gestärkt wurde, etwa durch den erwähnten Kündigungsschutz.[95] Der betriebliche Datenschutzbeauftragte hat unmittel-

83 Schon BAG vom 17.3.1987 – 1 ABR 59/85, BB 1987, 1806, NZA 1987, 747.
84 *Thüsing*, in: Richardi, BetrVG, 2014, Rn. 8 zu § 80.
85 *Richardi*, in: Richardi, BetrVG, 2014, Rn. 89 zu § 77.
86 *Gola/Wronka*, Handbuch Arbeitnehmerdatenschutz, 2013, Rn. 1484.
87 *Scheja*, in: Taeger/Gabel, BDSG, 2013, Rn. 72 zu § 4f.
88 V. d. *Bussche*, in: Plath, BDSG, 2013, Rn. 31 zu § 4f.; *Simitis*, in: Simitis, BDSG, 2014, Rn. 97 ff. zu § 4f.
89 V. d. *Bussche*, in: Plath, BDSG, 2013, Rn. 32 zu § 4f.
90 Streitig, zuletzt hat das BAG die Kontrolle des Betriebsrates durch den Datenschutzbeauftragten ausdrücklich dahinstehen lassen, BAG, 23.3.2011 – 10 AZR 562/09, BB 2011, 2683, NZA 2011, 1036, 1038.
91 BAG vom 23.3.2011 – 10 AZR 562/09, BB 2011, 2683, NZA 2011, 1036.
92 So auch *Kröpelin/Dzida*, NZA 2011, 1018; *Simitis*, in: Simitis, BDSG, 2014, Rn. 108 zu § 4f.
93 BAG vom 11.11.1997 – 1 ABR 21/97, BB 1998, 897, NJW 1998, 2466, 2467 f.
94 Kritisch auch *Scheja*, in: Taeger/Gabel, BDSG, 2013, Rn. 13 zu § 4g; v. d. *Bussche*, in: Plath, BDSG, 2013, Rn. 30 ff. zu § 4g; differenzierend: *Simitis*, in: Simitis, BDSG, 2014, Rn. 40 zu § 4g.
95 V. d. *Bussche*, in: Plath, BDSG, 2013, Rn. 30 zu § 4g.

baren Zugang zur Geschäftsleitung und kann mit dieser Datenschutzfragen erörtern.

Abschließend ist festzustellen, dass der Betriebsrat Teil der verantwortlichen Stelle ist und keinesfalls ein ‚Dritter'.[96] Die Übersendung von Listen mit personenbezogenen Arbeitnehmerdaten stellt dementsprechend auch keine Übermittlung dar, sondern eine Nutzung. In der Praxis ergeben sich aus der Konstellation Arbeitgeber – Betriebsrat – Datenschutzbeauftragter bisweilen Rechtsfragen.[97] Dazu gehört die, dass der Arbeitgeber verpflichtet ist, dem Datenschutzbeauftragten Übersichten über die im Betrieb erfolgenden Datenverarbeitungsverfahren zu geben. Tatsächlich aber ist dem Arbeitgeber gar nicht bekannt, welche Datenverarbeitungsverfahren beim Betriebsrat eingesetzt werden, so dass er dieser Rechtspflicht, die den Datenschutzbeauftragten in die Lage versetzt, seine Kontrolle gezielt vorzunehmen, gar nicht erfüllen kann.

5. Kontrolle durch Aufsichtsbehörden

Schließlich kann auch die zuständige Landesaufsichtsbehörde für den Datenschutz die Einhaltung der Datenschutzvorschriften überprüfen. Aus § 38 BDSG ergeben sich vielfältige Möglichkeiten der Behörden, Verstöße zu ermitteln. Gemäß § 38 Abs. 5 BDSG können sie bei Verstößen Maßnahmen anordnen. Zwangs- und Bußgelder können verhängt werden. Ein Blick in den Katalog der §§ 42, 44 BDSG zeigt, dass kaum eine Anforderung aus dem BDSG oder anderen Datenschutzvorschriften nicht als Ordnungswidrigkeit mit einem Bußgeld oder gar mit Strafe bewehrt ist. § 42a BDSG sieht eine Informationspflicht gegenüber Betroffenen, Behörden und eventuell der Öffentlichkeit bei unrechtmäßiger Kenntniserlangung von Daten vor. Das ist eine neue, aus den USA kommende Idee, die nicht nur zur Information der Betroffenen, sondern auch zu einem erheblichen Imageverlust des rechtswidrig handelnden Unternehmens führen kann.[98]

Auch die Datenschutzgrundverordnung sieht vor, dass in den Mitgliedstaaten eine oder mehrere Aufsichtsbehörden die Einhaltung des Datenschutzrechts „überwachen und durchsetzen" sowie aufklären und beraten (Art. 52 DSGVO).

VII. Betriebsratsrechte vs. Datenschutz

Mehrfach bereits hatte sich die Rechtsprechung mit der Frage zu beschäftigen, welche datenschutzrechtlichen Grenzen den Informationsansprüchen des Betriebs- bzw. Personalrates gesetzt sind.

1. Betriebliches Eingliederungsmanagement

Das erste Beispiel betrifft das Betriebliche Eingliederungsmanagement (BEM). Es ist nach § 84 Abs. 2 SGB IX für Arbeitnehmer vorgesehen, die innerhalb eines Jahres länger als sechs Wochen arbeitsunfähig waren. Die Vorschrift erging im Interesse der Arbeitnehmer; gleichwohl besteht die Besorgnis, dass die Daten aus diesem Verfahren auch einer krankheitsbedingten Kündigung Vorschub leisten könnten. Deshalb bedarf das Verfahren der Zustimmung des Betroffenen. § 84 Abs. 2 SGB IX geht dem BDSG vor. Zustimmung ist auch nicht mit Einwilligung im Sinne von § 4a BDSG gleichzusetzen, so dass es auch nicht der hohen formalen Anforderungen des BDSG an die Wirksamkeit einer Einwilligung bedarf. Die Daten, die aufgrund der Zustimmung erhoben und gespeichert werden, dürfen dann nur für Zwecke des Eingliederungsmanagements genutzt werden.

Auch hier kommt wieder das Verhältnis zum Betriebsrat ins Spiel. Die Regelungen zum Eingliederungsverfahren unterliegen seiner Mitbestimmung nach § 87 Abs. 1 Nr. 1 und Nr. 7 BetrVG. Das BAG hat 2012 entschieden,[99] dass der Betriebsrat verlangen kann, dass ihm der Arbeitgeber diejenigen Arbeitnehmer benennt, die die Voraussetzungen für die Durchführung des betrieblichen Eingliederungsmanagements erfüllen.

Diese Entscheidung ist in der Literatur auf Widerspruch gestoßen.[100] Das BAG verkenne, dass der Arbeitnehmer trotz des Informationsrechts des Betriebsrats aus § 80 BetrVG auch gesondert der Weitergabe seines Namens und der Daten, aus der sich die Notwendigkeit einer Eingliederungsmaßnahme ergeben, an den Betriebsrat zustimmen müsse. Das BAG hat sich in der Tat im Urteil nicht mit dem Selbstbestimmungsrecht des Arbeitnehmers auseinandergesetzt. Es räumt dem Überwachungsrecht des Betriebsrats ein höheres Gewicht ein als dem Grundrecht des einzelnen Arbeitnehmers auf informationelle Selbstbestimmung.

Verwaltungsgerichte gehen deshalb den Weg des BAG nicht mit. So hat etwa der BayVGH entschieden, dass § 84 Abs. 2 S. 7 SGB IX i.V.m. dem bayerischen Personalvertretungsgesetz der Personalvertretung kein Recht verleihe, vom Leiter einer Dienststelle ohne die Einwilligung der Betroffenen die Bekanntgabe der Namen der Personen verlangen zu können, denen ein betriebliches Eingliederungsmanagement angeboten wurde.[101]

Dem ist beizupflichten. Der Informationsanspruch aus § 80 BetrVG dient der Wahrnehmung von Mitbestimmungs- und Kontrollrechten des Betriebsrats. Beim betrieblichen Eingliederungsmanagement kann er diese Rechte auch wahrnehmen, wenn ihm anonymisierte Listen vorgelegt werden; ein Personenbezug ist nicht erforderlich. Aber selbst dann, wenn das Informationsinteresse des Betriebsrats über die Tatsache hinausgehen sollte, dass und wieviele Arbeitnehmer dem betrieblichen Eingliederungsmanagement unterliegen, so dürfen ihm jedenfalls keine Informationen über die Art und Schwere der Erkrankungen mitgeteilt werden.

2. Einsichtnahme des Betriebsrates in Lohn- und Gehaltslisten

Als weiteres Beispiel ist auf eine weitere, jüngere Entscheidung des BAG vom Januar 2014[102] hinzuweisen. Das Urteil gab dem Betriebsrat Recht, der vom Arbeitgeber eine Einsicht in alle Lohn- und Gehaltslisten verlangte. Der Arbeitgeber hatte dies mit dem Hinweis darauf verweigert, dass mehr als die Hälfte der Arbeitnehmer der Einsichtnahme widersprochen hatten. Das BAG sah hier aber gleichwohl einen Anspruch des Betriebsrats aus § 80 Abs. 1 Nr. 1 BetrVG. Der Betriebsrat habe darüber zu wachen, dass die sich aus § 75 Abs. 1 BetrVG ergebende Verpflichtung des Arbeitgebers zur Beachtung des allgemeinen Gleichheitsgrundsatzes eingehalten werde. Der Betriebsrat müsse sich ein Bild davon machen, ob die innerbetriebliche Lohngerechtigkeit beachtet werde. Hinsichtlich der Lohngestaltung könne

96 So auch BAG, 11.11.1997 – 1 ABR 21/97, BB 1998, 897, NJW 1998, 2466; zuletzt erneut BAG, 14.1.2014 – 1 ABR 54/12, NZA 2014, 738.
97 Näher *Kort*, NZA 2015, 1345, 1347.
98 Hierzu näher *Duisberg/Picot*, CR 2009, 823; *Gabel*, BB 2009, 2045.
99 BAG vom 7.2.2012 – 1 ABR 46/10, BB 2012, 2310, NZA 2012, 744.
100 *Kort*, Anmerkung zu BAG vom 7.2.2012 – 1 ABR 46/10, BB 2012, 2310, AP Nr. 4 zu § 84 SGB IX.
101 VGH München, 30.4.2009 – 17 P 08.3389, BeckRS 2010, 53777, s. allerdings BVerwG, 4.9.2012 – 6 P 5/11, NZA-RR 2013, 164.
102 BAG vom 14.1.2014 – 1 ABR 54/12, NZA 2014, 738.

ein Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 10 BetrVG in Betracht kommen.

Das BAG sah das Einsichtsrecht datenschutzrechtlich als eine zulässige Nutzung im Sinne des § 32 Abs. 1 S. 1 BDSG. Weil der Betriebsrat im Verhältnis zum Arbeitgeber Teil der verantwortlichen Stelle sei, handele es sich nicht um eine Datenübermittlung an einen Dritten. Im Übrigen könne sich der Arbeitgeber bei seiner Weigerung nicht auf das informationelle Selbstbestimmungsrecht der Arbeitnehmer aus Art. 2 Abs. 1 GG oder auf das entsprechende Grundrecht in Art. 8 EU-Grundrechtecharta berufen. Das Beteiligungsrecht des § 80 Abs. 1 Nr. 1 BetrVG diene der Sicherstellung eines ordnungsgemäßen Normvollzugs durch den Arbeitgeber. Das BAG hat deutlich gemacht, dass die Wahrnehmung der Betriebsratsrechte nach der Konzeption des Betriebsverfassungsgesetzes nicht zur Disposition der Arbeitnehmer stehe.

Das Ergebnis ist nicht überraschend; es entspricht der ständigen Rechtsprechung. Hier wird aber erstmals Bezug auf das Datenschutzrecht und das Selbstbestimmungsrecht der Arbeitnehmer genommen. Die Rechte werden für unbeachtlich erklärt, soweit Betriebsverfassungsrechte berührt sind.

VIII. Ausblick auf die DSGVO

Die eingehende Betrachtung zahlreicher Aspekte des Beschäftigtendatenschutzes hat deutlich gemacht, das trotz großer Bemühungen der Rechtsprechung, die Rechtslage zu klären, einige offene Fragen nach wie vor für Rechtsunsicherheit sorgen. Der Gesetzgeber ist also aufgefordert, den Beschäftigtendatenschutz gesetzlich präzise zu regeln.

Aktuell sind mit Einigung der europäischen Gesetzgebungsorgane auf die künftige EU-Datenschutzgrundverordnung im Dezember 2015 die Chancen auf ein spezielles nationales Beschäftigtendatenschutzgesetz deutlich gestiegen; denn die Endfassung der DSGVO, die mit hoher Wahrscheinlichkeit im Juli 2016 in Kraft tritt und zwei Jahre später unmittelbare Geltung in den Mitgliedsstaaten erlangt, enthält – wie bereits angesprochen – eine Öffnungsklausel in Art. 82 DSGVO für nationale Regelungen des Beschäftigtendatenschutzes, die allerdings an bestimmte inhaltliche Bedingungen geknüpft ist.

Zunächst ist zu beachten, dass mit Art. 91 DSGVO bestimmt wird, dass die DSGVO – wie für EU-Verordnungen gem. Art. 288 Abs. 2 S. 1 AEUV vorgesehen[103] – unmittelbar in den Mitgliedsstaaten anzuwenden sein wird.[104] Eine Umsetzung in nationales Recht, wie sie für EU-Richtlinien erforderlich ist, findet also nicht statt. Bei einem inhaltlichen Konflikt zwischen der DSGVO und dem nationalen Recht führt der Anwendungsvorrang dazu, dass jede der Verordnung „entgegenstehende Bestimmung des geltenden staatlichen Rechts ohne weiteres unanwendbar“ wird.[105] Der Verordnung kommt allerdings kein Geltungsvorrang zu.[106] Das entgegenstehende nationale Recht verliert also nicht automatisch seine Geltung. Es darf nur nicht angewendet werden. Es ist anzunehmen, dass der nationale Gesetzgeber diese zu noch mehr Rechtsunsicherheit führende Situation zu vermeiden trachtet und die der DSGVO widersprechenden Vorschriften durch ein Anpassungsgesetz außer Kraft setzen wird. Steht die nationale Norm nicht im Widerspruch zum Verordnungsrecht, sondern konkretisiert diese lediglich oder füllt Regelungslücken, kann sie jedoch – unabhängig davon, ob sie von einer Öffnungsklausel berührt ist – bestehen bleiben.

Die DSGVO enthält eine Reihe von Öffnungsklauseln, die für spezielle Regelungsfelder zu einer Regelungspflicht bzw. -option führen. Neben den Regelungsgeboten bestehen Handlungsoptionen, darunter gemäß Art. 82 DSGVO auch zugunsten einer Regelung des Beschäftigtendatenschutzes. Die Formulierung der Öffnungsklausel in Art. 82 DSGVO, die das gesamte Feld des Beschäftigtendatenschutzes betrifft, wirft mehrere Besonderheiten auf, die die weitere Rechtsentwicklung in Deutschland beeinflussen werden.[107]

Erstens sieht die Öffnungsklausel in Art. 82 Abs. 1 DSGVO vor, dass spezifischere Regelungen durch Gesetz oder Kollektivvereinbarung für den Beschäftigungskontext getroffen werden können. Es heißt nicht mehr, wie dies noch im Ursprungsentwurf der Kommission von 2012 der Fall war, dass solche spezifischeren Regelungen nur „in den Grenzen“ der DSGVO getroffen werden können. Nachdem diese Einschränkung entfallen ist, kann für den Beschäftigungskontext national nunmehr also ein eigenständiges Datenschutzregime entwickelt werden, das außer an übergeordnete Grund- und Menschenrechte einzig an den erst im Trilog 2015 hinzugefügten Art. 82 Nr. 2 DSGVO gebunden ist. Der Freiraum für nationale Regelungen ist also beträchtlich. Denn die gegenwärtig geltende Datenschutz-Richtlinie 95/46/EG, auf die die DSGVO folgt, enthält eine entsprechende Öffnungsklausel nicht. Nachdem ihr von der EuGH-Rechtsprechung vollharmonisierender Charakter zugesprochen worden ist,[108] engte sie daher den Spielraum des nationalen Gesetzgebers im Beschäftigtendatenschutz erheblich ein. Abweichungen zugunsten eines höheren Schutzniveaus nationaler Regelungen zum Beschäftigtendatenschutz standen daher im Verdacht, gegen die Richtlinie zu verstoßen. Dies wird sich mit der Öffnungsklausel der DSGVO ändern.

Zweitens hat der Trilog dem nationalen Gesetzgeber, der von der Öffnungsklausel im Beschäftigungskontext Gebrauch machen will, in Art. 82 Abs. 2 DSGVO konkrete Vorgaben gemacht. Seine Vorschriften müssen geeignete und besondere Maßnahmen umfassen, um die menschliche Würde, legitimen Interessen und grundlegenden Rechte der betroffenen Personen (also der Arbeitnehmer und Bewerber) zu gewährleisten, wobei besondere Beachtung der Transparenz der Datenverarbeitung, des Datentransfers in Unternehmensgruppen und Überwachungssystemen am Arbeitsplatz zu schenken ist.

Es wird abzuwarten sein, welche Bedeutung diese Vorgaben in der Rechtspraxis haben werden. Da europäisches Recht generell so auszulegen ist, dass es „praktische Wirksamkeit“[109] erlangt, muss Abs. 2 so verstanden werden, dass unter Geltung der DSGVO nur solche nationalen Regelungen des Beschäftigtendatenschutzes auf die Öffnungsklausel des Art. 82 DSGVO gestützt werden können, die diese Vorgaben auch tatsächlich umsetzen. Nationales Recht, das hinter den Vorgaben zurückfällt, wäre also unwirksam. Es ist derzeit davon auszugehen, dass der Gesetzgeber in einem Anpassungsgesetz die derzeitige Regelung des § 32 BDSG (zunächst) erhält und nicht schon bis zum Inkrafttreten 2018 zu einem umfassenden Beschäftigtendatenschutzgesetz ausbauen wird. Ob er die jetzige Regelung – im Kontext mit anderen Vorschriften – ergänzt, damit die Vorschriften zum Beschäftigtendatenschutz den Anforderungen aus Art. 82 Abs. 2

103 S. dazu näher *Geismann*, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, 2015, Art. 288 AEUV, Rn. 34.
104 Im Detail *Wybitul/Sörup/Pötters*, ZD 2015, 559, 559 f.
105 EuGH, 9.3.1978 – Rs. 106/77, Simmenthal II, Slg. 1978, 629, Rn. 17/18.
106 Vgl. *Ehlers*, in: Schulze/Zuleeg/Kadelbach, Europarecht, 2015, § 11, Rn. 48.
107 Vgl. auch *Wybitul/Fladung*, BB 2012, 509, 514.
108 Zuletzt EuGH, 24.11.2011 – C-468/10, C-469/10, K&R 2012, 40, NZA 2011, 1409.
109 *Potacs*, EuR 2009, 465, 467 f.

DSGVO auch „im Hinblick auf die Transparenz der Verarbeitung, die Datenübermittlung innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen und die Überwachungssysteme am Arbeitsplatz" genügen, wird sich zeigen.

Drittens wird in Art. 82 Abs. 2a DSGVO bestimmt, dass Mitgliedsstaaten, die von der Öffnungsklausel Gebrauch machen, die Vorschriften ihres nationalen Rechts, die bereits bestehen oder noch zu verabschieden sein werden,[110] innerhalb von zwei Jahren nach der Veröffentlichung im Amtsblatt, also zum Beginn der Geltung der DSGVO der Kommission, zu melden haben, was auch dazu führt, dass die deutschen Gerichte für die Normanwendung und -auslegung des § 32 BDSG weiter zuständig blieben. Im Interesse der Rechtsklarheit für die Rechtsunterworfenen ist also genau zu klären, wie das nationale Beschäftigtendatenschutz künftig aussehen soll. Belässt es der deutsche Gesetzgeber bei § 32 BDSG, gegebenenfalls mit ergänzenden Klarstellungen, oder einer inhaltsgleichen Nachfolgenorm, dann hat er diese Vorschrift neben anderen spezifischen für Beschäftigte geltende Datenschutzvorschriften der Kommission zu melden. Diese benannten Vorschriften kann er sodann künftig ändern, was dann der Kommission unverzüglich mitzuteilen ist. Er kann aber innerhalb der Frist auch einen erneuten Anlauf für ein komplexes Beschäftigtendatenschutzgesetz nehmen, wie es von Datenschutzaufsichtsbehörden[111] und von Seiten der Gewerkschaften gefordert wird.[112]

Alle Aspekte sprechen dafür, dass der nationale Gesetzgeber spätestens bis Frühjahr 2018 gehandelt haben muss, um unter Nutzung der Öffnungsklausel für den Beschäftigungskontext Datenschutzregelungen zu schaffen. Der nötige Freiraum ist durch die einerseits sehr offen formulierte Klausel geschaffen. Andererseits gibt es Vorgaben in Art. 82 Abs. 2 DSGVO, die durch das bestehende Beschäftigtendatenschutzrecht mit § 32 BDSG nicht abgedeckt sind. Es werden ausdrücklich spezifische Maßnahmen mit besonderer Beachtung von konkret genannten Problemkreisen gefordert. Dies ist mit dem § 32 BDSG allein nicht erfüllbar.

Vor welchen Optionen also steht jetzt der deutsche Gesetzgeber. Die Bandbreite reicht von schlichtem Nichthandeln bis zur Verabschiedung eines detaillierten Beschäftigtendatenschutzgesetzes. Es darf nicht außer Acht gelassen werden, dass der Gesetzgeber vor einer gewaltigen Herausforderung steht. Nicht nur im Bundesministerium des Innern, das für das BDSG zuständig ist, sondern in allen Ministerien wird zunächst zu prüfen sein, welche Datenschutzvorschriften weiter bestehen können, etwa weil sie aufgrund anderer Sekundärakte der Europäischen Union geschaffen wurden. Dass wir uns erst in einem Frühstadium der Anpassungsüberlegungen befinden, unterstreicht auch die Vergabe von Gutachtenaufträgen zur Feststellung des Anpassungsbedarfs.

Nach all' den Erfahrungen der letzten Jahrzehnte mag man vor diesem Hintergrund an ein komplexes, umfassendes Beschäftigtendatenschutzgesetz in absehbarer Zeit nicht glauben; wahrscheinlicher dürfte es sein, dass es zunächst bei § 32 BDSG oder einer inhaltsgleichen Nachfolgevorschrift bleibt, obwohl die Anforderung aus Art. 82 Abs. 2 DSGVO damit schwerlich erfüllt wären. Ein denkbares Szenario könnte sein, dass der Gesetzgeber diese Vorschrift um Regelungen ergänzt, die die Anforderungen des Art. 82 Abs. 2 DSGVO berücksichtigen. Die kommenden Jahre werden dann möglicherweise zu einem weiteren Ausbau dieser Vorschrift genutzt werden.

IX. Fazit

Als Fazit ist festzuhalten, dass auch nach Vorliegen der – bis auf redaktionelle Feinheiten – endgültigen Fassung der DSGVO, die der Rat für Justiz und Inneres am 21.4.2016 in erster Lesung beraten, über die Zukunft des Beschäftigtendatenschutzes und der jetzt noch geltenden Vorschriften, die im BDSG und den zahlreichen anderen Gesetzen die Verarbeitung von Arbeitnehmerdaten regeln, derzeit noch wenig Klarheit besteht. Sicher ist nur, dass eine Harmonisierung des Beschäftigtendatenschutzes innerhalb der Europäischen Union jedenfalls auf absehbare Zeit nicht zu erwarten sein wird.

Inhaltsverzeichnis: Seit mehr als 30 Jahren wird ein Gesetz zum Arbeitnehmerdatenschutz von allen Seiten gefordert, von den politischen Parteien, Gewerkschaften, Datenschutzaufsichtsbehörden und der Wissenschaft. In diesem Zeitraum hat sich die betriebliche Praxis der Datenverarbeitung mehrfach dramatisch verändert, wodurch immer neue Herausforderungen für den Datenschutz der Beschäftigten aufgetreten sind. Videoüberwachung, Dokumentenmanagementsysteme mit Leistungsdaten über Arbeitnehmer, private Nutzung von betrieblichen Kommunikationsmitteln und umgekehrt BYOD („Bring-Your-Own-Device"), genetische Untersuchungen, biometrische Zugangssysteme, GPS-Ortung der Dienstwagen, soziale Medien – das alles gab es früher nicht, bestimmt heute aber die Realität im Unternehmen. Es liegt auf der Hand, dass die Wahrung der Persönlichkeitsrechte von Arbeitnehmern im Unternehmen besonders vor dem Hintergrund der digitalen Erfassung von Daten ein wichtiges Thema ist. Im digitalen Zeitalter sind das berechtigte Informationsinteresse des Arbeitgebers und die Wahrung der Persönlichkeitsrechte der Beschäftigten mit einem Beschäftigtendatenschutzgesetz ausbalancieren, um Interessengegensätze auszugleichen. In diesem Zusammenhang gilt es auch, die Stellung des Betriebs- bzw. Personalrats zu regeln. Der Beitrag geht dabei vom aktuellen Stand des BDSG aus und verweist gleichzeitig auf die zu erwartenden Veränderungen aus der DSGVO.

Prof. Dr. Jürgen Taeger, Inhaber des Lehrstuhls für Bürgerliches Recht, Handels- und Wirtschaftsrecht an der Carl von Ossietzky Universität Oldenburg, Vorsitzender der Deutschen Stiftung für Recht und Informatik; Leiter des Studiengangs Informationsrecht LL.M. in Oldenburg.

Dr. Edgar Rose, Wissenschaftlicher Mitarbeiter am Lehrstuhl; Projektleiter des BMBF-Forschungsprojekts „Chancen und Risiken von Smart Cams im öffentichen Raum."

110 S. dazu näher *Wybitul/Sörup/Pötters*, ZD 2015, 559, 561.
111 S. die Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder v. 27.3.2014, Beschäftigtendatenschutz jetzt!
112 S. nur *Hayen*, CuA 3/2016, 20.