Marita Körner

Die Auswirkungen der Datenschutz-Grundverordnung (DSGVO) in der betrieblichen Praxis

HSI-Schriftenreihe
Band 28

Marita Körner

Die Auswirkungen der Datenschutz-Grundverordnung (DSGVO) in der betrieblichen Praxis

BUND
VERLAG

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

Herstellung: Kerstin Wilke
Umschlaggestaltung: Neil McBeath, Stuttgart
Satz: Reemers Publishing Services GmbH, Krefeld
Druck: CPI books GmbH, Leck
Printed in Germany 2019
ISBN 978-3-7663-6928-4

www.bund-verlag.de

Vorwort

Selten hat ein europäisches Projekt in den letzten Jahren so viel Aufregung in Unternehmen und Betrieben verursacht wie die EU-Datenschutz-Grundverordnung (DSGVO). Dies überrascht einerseits, weil das Datenschutzrecht hierdurch keineswegs neu erfunden wurde und auch ein ausreichender zeitlicher Vorlauf dem Inkrafttreten am 25.05.2018 vorausging. Andererseits werden durch die DSGVO neue Fragen und auch alte Fragen neu, wie z.B. die nach der Rolle von Betriebsräten, aufgeworfen. Die hierzu geführte datenschutz- und arbeitsrechtliche Debatte ist sehr lebhaft, auch, weil die betrieblichen Praktiker in Management und Betriebsräten selbstverständlich eine gewisse Rechtssicherheit anstreben.

Wir sind deshalb sehr froh, dass wir Prof. Dr. Marita Körner dafür gewinnen konnten, die Auswirkungen der Verordnung auf die betriebliche Praxis zu untersuchen. Ihr eingehendes Gutachten beantwortet betriebsnah die aufgetretenen Fragen und wird, wie wir glauben, die weitere Diskussion maßgeblich beeinflussen.

Dr. Thomas Klebe

Inhaltsübersicht

Vorwort 5

Einleitung 9

A. Hintergrund: Reform des Datenschutzes durch die DSGVO 10

B. DSGVO und Beschäftigtendatenschutz: „Öffnungsklausel" in Art. 88 DSGVO 13

C. Die Rolle des Betriebsrats im Beschäftigtendatenschutz 17

I. Betriebsvereinbarung als zentrales Datenschutz-Regelungsinstrument 17
II. Kollision zwischen Datenschutz und Mitbestimmungsrechten? 19
III. Einbeziehung des Betriebsrats in die Datenschutzfolgen-abschätzung? 21

D. Datenschutzrechtliche Anforderungen an Betriebs-vereinbarungen zum Beschäftigtendatenschutz 25

I. Anforderungen aus Art. 88 DSGVO 25
1. Aus Art. 88 Abs. 1 DSGVO 25
2. Aus Art. 88 Abs. 2 DSGVO 26
II. Datenschutzgrundsätze nach der DSGVO 29
1. Berücksichtigung von Art. 6 DSGVO 29
2. Berücksichtigung von Art. 9 DSGVO 30
3. Berücksichtigung von Art. 5 DSGVO 30
4. Transparenzregeln 33
III. Betroffenenrechte 36

E. Zu regelnde Datenschutzinhalte in Betriebsvereinbarungen 38

I. Notwendige Datenschutzinhalte in Einzelbetriebsvereinbarungen 38
II. Datenschutzregelungen in Rahmenbetriebsvereinbarungen 40
III. Übersicht über Datenverarbeitungs-Regelungsgegenstände 42
IV. Technische Maßnahmen 44
V. Konzerndatenverarbeitung 47

F. Umgang mit alten Betriebsvereinbarungen ... 49

I. Grundsätzliche Überlegungen ... 49
II. Einzelprüfung ... 51
III. FAQ ... 52
IV. Rahmenbetriebsvereinbarungen ... 53
V. Steckbriefe ... 54

G. Eigene Datenverarbeitung des Betriebsrats ... 56

I. Betriebsrat als verarbeitende Stelle ... 56
II. Zulässigkeit von Datenverarbeitung durch den Betriebsrat ... 60
III. Verzeichnis der Verarbeitungstätigkeiten, Art. 30 DSGVO ... 60
IV. Überwachung der Datenverarbeitung des Betriebsrats ... 62
1. Kontrolle durch den Arbeitgeber ... 63
2. Betrieblicher Datenschutzbeauftragter ... 64
3. Eigener DSB des Betriebsrats ... 66
4. Staatliche Aufsichtsbehörden ... 67

H. Aufsichtsbehörden und Betriebsrat ... 68

I. Überwachung des Betriebsrats ... 68
II. Einschaltung der Aufsichtsbehörden durch den Betriebsrat ... 70
1. Beratung durch die Aufsichtsbehörde ... 70
2. Initiativrecht des Betriebsrats? ... 71

J. Ergebnisse ... 73

Literaturverzeichnis ... 75

Einleitung

Durch die EU-Datenschutz-Grundverordnung (DSGVO),[1] seit dem 25.5.2016 in Kraft und nach einer Übergangsphase von zwei Jahren seit dem 25.5.2018 für staatliche Stellen und Unternehmen anwendbar, stellen sich auch im Beschäftigtendatenschutz[2] zahlreiche Fragen neu. Zum einen geht es um Änderungen im materiellen Datenschutzrecht, zum anderen um Veränderungen im Verfahren und schließlich um strengere Sanktionen bei Datenschutzverstößen.[3] Vor allem aber interessiert Beschäftigte und ihre Vertretungsorgane der zukünftige Umgang mit dem Regelungsinstrument Betriebsvereinbarung. Dass der Betriebsrat als wichtiger Akteur bei der Schaffung von Regelungen zum Beschäftigtendatenschutz erhalten bleibt, war im Entstehungsprozess der DSGVO nicht selbstverständlich, ist aber schließlich politisch durchgesetzt worden. Dennoch bleibt nicht alles beim gewohnten Alten. Dieser Umstand ist Ausgangspunkt der folgenden Überlegungen. Im Mittelpunkt steht die Frage, wie die neuen Anforderungen an Betriebsvereinbarungen zum Beschäftigtendatenschutz aussehen, welche Datenschutzthemen in ihnen geregelt werden sollten und wie mit den zahlreichen alten, noch geltenden Betriebsvereinbarungen im Lichte der Datenschutz-Grundverordnung umzugehen ist. Darüber hinaus stellt sich die Frage, welche Datenschutzanforderungen an den Betriebsrat selbst zu stellen sind. Schließlich geht es um die Beziehung zwischen Betriebsrat und Aufsichtsbehörden. Gestreift wird das Verhältnis zwischen Datenschutz und Arbeitsrecht – Gegenstand für eine eigene Untersuchung – in Gestalt der Frage, ob und inwieweit die europäischen Datenschutzanforderungen die aus nationalem Arbeitsrecht erwachsenden Mitbestimmungsbefugnisse des Betriebsrats ggfs. beeinträchtigen.

---

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

2 Zur Begrifflichkeit „Arbeitnehmer" und „Beschäftigter" vgl. *Reinecke*, Die Begriffe Arbeitnehmer und Beschäftigter, NJW 2018, 2081.

3 Zu diesen Punkten schon *Körner*, Wirksamer Beschäftigtendatenschutz im Lichte der Europäischen Datenschutz-Grundverordnung (DSGVO), HSI-Schriftenreihe Band 18, Frankfurt 2017, S. 15ff.

A. Hintergrund: Reform des Datenschutzes durch die DSGVO

Nach Jahrzehnten ausschließlich nationaler Datenschutzgesetzgebung in Deutschland – dort besonders umfassend – und einigen wenigen weiteren EU-Mitgliedstaaten und einem ersten europäischen Regelungsversuch 1995 in Gestalt der Datenschutzrichtlinie,[4] deren einzelstaatliche Umsetzung in vielen EU-Mitgliedstaaten im Sande verlief, hat die EU nun mit der DSGVO das gemäß Art. 288 AEUV allgemein, unmittelbar und zwingend geltende Rechtsinstrument der Verordnung gewählt. In 99 Artikeln wird das gesamte Datenschutzrecht geregelt. Problem und Chance dabei ist, dass die Verordnung im Wesentlichen mit Generalklauseln und unbestimmten Rechtsbegriffen arbeitet, gleichzeitig aber die angedrohten Sanktionen bei Datenschutzverstößen mit einem Bußgeldrahmen bis zu 20 Mio. Euro oder vier Prozent des weltweiten Umsatzes erheblich erhöht. Letzte Instanz für eine verbindliche Interpretation der geltenden Datenschutzstandards sind nicht mehr die nationalen Gerichte, sondern ist der Europäische Gerichtshof (EuGH).

Probleme ergeben sich dabei daraus, dass wegen der offenen Formulierungen in den Artikeln der DSGVO auf Jahre hinaus rechtsunsicher bleiben wird, wie die Bestimmungen der Verordnung zu interpretieren sind. Die nationalen Gerichte in den EU-Mitgliedstaaten werden das jeweils vor dem Hintergrund ihrer eigenen Rechtstraditionen und Interpretationsgewohnheiten tun. Daher kann man sich unschwer vorstellen, dass die nationale Rechtsprechung zu vielen unbestimmten Rechtsbegriffen der Verordnung nicht einheitlich sein wird. Nur in Einzelfällen wird der EuGH angerufen werden und dann i.d.R. nach Jahren die jeweilige Fragestellung klären. Da auch das europäische Aufsichtsverfahren äußerst komplex ist,[5] wird man auch hier nur langsam mit verbindlichen Klärungen zu punktuellen Streitfragen rechnen können. Allerdings wird es längst nicht immer um grenzüberschreitende Fragestellungen gehen und werden da-

---

4 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Abl. Nr. L 281 S. 31.

5 *Körner*, a.a.O., S. 31ff.

her zunächst primär die nationalen Aufsichtsbehörden zuständig sein. Deren Einschätzungen allerdings können letztlich auch vom EuGH kassiert werden.

Besonders im deutschen Kontext liegen in den zahlreichen vagen Formulierungen der Verordnung aber auch Chancen, bisher bewährte Datenschutzauslegungen fortzuschreiben. Das hängt damit zusammen, dass anders als in anderen Rechtsmaterien, wie etwa dem Gleichstellungsrecht, die Rechtskonzepte beim Datenschutz nicht auf europäischer Ebene geboren wurden, ja nicht einmal ein Kondensat aus einer Zusammenschau der Datenschutzregeln aller Mitgliedstaaten sind, sondern – in Ermangelung von nationalen Datenschutzregelungen in den meisten Mitgliedstaaten – schon die Datenschutzrichtlinie von 1995 war im Großen und Ganzen eine Anlehnung an das BDSG mit einigen Verbesserungen. Bei der DSGVO ist es, vor allem im materiellen Datenschutzrecht, ähnlich. Das fiel nur nicht mehr so auf wie in den 1990er Jahren, da für die DSGVO formal die europäische Datenschutzrichtlinie Grundlage war. Die DSGVO sollte zwar an die rasante Informationstechnikentwicklung angepasst werden, was aber im materiellen Datenschutzrecht nur punktuell gelungen ist. Im Wesentlichen sind die seit den 1970er Jahren bekannten Datenschutzkonzepte beibehalten worden, wie Verbot mit Erlaubnisvorbehalt, Zweckbindung, Datensparsamkeit etc. Der Rückgriff auf die alten Konzepte lässt zwar Zweifel aufkommen, ob damit neue Phänomene wie etwa Big Data-Anwendungen datenschutzrechtlich greifbar werden, haben aber den Vorteil, dass jedenfalls in Deutschland, wo seit Jahrzehnten Rechtsübung mit diesen Konzepten besteht, in der Auslegung des materiellen Datenschutzrechts über weite Strecken auf die bisherige Rechtsprechung zurückgegriffen werden kann. Zwar dürfen deren Grundsätze nicht völlig unkritisch übernommen werden, aber soweit die Begrifflichkeiten der DSGVO mit denen des bisherigen deutschen Datenschutzrechts übereinstimmen, nicht die DSGVO selbst eine andere Auslegung nahelegt oder sich der EuGH schon geäußert hat – was in der Datenschutzmaterie in den letzten Jahren zwar vermehrt vorgekommen, aber immer noch die Ausnahme ist – spricht nichts dagegen, die bisherige Datenschutz-Rechtsprechung der deutschen Gerichte auch für die Auslegung der DSGVO heranzuziehen.

Das gilt auch und gerade für den Beschäftigtendatenschutz, da hier die DSGVO ohnehin nicht spezialgesetzlich regelt, sondern die Materie den Mitgliedstaaten überlässt. Zwar muss deren Ausfüllung der Verordnungsöffnung wiederum den zentralen Grundsätzen der DSGVO entsprechen – das gilt auch für Betriebsvereinbarungen –, aber da die Verordnung selbst die Spezialfragen der

Verarbeitung von Beschäftigtendaten nicht regelt, die deutsche Ausfüllung der Öffnung in § 26 BDSG dagegen auch auf § 32 BDSG a.F. zurückgreift[6] – wenn § 26 BDSG auch umfassender ist –, bleibt auch die bisherige Rechtsprechung dazu weiter relevant.

6 BT-Drs. 18/11325, S. 99.

B. DSGVO und Beschäftigtendatenschutz: „Öffnungsklausel“ in Art. 88 DSGVO

Obwohl die EU für ihre neue Datenschutzgesetzgebung aus Gründen der Effizienz und Rechtssicherheit das Instrument der unmittelbar geltenden Verordnung gewählt hat, enthält die DSGVO zahlreiche Öffnungen für nationale Regelungen, so auch für den Beschäftigtendatenschutz. Hier nimmt der europäische Gesetzgeber eine besondere Verarbeitungssituation an, regelt Beschäftigtendatenschutz aber nicht selbst, sondern erlaubt in Art. 88 DSGVO in Verbindung mit Erwägungsgrund 155 „spezifischere“ nationale Regelungen zum Beschäftigtendatenschutz und legt in Abs. 2 Mindestanforderungen für diese nationalen Regelungen fest.[7] Das allein deutet schon darauf hin, dass es sich bei den nationalen Regelungen, seien es gesetzliche oder kollektivvertragliche, um eigenständige Erlaubnistatbestände handelt.[8]

Wie streng die Bindung des deutschen Gesetzgebers in der Bereichsausnahme an die unionsrechtlichen Vorgaben ist, lässt sich mit Blick auf den Verordnungstext kaum festlegen. Nach der Rechtsprechung des BVerfG und des EuGH besteht nur eine Bindung im unionsrechtlich determinierten Teil,[9] aber was heißt das bei einer Bereichsausnahme wie Art. 88 DSGVO? Wenn eine Bereichsausnahme ohnehin nur das regeln dürfte, was ohnehin schon in der Verordnung steht, wäre sie überflüssig. Daher ist eher davon auszugehen, dass die Bereichsausnahme nicht unionsrechtlich (nach oben) determiniert ist, wenn der nationale Gesetzgeber von dem ihm eingeräumten Spielraum Gebrauch gemacht hat und insoweit keine Vollharmonisierung im Bereich des Beschäftigtendatenschutzes eintritt.[10] Dieser Spielraum enthebt den nationalen Gesetzgeber aber nicht der Einhaltung der Minimumgrundsätze der europäischen Verordnung auch in den geöffneten Bereichen. Das stellt Art. 88 Abs. 2 DSGVO klar, in dem ausgesprochen wird, unter welches Niveau eine nationale Regelung im Beschäftigtendatenschutz keinesfalls sinken darf, was materiell dem

---

7 Dazu unten D.I.2.

8 Dazu noch unten C.I.

9 Vgl. *Körner*, a.a.O., S. 17ff.

10 So auch *Tiedemann*, ArbRB 2016, 334; a.A. *Franzen*, EuZA 2017, 313, 343ff.

Niveau von § 75 Abs. 2 BetrVG entsprechen dürfte. Eine klare „Obergrenze“ für nationale Regelungen wäre natürlich auch möglich gewesen und war zunächst in den ersten Entwürfen der DSGVO auch enthalten. Im Entstehungsprozess der DSGVO hieß es zunächst, „spezifischere“ nationale Regelungen seien nur „im Rahmen der Verordnung“ erlaubt. Diese Formulierung ist ersatzlos gestrichen worden. Bei dieser Streichung hat sich der europäische Gesetzgeber etwas gedacht. Eine derart explizite Veränderung in der gesetzgeberischen Bewertung kann nicht einfach, wie aber in der deutschen Fachliteratur z.T. praktiziert,[11] übergangen werden, ohne die Absicht des Gesetzgebers zu konterkarieren. Daher kann für den Beschäftigungskontext national ein eigenes Datenschutzregime geschaffen werden. „Der Freiraum für nationale Regelungen ist also beträchtlich.“[12] Dafür spricht auch der Vergleich mit der Datenschutzrichtlinie von 1995, die keine entsprechende Öffnungsklausel für eigenständigen Beschäftigtendatenschutz enthielt. Der EuGH hatte ihr vollharmonisierende Wirkung zugesprochen,[13] was nationale Abweichungen zugunsten eines höheren Schutzniveaus erschwerte. Die Situation stellt sich bei der DSGVO gerade wegen der Öffnung für nationale Regelung anders dar.[14]

Die Vorgaben der Verordnung sind also als Mindestbedingungen für den Beschäftigtendatenschutz zu verstehen.[15] Nach oben darf strengerer Schutz der personenbezogenen Beschäftigtendaten festgelegt werden. Anderenfalls würde die Öffnung in Art. 88 DSGVO keinen Sinn ergeben, denn dann würden auch für den Beschäftigtendatenschutz nur die Vorgaben der DSGVO direkt gelten. Eine nationale Regelung, die ohnehin keine Verbesserung des Schutzes bewirken dürfte, wäre also überflüssig.

---

11 *Pötters*, in: Gola/Pötters, DSGVO, 2018, Art. 88 Rn. 18 ff.; *Maschmann*, in: Kühling/Buchner, DSGVO, 2017, Art. 88 Rn. 30 ff.; *Franzen*, Datenschutz-Grundverordnung und Arbeitsrecht, EuZA 2017, 313, 343 ff.; *Wybitul*, Der neue Beschäftigtendatenschutz nach § 26 BDSG und Art. 88 DSGVO, NZA 2017, 413.

12 So *Taeger/Rose*, Zum Stand des deutschen und europäischen Beschäftigtendatenschutzes, BB 2016, 819, 830 noch zum damaligen Art. 82 DSGVO-E.

13 EuGH, Urt. v. 24.11.2011 – C-468/10, NZA 2011, 1409.

14 A.a.O.

15 So auch u.a. *Pauly*, in: Paal/Pauly, Datenschutzgrundverordnung, 2018, 2. Aufl., Art. 88 Rn. 4; *Riesenhuber*, in: BeckOK Datenschutzrecht, 24. Aufl. 1.5.2018, DSGVO, Art. 88 Rn. 66ff.; *Selk*, in: Ehmann/Selmayr, EU-DSGVO, 2017, Art. 88 Rn. 56ff. mit Argumenten für die Zulässigkeit strengerer Vorschriften, aber keiner endgültigen Festlegung, sondern Verweis auf zukünftige EuGH-Rechtsprechung; *Roßnagel*, DuD 2017, 290, 292.

Allerdings gehört zu den DSGVO-Grundsätzen, die auch in den geöffneten Bereichen einzuhalten sind, auch Art. 1 Abs. 3 DSGVO, wonach der freie Verkehr personenbezogener Daten in der Union aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden darf. Hierin liegt eine etwas andere Wertung als noch im deutschen Datenschutzrecht bis 2018, dem es ausschließlich um den Persönlichkeitsschutz ging. Entsprechend hatte § 1 Abs. 1 BDSG a.F. als Zweck des Gesetzes den Schutz des Persönlichkeitsrechts des Einzelnen genannt. Das neue BDSG definiert überhaupt keinen Zweck mehr, weil es kein umfassendes Datenschutzrecht mehr enthält, sondern nur die Öffnungen der DSGVO ausfüllt. Nach europäischem Datenschutzrecht ist also immer auch zu berücksichtigen, dass der freie Datenverkehr nicht zu stark eingeschränkt wird. Das war zwar auch schon in Art. 1 Abs. 1 und 2 der Datenschutzrichtlinie von 1995 so. Deren mangelnde Effizienz hat aber gerade zum Erlass einer unmittelbar verbindlichen Verordnung geführt, weshalb aus der Formulierung in der Datenschutzrichtlinie von 1995 für den zukünftigen Umgang mit dem Doppelziel der DSGVO Persönlichkeitsschutz und freier Datenverkehr nicht allzu viel abgeleitet werden kann.

Für die Praxis des Beschäftigtendatenschutzes spielt das aber nur eine untergeordnete Rolle. Zum einen ist Art. 1 Abs. 3 DSGVO im Lichte von Art. 7 und 8 GR-Charta auszulegen, in denen der Schutz personenbezogener Daten im Vordergrund steht. Zum anderen geht es beim freien Verkehr personenbezogener Daten um binnenmarktrelevante Datenverarbeitungsvorgänge, d.h. es muss ein grenzüberschreitendes Element vorliegen. Solange das nicht der Fall ist, besteht keine Gefährdungslage für den freien Datenverkehr. Schließlich hat auch der klassische Beschäftigtendatenschutz, der innerhalb eines Unternehmens oder Konzerns stattfindet, i.d.R. keine Marktrelevanz. Daher spielt der Topos „freier Datenverkehr“ in Art. 1 Abs. 3 DSGVO üblicherweise für den Beschäftigtendatenschutz keine Rolle und kann etwa Erhebungs- und Verarbeitungsverbote von Beschäftigtendaten für bestimmte Verarbeitungszusammenhänge nicht ausschließen.

Auch wenn es sich beim Umgang mit Beschäftigtendaten um grenzüberschreitende Vorgänge handeln würde, wären Verbote von Leistungs- und Verhaltenskontrolle nicht ausgeschlossen, da dadurch zum einen ja nicht der Datenverkehr als solcher eingeschränkt würde, sondern nur die Verwendung der Daten für bestimmte Zwecke. Zum anderen dürfte sich der Arbeitgeber in einer Betriebsvereinbarung natürlich selbst beschränken, auch wenn es um grenzüberschreitende Vorgänge ginge.

Möglicherweise entpuppt sich die Diskussion über „Obergrenzen“ bei Art. 88 DSGVO auch als Glasperlenspiel, da die Grenzen der Verordnung wegen ihrer Generalklauseln und unbestimmten Rechtsbegriffe gar nicht eindeutig und verbindlich bestimmt werden können, sondern erst in der Zukunft durch die Rechtsprechung. Daher ist den Betriebsparteien zu raten, neue Betriebsvereinbarungen nach den formalen und materiellen Grundsätzen der DSGVO abzuschließen[16] und alte daran kritisch zu überprüfen.[17] An den Themen, die bisher schon Gegenstand von datenschutzrechtlichen Betriebsvereinbarungen waren, muss sich ohnehin nichts ändern. Eher werden neue Verarbeitungsformen dazu kommen, bei denen die DSGVO kaum Hilfestellung leistet, wie etwa bei Big Data-Anwendungen.[18] Dann wird es bei der Auslegung, was „spezifischere“ Vorschriften meinen, nicht nur darum gehen, ob stärkerer Schutz möglich ist, sondern vor allem auch, angesichts der alten Datenschutzkonzepte der DSGVO, darum, inwieweit andere, neue Schutzformen national erlaubt sind.

16 Dazu unten E.
17 Dazu unten F.
18 Dazu unten E.III.

C. Die Rolle des Betriebsrats im Beschäftigtendatenschutz

I. Betriebsvereinbarung als zentrales Datenschutz-Regelungsinstrument

Dass die Betriebsvereinbarung ein eigenständiges Regelungsinstrument i.S.v. § 4 Abs. 1 BDSG a.F. („andere Rechtsvorschrift") für Beschäftigtendatenschutz sein kann,[19] war zunächst umstritten, da das BetrVG keine eigenständige Mitbestimmungsbefugnis für Datenschutz enthält. Nach §§ 75 und 80 BetrVG hat der Betriebsrat nur allgemein die Aufgabe, die Einhaltung von Datenschutzvorschriften zu überwachen.

Aus datenschutzrechtlicher Sicht wurde schließlich angenommen, dass der Betriebsrat Beschäftigtendatenschutz eigenständig regeln kann, sofern das gesetzliche Datenschutzniveau eingehalten wird.[20] Das BAG hatte allerdings in den 1980er Jahren auch eine Abweichung zu Lasten des Datenschutzniveaus der Beschäftigten erlaubt,[21] hat das aber in den letzten Jahren relativiert, jedenfalls die Berücksichtigung des allgemeinen Persönlichkeitsrechts der Beschäftigten i.S.v. § 75 Abs. 2 BetrVG in datenschutzrelevanten Betriebsvereinbarungen eingefordert[22] und damit die Abweichungen zulasten der Beschäftigten erschwert.

Der europäische Gesetzgeber hat zu dieser Frage in Art. 88 DSGVO mehr Klarheit gebracht. Die Öffnungsnorm Art. 88 Abs. 1 DSGVO erlaubt neben beschäftigtendatenschutzrechtlichen Gesetzen durch die Mitgliedstaaten auch „spezifischere" Vorschriften durch Kollektivvereinbarungen. Zunächst war in den DSGVO-Vorschlägen nationaler Beschäftigtendatenschutz nur „durch Gesetz" vorgesehen, was schließlich, nicht zuletzt auf deutsche Initiative, durch Kollektivvereinbarungen ergänzt wurde. Diese nachträgliche Einfügung erklärt auch den nicht ganz geglückten Wortlaut der Norm. Allerdings stellt Erwägungsgrund 155 klar, dass es sich dabei neben Tarifverträgen ausdrücklich auch um

---

19 Vom BAG anerkannt seit: BAG, Beschl. v. 27.5.1986 – 1 ABR 48/84, BAGE 52, 88.

20 *Seifert*, in: Simitis, BDSG Kommentar, 2014, 8. Aufl., § 32 Rn. 167 m.w.N.

21 BAG, Beschl. v. 27.5.1986 – 1 ABR 48/84, NZA 1986, 643.

22 BAG, Beschl. v. 9.7.2013 – 1 ABR 2/13, NZA 2013, 1433; DKKW, § 87 Rn. 195.

Betriebsvereinbarungen handelt, die als Datenschutzregelungsinstrument bislang nur in Deutschland eine Rolle spielen, wohingegen sich das von Tarifverträgen für den Bereich Beschäftigtendatenschutz nicht sagen lässt.[23]

Art. 88 Abs. 1 DSGVO hat, vergleichbar mit § 4 Abs. 1 BDSG a.F., die Funktion, Betriebsvereinbarungen als eigenständige Erlaubnisnormen für den Beschäftigtendatenschutz zu etablieren. Wenn letztlich doch nur die allgemeine Erlaubnisnorm in Art. 6 DSGVO zum Tragen kommen müsste, hätte die Ermächtigung des europäischen Gesetzgebers in Art. 88 Abs. 1 DSGVO gerade auch für Kollektivvereinbarungen keinen Sinn. Man hätte es dann auch bei der DSGVO ohne Öffnung für nationale Regelungen belassen können. Darüber hinaus legen auch die besonderen Anforderungen in Art. 88 Abs. 2 DSGVO an die „spezifischeren" Regelungen nahe, dass es sich dabei um eigenständige Regelungen handelt, bei denen sichergestellt werden soll, dass bestimmte Mindeststandards eingehalten werden.[24] Schließlich belegt auch die Genese der Verordnung, dass eigenständige Regelungen gewollt waren. Zunächst sollte die Öffnung für Beschäftigtendatenschutz nur „in den Grenzen der Verordnung", in einer späteren Version „im Rahmen der Verordnung" erlaubt sein. Diese Einschränkungen sind in der nun geltenden Fassung ganz entfallen, was die Eigenständigkeit der nationalen Regelungen unterstreicht.

Auch der deutsche Gesetzgeber hat Art. 88 DSGVO offenbar so verstanden, da er in § 26 Abs. 4 BDSG n.F. regelt, dass die Verarbeitung personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses auf der Grundlage von Kollektivvereinbarungen zulässig ist.

Damit wird nur der Umstand aufgegriffen und in einen rechtlichen Rahmen gegossen, dass die Betriebsvereinbarung längst zu einem zentralen Instrument des Beschäftigtendatenschutzes geworden ist, nicht zuletzt auch wegen der Zurückhaltung des Gesetzgebers, der mit § 32 BDSG a.F. nur eine symbolische Norm zum Beschäftigtendatenschutz erlassen hatte und nun im Rahmen des Art. 88 DSGVO mit § 26 BDSG n.F. nur unwesentlich mehr selbst regelt.

---

23 *Kort*, DB 2016, 711, 714.

24 So auch *Klösel/Mahnhold*, NZA 2017, 1428, 1429 m.w.N. zu den Gegenstimmen.

II. Kollision zwischen Datenschutz und Mitbestimmungsrechten?

§ 26 Abs. 6 BDSG lässt die Beteiligungsrechte der Interessenvertretungen der Beschäftigten unberührt. Der Betriebsrat kann auf der Basis mehrere Anknüpfungspunkte im BetrVG Betriebsvereinbarungen zum Beschäftigtendatenschutz durchsetzen. So steht ihm für die Einführung technischer Einrichtungen, die auch das Verhalten von Beschäftigten überwachen können, § 87 Abs. 1 Nr. 6 BetrVG zu Gebote. § 87 Abs. 1 Nr. 1 BetrVG gewährt Mitbestimmung bei Verhaltensregeln zu Datenschutzfragen und §§ 94 und 95 BetrVG ermöglichen Mitbestimmung bei der Aufstellung von Personalauswahl- und Beurteilungsgrundsätzen. Darüber hinaus können gemäß § 88 BetrVG freiwillige (Rahmen-) Betriebsvereinbarungen zur Verarbeitung von Beschäftigtendaten abgeschlossen werden.[25]

Da durch die betriebliche Mitwirkung bei der Regelung von Beschäftigtendatenschutz durch den Abschluss von entsprechenden Betriebsvereinbarungen die europäischen Datenschutzanforderungen auf nationale arbeitsrechtliche Befugnisse des Betriebsrats aus dem BetrVG treffen, stellt sich die Frage, inwieweit die Anforderungen des europäischen Datenschutzrechts ggfs. die deutschen betrieblichen Mitwirkungsbefugnisse beeinflussen oder gar einschränken können.

Zunächst ist zu beachten, dass der Betriebsrat nur für Beschäftigtendatenschutz zuständig ist, also eine eventuelle Kollision nur insoweit auftreten könnte. Da der Beschäftigtendatenschutz aber gerade für nationale Regelungen geöffnet ist und der deutsche Gesetzgeber mit § 26 BDSG n.F. dergestalt davon auch Gebrauch gemacht hat, dass sich materiell-rechtlich im Vergleich zu § 32 BDSG a.F. nicht sehr viel ändert, werden Betriebsvereinbarungen inhaltlich nur durch die allgemeinen Anforderungen in Art. 5, 6 u.a. und Art. 88 Abs. 2 DSGVO i.V.m. § 26 BDSG europarechtlich konturiert.[26] § 26 Abs. 1 BDSG n.F. stellt dabei, wie § 32 Abs. 3 BDSG a.F. klar, dass die Datenerhebung des Betriebsrats im Rahmen seiner betriebsverfassungsrechtlichen Aufgaben gerechtfertigt ist,[27] zumal Abs. 6 deutlich macht, dass es nicht zu einer Einschränkung von Beteiligungsrechten kommen darf, aber dabei die datenschutzrechtlichen Anforderungen der DSGVO eingehalten werden müssen. Bei genauer Betrachtung läuft das im

---

25 Zu Rahmenbetriebsvereinbarungen s.u. F. IV.

26 Details zu diesen Anforderungen unter D.

27 So auch Rundbrief Arbeitnehmeranwälte, 39/2018, S. 17 (unter www.arbeitnehmeranwaelte.de).

Wesentlichen darauf hinaus, dass der Betriebsrat dadurch inhaltlich kaum mehr eingeschränkt wird als durch die Anforderungen, die das BetrVG in § 75 Abs. 2 BetrVG selbst schon enthält, auch wenn einzuräumen ist, dass diese Anforderungen aus dem BetrVG – ebenso vage formuliert wie die gleichartigen Voraussetzungen in der DSGVO – bislang nicht in jeder Betriebsvereinbarung mit der nötigen Tiefe abgebildet worden sein mögen. In solchen Fällen hätte der Betriebsrat auch bisher schon nach dem BetrVG genauer sein müssen. Wenn die DSGVO nun insbesondere in Art. 88 Abs. 2 explizitere Forderungen stellt, beeinträchtigt das nicht Mitbestimmungsrechte des Betriebsrats als solche.

Die DSGVO macht zum Verhältnis zwischen betrieblicher Mitbestimmung und (Beschäftigten-)Datenschutz keine Aussagen. Das ist nicht weiter erstaunlich, denn das Regelungsinstrument der Betriebsvereinbarung ist der europäischen Verordnung zum Datenschutz an sich wesensfremd und erst auf Initiative Deutschlands in einem bereits fortgeschrittenen Gesetzgebungsprozess in der Öffnungsklausel Art. 88 DSGVO i.V.m. Erwägungsgrund 155 ermöglicht worden. Da es bei Art. 88 DSGVO um eine Öffnung für nationale Regelungen zum Beschäftigtendatenschutz geht und datenschutzrechtliche Kollektivverträge in Gestalt der Betriebsvereinbarung in der EU eine deutsche Besonderheit sind, hat der europäische Gesetzgeber ein mögliches Kollisionsproblem zwischen betrieblicher Mitbestimmung und Datenschutzanforderungen gar nicht erst in den Blick genommen.

Das materielle europäische Datenschutzrecht hat also nicht das Ziel, die Mitbestimmungsbefugnisse des Betriebsrats einzuschränken oder gar auszuhebeln, aber selbstverständlich muss der Betriebsrat, sofern er selbst personenbezogene Beschäftigtendaten verarbeitet, seinerseits die DSGVO einhalten,[28] die allerdings gemäß § 26 Abs. 6 BDSG von den Mitgliedstaaten ausgestaltet wird.

Wenn es um die Aufsicht und Kontrolle der Rechtmäßigkeit der datenschutzrechtlichen Inhalte von Betriebsvereinbarungen und deren Durchführung geht, könnte es eher zu Friktionen der Mitbestimmung mit der DSGVO kommen, wenn etwa der Arbeitgeber als die verarbeitende Stelle oder der betriebliche Datenschutzbeauftragte Kontrollbefugnisse hätte. Das hat allerdings das BAG schon 1997 abgelehnt.[29] Ob auch der EuGH das so sehen würde, ist nicht eindeutig, insbesondere wenn der Betriebsrat nicht als eigene verarbeitende Stelle angesehen wird.[30] Für den rechtlich korrekten Inhalt von Datenschutz-Betriebs-

---

28 Dazu unten G.

29 BAG, Beschl. v. 11.11.1997 – 1 ABR 21/97, NZA 1998, 385.

30 Dazu noch näher unten G.I.

vereinbarungen ist dann der Arbeitgeber als verarbeitende Stelle verantwortlich. Das BAG hat es ausreichen lassen, dass die externen staatlichen Aufsichtsbehörden die Datenverarbeitung beim Betriebsrat kontrollieren – was allerdings in der Praxis allein aus Kapazitätsgründen bei den Datenschutzbehörden bislang selten vorkommt.[31] Darüber hinaus hat der Arbeitgeber die Rechte aus § 23 Abs. 1 BetrVG.

III. Einbeziehung des Betriebsrats in die Datenschutzfolgenabschätzung?

Mit der Datenschutzfolgenabschätzung in Art. 35 DSGVO enthält die Verordnung eine § 4d BDSG a.F. entsprechende Verpflichtung. Bei Verarbeitungen, die z.B. aufgrund neuer technischer Möglichkeiten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen – Fälle sind exemplarisch in Art. 35 Abs. 3 DSGVO genannt –, muss vorab eine Folgenabschätzung durchgeführt werden, indem u.a. eine systematische Beschreibung der Verarbeitungsvorgänge und Zwecke und eine Risikoabschätzung i.S.v. Art. 35 Abs. 7 DSGVO vorgenommen werden muss. In der Praxis dürfte das jedenfalls bei permanenter Leistungskontrolle der Beschäftigten und bei der Verarbeitung sensibler Daten i.S.v. Art. 9 DSGVO notwendig sein.

Gemäß Art. 35 Abs. 2 DSGVO holt der Arbeitgeber bei der Durchführung einer Datenschutzfolgenabschätzung den Rat des betrieblichen Datenschutzbeauftragten ein, sofern ein solcher benannt wurde. Dagegen ist der Standpunkt der betroffenen Personen oder ihrer Vertreter nach Art. 35 Abs. 9 DSGVO nur „gegebenenfalls" zu erfragen. Daher spielt auf den ersten Blick offenbar hier der betriebliche Datenschutzbeauftragte eine wichtigere Rolle als der Betriebsrat, da schon gar nicht deutlich wird, ob er als Vertreter überhaupt mit umfasst ist. Allerdings gibt es bei Abs. 9 des Art. 35 DSGVO viel Spielraum: es ist vom Wortlaut her weder klar, was „gegebenenfalls" noch „Standpunkt einholen" genau bedeuten soll noch wie die Lage ist, wenn der Betriebsrat ohnehin nach § 87 Abs. 1 Nr. 6 BetrVG beteiligt ist oder was die Rechtsfolge ist, wenn Art. 35 Abs. 9 DSGVO nicht beachtet wird.

---

31 Vgl. dazu auch zur Überforderung der nationalen Datenschutzbehörden nach Inkrafttreten der DSGVO in FAZ 25.6.2018: „Behörden verzweifeln am neuen Datenschutz". Dazu auch noch unten H.I.

Jedenfalls ist der Vertreterbegriff in Art. 35 Abs. 9 DSGVO weiter als in der Definitionsnorm Art. 4 Abs. 17 DSGVO,[32] da es in Art. 35 Abs. 9 DSGVO um die Vertreter der Betroffenen geht. Z.T. bleibt in der Kommentarliteratur offen, ob neben Verbraucherverbänden u.Ä. auch Betriebsräte unter den Vertreterbegriff des Art. 35 Abs. 9 DSGVO fallen.[33]

„Standpunkt einholen" ist so zu verstehen, dass die Betroffenen bzw. ihre Vertreter sich zur beabsichtigten Verarbeitung äußern können sollen und zwar einerseits dazu, ob eine Folgenabschätzung durchzuführen ist, wobei es dabei um die Bewertung des Risikos nach Art. 35 Abs. 1 DSGVO geht und andererseits dazu, wie die Folgenabschätzung gemäß Art. 35 Abs. 7 DSGVO zu erfolgen hat.[34] Aus Abs. 9 des Art. 35 DSGVO wird, um einen Standpunkt überhaupt begründen zu können, auch eine Informationspflicht über die beabsichtigte Art der Folgenabschätzung abgeleitet.[35]

Allerdings ist der Standpunkt der Betroffenen nur „gegebenenfalls" einzuholen. Mit Blick auf den englischen Text („where appropriate …") sollen die betroffenen Personen oder ihre Vertreter nur zu konsultieren sein, wenn es angemessen, d.h. nicht mit hohem Aufwand verbunden ist.[36] Bei unbestimmt vielen Betroffenen, wie bei Online-Portalen, wäre die Angemessenheit zu verneinen, bei einem Betriebsrat, der eine leicht bestimmbare Anzahl von Beschäftigten vertritt, ist die Konsultation angemessen.

Wegen der Vorgaben in Art. 35 Abs. 3 DSGVO dürfte im Beschäftigungsverhältnis eine Datenschutzfolgenabschätzung jedenfalls immer dann erforderlich sein, wenn Systeme eingesetzt werden, die Verhalten oder Leistung von Beschäftigten überwachen können, wie Videokontrolle, Ortungs- und Chipkartensysteme oder Gesichts- und Spracherkennungssysteme. Da deren Einführung auch unter § 87 Abs. 1 Nr. 6 BetrVG fällt, ist der Betriebsrat aus mitbestimmungsrechtlichen Gründen zu beteiligen und wird eine Datenschutzfolgenabschätzung sogar verlangen können,[37] denn insoweit verfolgen das Mitbestim-

---

32 *Jandt*, in: Kühling/Buchner, DSGVO 2018, 2. Aufl., § 35 Rn. 55.

33 So bei *Jandt*, a.a.O., oder *Martini*, in: Paal/Pauly, Datenschutzgrundverordnung, 2017, Art. 35 Rn. 60ff.

34 *Martini*, in: Paal/Pauly, Datenschutzgrundverordnung, 2017, Art. 35 Rn. 60.

35 A.a.O.; *Jandt*, in: Kühling/Buchner, DSGVO, 2018, 2. Aufl., § 35 Rn. 57.

36 *Baumgartner*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2017, Art. 35 Rn. 47.

37 Im Ergebnis sehen das *Dzida/Grau*, DB 2018, 189, 194 auch so, wenn sie „Interdependenzen zwischen der Datenschutzfolgenabschätzung und Betriebsvereinbarungen" sehen und Arbeitgebern raten, schon zu Beginn von Verhandlungen über eine

mungsrecht in § 87 Abs. 1 Nr. 6 BetrVG und die Datenschutzfolgenabschätzung in Art. 35 DSGVO dasselbe Ziel: die Wahrung des Persönlichkeitsschutzes der Beschäftigten. Es wäre sinnwidrig, wenn der Betriebsrat bei bestehendem Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG wegen der Einführung von technischen Einrichtungen, die wegen Art. 35 Abs. 3 DSGVO gleichzeitig auch eine Pflicht zur Datenschutzfolgenabschätzung auslösen, an dieser nur „gegebenenfalls" zu beteiligen wäre. Jedenfalls ergänzt insbesondere Art. 35 Abs. 9 DSGVO die bestehenden Mitbestimmungsrechte.[38]

Der Widerspruch zwischen § 87 Abs. 1 Nr. 6 BetrVG und Art. 35 Abs. 9 DSGVO beruht nicht auf einer bewussten Wertung des (europäischen) Gesetzgebers, sondern ergibt sich daraus, dass Kollektivvereinbarungen und insbesondere (deutsche) Betriebsvereinbarungen als datenschutzrechtliche Erlaubnistatbestände erst in einem fortgeschrittenen Gesetzgebungsstadium in die DSGVO aufgenommen wurden und sich daraus eventuell ergebende Friktionen mit dem nationalen Betriebsverfassungsrecht nicht beachtet wurden.

Was genau mit dem eingeholten Standpunkt nach Abs. 9 des Art. 35 DSGVO zu geschehen hat, spricht die Norm nicht an. Damit der durch Abs. 9 bezweckte Selbstdatenschutz sein Ziel erreichen kann, ist davon auszugehen, dass der Verantwortliche sich mit den abgegebenen Standpunkten auseinandersetzen und dies dokumentieren muss – bei Befürwortung durch eine Klarstellung, bei Ablehnung durch eine Begründung.[39]

Im Übrigen werden die Aufsichtsbehörden in Zukunft dadurch mehr Rechtssicherheit schaffen können, dass sie gemäß Art. 35 Abs. 4 DSGVO eine Positivliste für Verarbeitungsvorgänge erstellen und veröffentlichen, für die immer eine Datenschutzfolgenabschätzung erforderlich ist. Aus der englischen Fassung („shall") ergibt sich eindeutiger als aus der deutschen Version, dass es sich dabei um eine Pflicht der Aufsichtsbehörde handelt. Das belegt auch Art. 57 Abs. 1 lit. k DSGVO, wo das Erstellen der Liste gemäß Art. 35 Abs. 4 DSGVO ausdrücklich als Aufgabe

---

Datenschutz-Betriebsvereinbarung dem Betriebsrat einen Entwurf der Datenschutzfolgenabschätzung vorzulegen.

38 *Wedde*, in: Däubler/Wedde/Weichert/Sommer, EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, Art. 35 Rn. 105. Gegen eine Erweiterung des Mitbestimmungsrechts aus § 87 Abs. 1 Nr. 6 BetrVG: *Baumgartner*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2017, Rn. 47 m.w.N. in Anm. 62.

39 *Jandt*, in: Kühling/Buchner, DSGVO, 2018, 2. Aufl., Art. 35 Rn. 58.

der Aufsichtsbehörde genannt ist.[40] Die Aufsichtsbehörden haben bereits begonnen, an einer als „Blacklist“ bezeichneten Liste zu arbeiten.[41]

40 *Jandt*, in: Kühling/Buchner, DSGVO, 2018, 2. Aufl., Art. 35 Rn. 13.

41 *Datenschutzkonferenz*, DSGVO-Kurzpapier Nr. 5 „Datenschutzfolgen-Abschätzung“ v. 24.7.2017, abrufbar unter: www.lfd.niedersachsen.de

D. Datenschutzrechtliche Anforderungen an Betriebsvereinbarungen zum Beschäftigtendatenschutz

I. Anforderungen aus Art. 88 DSGVO

Art. 88 DSGVO spielt eine zentrale Rolle bei der Frage der Geltung der Bestimmungen der DSGVO im Inland. Zwar können die Mitgliedstaaten den Beschäftigtendatenschutz selbst regeln. Es würde aber Sinn und Zweck der Verordnung widersprechen, wenn sie dabei die datenschutzrechtlichen Anforderungen der DSGVO nicht einhalten müssten.[42] Von der DSGVO und einem einheitlichen europäischen Datenschutz bliebe dann angesichts der zahlreichen Öffnungen für nationale Regelungen nicht viel übrig. Die Datenschutzanforderungen aber ergeben sich aus Art. 88 DSGVO.

Nationale Betriebsvereinbarungen zum Beschäftigtendatenschutz sind nur insoweit von Art. 88 DSGVO als Grundlage für die Datenverarbeitung ermächtigt als sie dessen Voraussetzungen einhalten. Die DSGVO benutzt nur noch den Begriff „Datenverarbeitung", der nach Art. 4 Nr. 2 DSGVO umfassend zu verstehen ist und u.a. Erhebung, Auswertung, Speicherung, Veränderung, Übermittlung abdeckt.

1. Aus Art. 88 Abs. 1 DSGVO

Art. 88 Abs. 1 DSGVO i.V.m. Erwägungsgrund 155 definiert die Betriebsvereinbarung als eigenständigen Erlaubnistatbestand für „spezifischere" Regelungen, definiert aber keine eigenen inhaltlichen Begrenzungen, sondern beschreibt nur klarstellend und exemplarisch („insbesondere") typische Verarbeitungszusammenhänge im Beschäftigungsverhältnis, wie Datenverarbeitung für den Zweck der Einstellung, Erfüllung des Arbeitsvertrages, Planung und Organisation der Arbeit, Gleichheit und Diversität am Arbeitsplatz, Gesundheit und Sicherheit am Arbeitsplatz oder Beendigung des Beschäftigungsverhältnisses. Auch wenn mit der Auflistung in Art. 88 Abs. 1 DSGVO die meisten Zwecke für Datenver-

42 So aber offenbar *Heuschmid*, SR 2019, 1ff.

arbeitung im Beschäftigungsverhältnis genannt sein dürften, können weitere legitime Zwecke hinzukommen, die dann auch in Betriebsvereinbarungen die Verarbeitung von Beschäftigtendaten rechtfertigen.

Funktion des ersten Absatzes von Art. 88 DSGVO ist es, deutlich zu machen, dass es um Regelungen gehen muss, die ausschließlich den Beschäftigungskontext charakterisieren.

Für den vorliegenden Untersuchungsgegenstand sind aus den in der datenschutzrechtlichen Literatur bereits umfassend kommentierten Aspekten des Art. 88 Abs. 1 DSGVO[43] nochmals zwei hervorzuheben: zum einen ist die nationale Regelungsbefugnis im Beschäftigtendatenschutz auch für Betriebsvereinbarungen geöffnet, zum anderen sind die nationalen Regelungsmöglichkeiten nach oben offen, d.h. das Recht auf informationelle Selbstbestimmung der Beschäftigten darf in Betriebsvereinbarungen strenger geschützt werden als in der DSGVO selbst.[44]

2. Aus Art. 88 Abs. 2 DSGVO

Die Anforderungen an die Datenschutzkonformität von kollektiven Regelungen zum Beschäftigtendatenschutz sind seit Inkrafttreten der DSGVO gestiegen. Schon bisher durfte die in Betriebsvereinbarungen geregelte Verarbeitung von Beschäftigtendaten nicht in Grundrechte von Beschäftigten eingreifen. Nun wird der Gestaltungsfreiraum von Arbeitgebern und Betriebsräten neben dem Schutzauftrag aus § 75 Abs. 2 BetrVG, nach dem das allgemeine Persönlichkeitsrecht der Beschäftigten zu wahren ist, zusätzlich durch Art. 88 Abs. 2 DSGVO geprägt,[45] worauf § 26 Abs. 4 S. 2 BDSG n.F. noch einmal ausdrücklich hinweist. Art. 88 Abs. 2 DSGVO erweitert den nötigen Regelungsumfang auf „angemessene und besondere Schutzmaßnahmen“ und enthält umfassende inhaltliche Vorgaben für den (Mindest-)Inhalt einer Betriebsvereinbarung und stellt damit letztlich sicher, dass auch in dem für nationale Regelungen geöffneten Bereich des Beschäftigtendatenschutzes das Mindestdatenschutzniveau der DSGVO nicht unterschritten wird.[46] Allgemeine Hinweise in Betriebsvereinbarungen auf die DSGVO reichen nicht; das wären keine „besonderen“ Maßnahmen. Vielmehr ist Leitlinie, dass Maßnahmen zur Wahrung der menschlichen Würde

---

43 So auch schon *Körner*, HSI-Schriftenreihe Nr. 18, S. 50ff.

44 Dazu schon oben B. und C.

45 So sehen das auch die Aufsichtsbehörden, vgl. etwa: Ratgeber ANDS, Landesdatenschutz BW, S. 9 (www.baden-wuerttemberg.datenschutz.de).

46 *Tiedemann*, ArbRB 2016, 334, 336.

sowie berechtigter Interessen und Grundrechte der betroffenen Personen getroffen werden müssen. Dabei geht es vor allem um das Recht auf informationelle Selbstbestimmung[47] und um das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme[48] mit dem Ziel, zum einen den Einzelnen trotz moderner Datenverarbeitung vor unbegrenzter Erhebung, Speicherung, Verwendung und Weitergabe seiner personenbezogenen Daten zu schützen und zum anderen die heimliche Infiltration eines informationstechnischen Systems durch Auslesen von Speichermedien u.Ä. einzuschränken.

Diese Schutzmaßnahmen müssen in der Betriebsvereinbarung selbst getroffen werden. Die reine Wiedergabe des Gesetzestextes wäre allerdings keine „besondere" Regelung. Es geht daher um Konkretisierungen des Auftrags aus Art. 88 Abs. 2 DSGVO in Bezug auf den konkreten Regelungsgegenstand. Hier besteht die Notwendigkeit einer eigenständigen Abwägung.[49] In den Betriebsvereinbarungen sind also angemessene und besondere Maßnahmen zur Wahrung der Grundrechtspositionen der Betroffenen vorzusehen. *„Das kann erhebliche Auswirkungen auf bestehende Betriebs- oder Dienstvereinbarungen haben, die in der Praxis oft nur die mitbestimmungsrechtliche Seite oder nur die datenschutzrechtliche Seite regeln, aber keine faktischen Vorgaben im Sinne von konkreten Maßnahmen vorsehen. Sollen diese als spezifische Vorschriften i.S.v. Art. 88 Abs. 1 gelten, müssten sie angepasst werden; ansonsten droht die ‚Nichtanwendung' aufgrund des Anwendungsvorrangs der DSGVO."*[50]

Bei neuen Betriebsvereinbarungen kann dieser allgemeinen Anforderung ohne Weiteres entsprochen werden. Bei alten Betriebsvereinbarungen ist davon auszugehen, dass, da sie auch schon bisher den inhaltlich vergleichbaren § 75 Abs. 2 BetrVG, aber auch Art. 7 und 8 GRC und das allgemeine Persönlichkeitsrecht des Beschäftigten aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (informationelle Selbstbestimmung) einhalten mussten, insoweit häufig kein Anpassungsbedarf bestehen dürfte oder nur dann, wenn die genannten Normen in der Betriebsvereinbarung nur vage berücksichtigt worden sind.

Bei den Fallgruppen in Art. 88 Abs. 2 DSGVO („insbesondere") sieht es z.T. anders aus: Bei der Transparenz der Verarbeitung (Art. 5 Abs. 1 lit. a, 12 DSG-

---

47 BVerfG v. 15.12.83 – 1 BvR 209/83, BVerfGE 65, 1.

48 BVerfG v. 27.2.2008 – 1 BvR 370/07, BVerfGE 120, 274.

49 In IGM, Handlungshilfe für Betriebsräte und Vertrauensleute Nr. 19: Datenschutzgrundverordnung, 4/2018, S. 30 heißt es etwas unscharf, dass Betriebsvereinbarungen die Garantien aus Art. 88 Abs. 2 DSGVO „enthalten" müssen.

50 *Selk*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2017, Art. 88 Rn. 122.

VO i.V.m. Erwägungsgrund 39) sind die Anforderungen der DSGVO höher als die bisherigen im BDSG. Hier ist zunächst zu unterscheiden zwischen der Transparenz der durch eine Betriebsvereinbarung erlaubten Datenverarbeitung und der formalen (transparenten) Ausgestaltung der Betriebsvereinbarung selbst, etwa im Hinblick auf eine klare, verständliche Sprache.[51] Diese Unterscheidung wird z.T. in der Literatur bestritten,[52] ergibt sich aber unmittelbar aus der DSGVO. Die fordert einerseits in Art. 88 Abs. 2 Maßnahmen im Hinblick auf die Transparenz der Verarbeitung, also der Verarbeitungsvorgänge und andererseits in den Erwägungsgründen 39 und 58, dass die Information über die Verarbeitung präzise, leicht zugänglich und verständlich abgefasst sein muss.

Es muss also erkennbar sein, welche Daten in welchem Umfang für wen erhoben werden. Vor allem über den Zweck der Verarbeitung muss informiert werden, wie auch über Auskunftsrechte der Beschäftigten und Informationspflichten des Verwenders. Wichtig ist auch die Angabe über Speicherfristen, die gemäß Erwägungsgrund 39 und 58 auf ein „unbedingt erforderliches Mindestmaß" zu beschränken sind. Auch wenn es bislang in der rechtswissenschaftlichen Literatur noch keine einheitliche Linie zum konkreten Umfang der Transparenzpflichten gibt, müssen neue Betriebsvereinbarungen möglichst umfassend formuliert und alte angepasst werden. Denkbar sind dafür Einzelanpassungen, Rahmenbetriebsvereinbarungen, Steckbriefe oder eine Ergänzung um „häufig gestellte Fragen"" (FAQ).[53]

Darüber hinaus verlangt Art. 88 Abs. 2 DSGVO Schutzmaßnahmen bei Datenübermittlungen im Konzern. Hier kommt es auf den Einzelfall an; viele Betriebsvereinbarungen enthalten bereits entsprechende Maßnahmen.[54]

Schließlich ist gemäß Art. 88 Abs. 2 DSGVO besondere Vorsicht geboten bei Überwachungssystemen am Arbeitsplatz. Da es in Betriebsvereinbarungen zum Beschäftigtendatenschutz i.d.R. gerade darum geht, den Persönlichkeitsschutz der Beschäftigten beim Einsatz von Überwachungssystemen am Arbeitsplatz zu gewährleisten, dürfte sich hier für deutsche Betriebsvereinbarungen kein großer Anpassungsbedarf ergeben, zumal weitgehend unbestritten ist, dass die DSGVO jedenfalls einen Mindeststandard darstellt, von dem nicht nach unten ab-

---

51 *Pauly*, in: Paal/Pauly, DSGVO, 2017, Art. 88 Rn. 11; a.A. *Klösel/Mahnhold*, NZA 2017, 1428, 1431.

52 Dazu *Riesenhuber*, in: BeckOK Datenschutzrecht, 24. Ed., 1.5.2018, DSGVO, Art. 88 Rn. 84ff.

53 Dazu s.u. F.II.–V.

54 Zur Datenübermittlung im Konzern noch unten E.V.

gewichen werden darf. Wenn also eine Betriebsvereinbarung den Einsatz von Überwachungssystemen am Arbeitsplatz erlaubt, der i.d.R. § 87 Abs. 1 Nr. 6 BetrVG entsprechen dürfte,[55] – insbesondere optische, mechanische, elektronische, z.B. Kameras, Stechuhren, Fahrtenschreiber, Ortungssysteme – muss sie besondere Regelungen zum Schutz der Beschäftigten enthalten.

Allerdings wird aus dem Begriff „angemessene" Maßnahmen in Art. 88 Abs. 2 DSGVO z.T. geschlossen, dass die Maßnahmen verhältnismäßig sein müssen und daher pauschale Kontrollverbote, etwa der Ausschluss von Verhaltens- und Leistungskontrolle in Betriebsvereinbarungen nicht mehr zulässig seien.[56] So grundsätzlich können Kontrollverbote nicht ausgeschlossen werden, da die DSGVO eine strengere nationale Regelung ermöglicht[57] und es bei deren Zulässigkeit auf die konkrete Konstellation ankommt. So sind Positivlisten zu erlaubten Zwecken denkbar, aus denen sich dann ergibt, was im Umkehrschluss nicht erlaubt ist.

II. Datenschutzgrundsätze nach der DSGVO

1. Berücksichtigung von Art. 6 DSGVO

Da auch nach der DSGVO das aus dem deutschen Datenschutzrecht bekannte Verbot mit Erlaubnisvorbehalt gilt (**Art. 6 DSGVO**) und auch weiterhin Betriebsvereinbarungen Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten sein können (§ 26 Abs. 4 BDSG n.F.), stellt sich die Frage, ob in jeder entsprechenden Betriebsvereinbarung besonders darauf hingewiesen werden muss, dass es sich um eine datenschutzrechtliche Erlaubnisnorm handelt.[58]

Eine ausdrückliche Regelung dazu enthält die DSGVO nicht. In der rechtswissenschaftlichen Literatur wird das z.T. empfohlen[59] bzw. sogar für verpflichtend

---

55 *Wedde*, in: Däubler/Wedde/Weichert/Sommer, EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, Art. 88 Rn. 47.

56 *Maschmann*, DB 2016, 2480.

57 *Körner*, a.a.O., S. 52ff.

58 U.a. *Wurzberger*, ZD 2017, 258; *Dzida/Grau*, Beschäftigtendatenschutz nach der Datenschutz-Grundverordnung und dem neuen BDSG, DB 2018, 189; *Klösel/Mahnhold*, Die Zukunft der datenschutzrechtlichen Betriebsvereinbarung, NZA 2017, 1428.

59 *Tiedemann*, ArbRB 2016, 334, 336; *Wurzberger*, ZD 2017, 258, 260; *Wybitul*, NZA 2017, 1488, 1492.

gehalten.[60] Bei Betriebsvereinbarungen, bei denen sich das ohne weiteres aus dem Kontext ergibt, also vor allem bei denen, die ausschließlich Fragen des Beschäftigtendatenschutzes regeln, ist eine ausdrückliche Nennung eigentlich überflüssig. Bei Betriebsvereinbarungen, die neben der Verarbeitung von Beschäftigtendaten auch andere Themen regeln, kann es eher geboten sein, wenn sich der datenschutzrechtliche Erlaubnisnormcharakter nicht anstandslos erkennen lässt. Daher und weil es ohne großen Aufwand möglich ist, ist zu empfehlen, dass jede Betriebsvereinbarung, die (auch) die Verarbeitung von Beschäftigtendaten zum Gegenstand hat, ihre Funktion als datenschutzrechtliche Erlaubnisnorm (kurz) benennt. Daher sollte jede Betriebsvereinbarung in ihrem Vorspann erwähnen, dass die jeweilige Betriebsvereinbarung als Erlaubnistatbestand i.S.v. Art. 6 DSGVO gelten soll.[61] Eine Pflicht dazu besteht aber nicht.[62]

2. Berücksichtigung von Art. 9 DSGVO

Ähnliches gilt, wenn es um die Verarbeitung sensibler Daten geht. Die nehmen nach **Art. 9 DSGVO** eine Sonderstellung ein, indem ihre Verarbeitung gemäß Abs. 2 nur unter engeren Voraussetzungen zulässig ist als sonst nach Art. 6 DSGVO. Auch hier bliebe die Lage rechtsunsicher, wenn man es genügen ließe, dass sich die Betriebsparteien nur an Art. 9 Abs. 2 DSGVO halten müssten. Besser ist es, die Verarbeitungsbedingungen des Art. 9 Abs. 2 DSGVO, die für den jeweiligen Regelungsgegenstand relevant sind, zu benennen. Das ist ohnehin schon für eine jedenfalls verpflichtende klare Zweckbestimmung und daher aus Transparenzgründen erforderlich. Da Art. 9 DSGVO neben den auch schon in § 3 Abs. 9 BDSG a.F. als sensibel eingestuften Daten jetzt auch genetische und biometrische Daten umfasst, sind die besonderen Schutzbedingungen von Art. 9 DSGVO zu beachten, wenn etwa eine Betriebsvereinbarung Zutrittssysteme mit biometrischen Daten regelt.

3. Berücksichtigung von Art. 5 DSGVO

Ob die datenschutzrechtlichen Grundsätze in Art. 5 Abs. 1 DSGVO, vor allem Zweckbindung, Speicherbegrenzung, Datenminimierung, Transparenz, ausdrücklich in Betriebsvereinbarungen einbezogen werden müssen, wird bislang nicht einheitlich beantwortet. Die Argumente für die Nichtberücksichtigung

---

60 *Klösel/Mahnhold*, NZA 2017, 1428, 1432.

61 *Sydow*, Europäische Datenschutzgrundverordnung, 2017, Art. 88 Rn. 11.

62 So auch *Dzida/Grau*, DB 2018, 189, 194.

überzeugen häufig nicht. So wird dort dann doch für erforderlich gehalten, jedenfalls die Zweckbindung in jede Betriebsvereinbarung aufzunehmen.[63] Auch andere, die die faktische Einhaltung der Datenschutzgrundsätze ausreichen lassen und eine ausdrückliche Aufnahme in die einzelne Betriebsvereinbarung ablehnen, machen Ausnahmen: zusätzlich zum Zweck soll jedenfalls auch noch die Speicherdauer verpflichtend aufzunehmen sein, „gegebenenfalls" auch noch die Datenrichtigkeit.[64]

Diese nicht sehr gradlinigen Vorschläge dürften zu Rechtsunsicherheit führen. Daher ist es besser und ergibt sich auch aus Art. 26 Abs. 5 BDSG n.F., der verlangt, sicherzustellen, dass insbesondere die in Art. 5 DSGVO dargelegten Grundsätze eingehalten werden, die allgemeinen Verarbeitungsgrundsätze aus Art. 5 DSGVO in Betriebsvereinbarungen aufzunehmen, aber danach zu differenzieren, ob es sich um für jede Verarbeitungserlaubnis spezifische Grundsätze handelt, die dann direkt in der fraglichen Betriebsvereinbarung erscheinen müssen (z.B. Zweck und daran gekoppelte Speicherdauer) oder um Verarbeitungsgrundsätze, die für alle Datenverarbeitungsbetriebsvereinbarungen gleichartig sind und daher in einer Rahmenbetriebsvereinbarung geregelt werden könnten, wie die Unterrichtungspflichten nach Art. 13 und 14 DSGVO, Auskunftspflichten nach Art. 15 DSGVO oder Löschkonzepte nach Art. 17 DSGVO.[65]

Jedenfalls reicht es nicht, wenn die datenschutzrechtlichen Grundsätze nur beachtet werden.[66] Auch nach dieser Ansicht wird allerdings konzediert, dass es für neu abzuschließende Kollektivvereinbarungen zu empfehlen ist, „die datenschutzrechtlichen Grundsätze in ausdrückliche Regelungen zu übersetzen".[67]

Der zentrale Grundsatz des Datenschutzrechts, die Zweckbindung jeder Verarbeitung (**Art. 5 Abs. 1 lit. b DSGVO**) ist zwar in vielen Betriebsvereinbarungen bereits enthalten, häufig aber nicht präzise genug. Hier besteht Kontroll-

---

63 *Dzida*/*Grau*, DB 2018, 189, 192.

64 *Wurzberger*, ZD 2017, 258, 261, der von *Dzida*/*Grau* fälschlicherweise als ein Vertreter der Ansicht zitiert wird, alle Datenschutzgrundsätze aus Art. 5 DSGVO wären in jede Betriebsvereinbarung aufzunehmen. Tatsächlich meint *Wurzberger* etwas vage, die Grundsätze wären „zu adressieren" und hebt dann besonders wichtige hervor, die jedenfalls in jede einzelne Betriebsvereinbarung aufzunehmen seien.

65 Zu Rahmenbetriebsvereinbarungen noch unten E.II. und F.IV.

66 So aber *Dzida*/*Grau*, a.a.O.

67 A.a.O.

und ggfs. Nachbesserungsbedarf in jedem Einzelfall,[68] weil der Zweck der Dreh- und Angelpunkt für jede Datenverarbeitung und alle daraus folgenden Befugnisse und Einschränkungen für die Verwendung der Beschäftigtendaten ist. Soll etwa eine Personaldatenbank eingeführt werden, würde als Zweckbestimmung „Personalverwaltung" nicht reichen, sondern es müsste genau angegeben werden, welche Daten für wie lange und für welche Verwendungen im Einzelnen verarbeitet werden sollen. Für diese genauen Beschreibungen bieten sich die Verzeichnisse gemäß Art. 30 DSGVO an.[69]

In vielen Betriebsvereinbarungen dürfte es Anpassungsbedarf beim Aspekt Datenminimierung geben (**Art. 5 Abs. 1 lit. c DSGVO**), also die Begrenzung der Daten auf das für den Zweck unbedingt erforderliche Maß, etwa wenn für statistische Personalplanungszwecke pseudonymisierte Daten ausreichen würden, aber Klarnamendaten verarbeitet werden. Bei der Datenminimierung sind technische Maßnahmen von besonderer Bedeutung.[70] Da Art und Umfang der Datenminimierung vom jeweiligen Zweck der Datenverarbeitung abhängen, müssen die entsprechenden Minimierungsmaßnahmen in die konkrete Betriebsvereinbarung aufgenommen werden und es reichen nicht etwa allgemeine Hinweise in einer Rahmenbetriebsvereinbarung, dass der Grundsatz der Datenminimierung einzuhalten sei.

Entsprechendes gilt für **Art. 5 Abs. 1 lit. d DSGVO** zur Datenrichtigkeit, wo es darum geht, dass die Daten sachlich richtig und, soweit erforderlich, auf dem neuesten Stand sind, wenn Betriebsvereinbarungen noch keine Berichtigungsverfahren vorsehen. Da ursprünglich richtige Daten aber rasch veralten können, wird man eine laufende Prüfungs- und Korrekturpflicht nicht annehmen, sondern auf die Fälle begrenzen können, dass Fehler bekannt werden. Im Einzelfall kann das aber auch anders aussehen. Ob hier die Aufnahme in eine Rahmenbetriebsvereinbarung reicht oder Berichtigungsverfahren in die konkrete Betriebsvereinbarung aufgenommen werden müssen, hängt von den Beschäftigtendaten-Betriebsvereinbarungen im Betrieb ab. Wenn für alle die gleichen Berichtigungsverfahren in Betracht kommen, können die in einer Rahmenbetriebsvereinbarung geregelt werden.

---

68 Das sehen auch diejenigen so, die ansonsten – für Altvereinbarungen – keine ausdrückliche Neuregelungspflicht annehmen, vgl. *Dzida*/*Grau*, a.a.O.; *Gaul*/*Pitzer*, ArbRB 2017, 241, 243; *Wybitul*, NZA 2017, 1488, 1492.

69 Vgl. dazu unten G.III.

70 Dazu unten E.IV.

Auch eine Speicherbegrenzung muss gemäß **Art. 5 Abs. 1 lit. e DSGVO** ausdrücklich vorgesehen werden. Eine Regelung, dass Beschäftigungsdaten zu löschen sind, wenn sie nicht mehr benötigt werden, ist zu ungenau. Fristen müssen klar festgelegt werden und ihre Länge dem konkreten Zweck angepasst sein. Unzweifelhaft kann das Speichern von Beschäftigtendaten, deren Zweck erfüllt ist, für den Betriebsrat weiterhin nützlich sein, etwa um länger zurückliegende Vorgänge rekonstruieren zu können, ist aber nicht zulässig, wenn es dafür keinen konkreten Zweck (mehr) gibt. Das war zwar nach bisheriger Rechtslage auch schon so, wurde aber längst nicht immer beachtet. Da die zulässige Speicherdauer vom Zweck der Datenverarbeitung abhängt, muss sie in die Einzelbetriebsvereinbarung aufgenommen werden.

Bei **Art. 5 Abs. 1 lit. f i.V.m. Art. 32 DSGVO** („Integrität und Vertraulichkeit", Datensicherheit) geht es um den Schutz vor unbefugter Datenverarbeitung, besonders um klare Regelungen etwa zum Kreis auswertungsberechtigter Personen von Videoaufnahmen, aber auch sonstigen Zugriffsrechten. Dabei reicht es nicht, dass die berechtigten Personen nur genannt werden. Der Kreis der berechtigten Personen muss auch mit dem Zweck korrelieren und darf nicht zu weit gesteckt sein. Da der Zweck der Datenverarbeitung in jeder Betriebsvereinbarung zum Beschäftigtendatenschutz ein anderer ist, muss auch der Kreis der berechtigten Personen jeweils genannt werden und es reicht nicht, diesen Punkt in einer Rahmenbetriebsvereinbarung zu regeln. Technische und organisatorische Vorkehrungen[71] spielen auch hier eine große Rolle.

4. Transparenzregeln

Die inhaltlich-materiellen Transparenzvorgaben sind ein Kernstück der DSGVO.[72] Es müssen dabei sowohl die Datenverarbeitung als solche für die Betroffenen „durchsichtig", wie auch nach Art. 12 Abs. 1 DSGVO die Betroffenenrechte und die Modalitäten ihrer Ausübung leicht nachvollziehbar sein.

Bei den Transparenzanforderungen aus **Art. 5 Abs. 1 lit. a DSGVO** dürfte in vielen Fällen alter Betriebsvereinbarungen nachzubessern sein und ist bei neuen auf klare Angaben dazu, wie die Transparenz gewährleistet werden soll, zu achten. Ob das jeweils in der konkreten Betriebsvereinbarung geregelt werden muss oder eine allgemeine Regelung in einer Rahmenbetriebsvereinbarung[73]

---

71 Zum Datenschutz durch Technik vgl. unten E.IV.

72 *Korinth*, ArbRB 2018, 47.

73 Dazu noch unten E.II. und F.IV.

ausreicht, hängt vom konkreten Einzelfall ab. Wenn vor dem Hintergrund der bestehenden Betriebsvereinbarungen zum Beschäftigtendatenschutz in einem Betrieb die Transparenzregeln jeweils gleich auszugestalten wären, reicht deren Aufnahme in eine Rahmenbetriebsvereinbarung. Wenn sich allerdings die Datenverarbeitungsvorgänge je nach Zweck der Datenerhebung unterscheiden, müssen diese Datenverarbeitungsmodalitäten in der jeweiligen Betriebsvereinbarung genau und verständlich dargestellt werden. Jedenfalls müssen sich Art, Inhalt und Umfang der legitimierten Verarbeitungsvorgänge klar aus der Betriebsvereinbarung ergeben.[74]

Als derzeit gültiger Maßstab können dafür die Grundsätze der *Keylogger*-Entscheidung des BAG (noch zum alten Recht)[75] und die EGMR-Entscheidung in der Sache *Barbulescu*[76] herangezogen werden. In der *Keylogger*-Entscheidung hatte der Arbeitgeber auf dem PC des Arbeitnehmers ein Programm (Keylogger) installiert, das alle Tasteneingaben protokollierte und regelmäßig Screenshots anfertigte und speicherte. Die Auswertung ergab eine teilweise Privatnutzung durch den Arbeitnehmer während der Arbeitszeit, die den Arbeitgeber zur Kündigung veranlasste. Das BAG behandelte den Einsatz des Keyloggers wie eine verdeckte Videokontrolle, sah aber deren Voraussetzungen als nicht erfüllt an – weder hatte der Arbeitnehmer in derartige Kontrollmaßnahmen wirksam eingewilligt noch lag ein konkreter Anfangsverdacht einer Straftat oder anderen schweren Pflichtverletzung vor – und hielt daher die gewonnenen Erkenntnisse für nicht verwertbar. Allerdings ließ das BAG anklingen, dass transparente, also offene Überwachungsmaßnahmen, die der Verhinderung von Pflichtverletzungen dienen, denkbar seien, wenn diese nach abstrakten, keinen Arbeitnehmer unter Verdacht stellenden Kriterien durchgeführt würden. Genaueres sagt das Gericht dazu aber nicht, weil es darauf im konkreten Fall nicht ankam.

Ähnlich und für das Unionsrecht relevanter äußert sich der EGMR in der *Barbulescu*-Entscheidung. Entgegen eines ausdrücklichen Verbots, aber ohne Hinweis auf Überwachungsmaßnahmen hatte ein rumänischer Ingenieur ausweislich eines 45-seitigen Chat-Protokolls seinen dienstlichen PC und Internetzugang auch privat genutzt. Die Kleine Kammer des EGMR hatte die fristlose Kündigung noch für zulässig und die Verwertung des 45-seitigen Chat-Protokolls mit Art. 8 EMRK sowie der EU-Datenschutzrichtlinie für vereinbar

---

74 *Schrey/Kielkowski*, BB 2018, 629, 632.

75 BAG, Urt. v. 27.7.2017 – 2 AZR 681/16, NZA 2017, 1327.

76 EGMR, Urt. v. 5.9.2017 – 61496/08 – Barbulescu./.Rumänien, NZA 2017, 1443.

gehalten.[77] Die Große Kammer dagegen stellte einen Verstoß gegen das Recht auf Achtung des Privatlebens und der Korrespondenz aus Art. 8 EMRK fest. Zwar dürfe der Arbeitgeber im Prinzip den dienstlichen Internetanschluss überwachen, um Verstöße gegen das Privatnutzungsverbot festzustellen. Diese Überwachung müsse aber verhältnismäßig sein, was u.a. bedeute, dass der Arbeitnehmer vorab umfassend über Art und Umfang der Überwachung sowie über die tatsächliche Einführung informiert werden müsse, die darüber hinaus das mildeste Mittel sein müsse. Eine Überwachung ist also, wie nach der *Key-logger*-Entscheidung des BAG, nur offen zulässig.

Auf dieser Linie liegt auch die Entscheidung des EGMR im Fall *Lopez Ribalda*,[78] in dem es um die Installation von Überwachungskameras in einem Supermarkt ohne Wissen der Beschäftigten ging, was der EGMR auch für einen Verstoß gegen Art. 8 EMRK hielt. Im Fall *Libert/France* dagegen hielt der EGMR Art. 8 EMRK nicht für verletzt.[79] In diesem Fall hatte der Arbeitgeber in begrenztem Umfang die Speicherung von privaten Daten auf dem dienstlichen PC erlaubt unter der Voraussetzung, dass diese Daten ausdrücklich als privat gekennzeichnet würden. Das hatte der Arbeitnehmer versäumt, als er von einem Stick pornographisches Material auf den Dienst-PC überspielte. Daher erlangte der Arbeitgeber davon Kenntnis und kündigte, was alle Instanzen in Frankreich für gerechtfertigt hielten und auch der EGMR unter dem Gesichtspunkt von Art. 8 EMRK absegnete.

Über Art. 52 Abs. 3 S. 1 GR-Charta haben die EGMR-Entscheidungen Auswirkungen auf die Auslegung der DSGVO, denn Art. 7 GR-Charta auf Achtung des Privatlebens und Art. 8 GR-Charta über den Schutz personenbezogener Daten entsprechen Art. 8 EGMR. Für diesen Fall regelt Art. 52 Abs. 3 S. 1 GR-Charta, dass Rechte aus der GR-Charta, die Rechten aus der EMRK entsprechen, die gleiche Bedeutung und Tragweite haben wie die EMRK-Rechte. Die Auslegung von Art. 8 EMRK durch den EGMR in den genannten Fällen kann also direkt für die Auslegung der GR-Charta und die auf dieser beruhenden DSGVO herangezogen werden.

---

77 EGMR, Urt. v. 12.1.2016 – 61496/08, DuD 2016, 395.
78 EGMR, Urt. v. 9.1.2018 – 1874/13 (Lopez Ribalda u.a./Spanien), NLMR 2018, 38.
79 EGMR, Urt. v. 22.2.2018 – 588/13 (Libert/France), ZD 2018, 263.

III. Betroffenenrechte

Neben den Datenschutzgrundsätzen enthält die DSGVO umfangreiche Betroffenenrechte. Mit denen steht und fällt die Effizienz des Beschäftigtendatenschutzes. Daher kommt es darauf an, wie in Betriebsvereinbarungen damit umzugehen ist.

Es geht um die durch die DSGVO gestärkten Rechte der Betroffenen auf Information über die erhobenen Daten (nach **Art. 13 DSGVO**, wenn Daten direkt beim Betroffenen erhoben werden, nach **Art. 14 DSGVO**, wenn die Daten anderweitig erhoben werden – insgesamt gehen diese Informationspflichten weiter als in §§ 33–35 BDSG a.F.), Auskunft (**Art. 15 DSGVO**), Berichtigung (**Art. 16 DSGVO**) und Löschung (**Art. 17 DSGVO**), Einschränkung der Datenverarbeitung (**Art. 18 DSGVO**) sowie Widerspruch gegen bestimmte Datenverarbeitungen (**Art. 21 DSGVO**).

Über all diese Rechte ist der Betroffene gemäß **Art. 12 Abs. 1 DSGVO** in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu unterrichten". Diese Unterrichtungspflicht muss auch in einer die Verarbeitung von Beschäftigtendaten betreffenden Betriebsvereinbarung erfüllt werden.[80] Allerdings würde angesichts der Fülle der Informationspflichten und ihrer Gleichförmigkeit die Aufnahme der Betroffenenrechte in jede einzelne Betriebsvereinbarung zum reinen Formalismus degenerieren und würde daher gerade der Transparenz der Datenverarbeitung entgegenstehen. Aus diesem Grund bieten sich hier andere Formen der betrieblichen Umsetzung an, etwa Rahmenbetriebsvereinbarungen.[81]

Dort sollte dann nicht nur die gesetzliche Regelung wiedergegeben werden, sondern sollten Vorschriften formuliert werden, die die Transparenzvorgaben ausfüllen, z.B. den Kriterienkatalog des Art. 13 DSGVO konkretisieren.[82] Dennoch bleibt es möglich und kann es für die Betroffenen hilfreich sein, in einer (Rahmen-)Betriebsvereinbarung den Gesetzestext – sprachlich angepasst – zu wiederholen.

Gegen das europarechtliche Wiederholungsverbot würde das nicht verstoßen. Dabei geht es um die Frage, ob nationale spezifischere Vorschriften i.S.v. Art. 88

---

80 Z.T. als Pflicht gesehen bei *Imping*, CR 2017, 378, 380; *Wurzberger*, ZD 2017, 258, 262; *Tiedemann*, ArbRB 2016, 334, 336. Als Empfehlung gesehen bei *Sörup/Marquart*, ArbRAktuell 2016, 103, 105; *Wybitul*, NZA 2017, 1488, 1489.

81 So u.a. *Sörup*, ArbRAktuell 2016, 207; dazu auch noch unten E.II. und F.IV.

82 *Klösel/Mahnhold*, NZA 2017, 1428, 1431.

Abs. 1 DSGVO Teile enthalten dürfen, die die DSGVO nur wiederholen. Das ist eigentlich unzulässig, da verhindert werden soll, dass die Prüfungskompetenz des EuGH eingeschränkt wird, die sich gemäß Art. 267 AEUV auf Unionsrecht beschränkt.[83] Allerdings hat der europäische Gesetzgeber in der DSGVO in Erwägungsgrund 8 eine Ausnahme zugelassen. Danach dürfen Teile der Verordnung in die nationale Regelung übernommen werden, soweit dies erforderlich ist, „um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen". Das ist für Betriebsvereinbarungen besonders relevant, denn anders als in einem eine Materie systematisch regelnden Gesetz werden dort nur bestimmte Sachverhalte aufgegriffen, weshalb es für die Adressaten zum Verständnis sogar nötig sein kann, dass allgemeine Regelungen der DSGVO wiedergegeben werden.[84]

Da sich allerdings die Betroffenenrechte zunächst an den Arbeitgeber richten, treffen sie ihn jedenfalls unabhängig davon, ob eine Betriebsvereinbarung vorliegt oder nicht. Daher kann es auch ausreichen, dass der Arbeitgeber diesen Pflichten einseitig nachkommt.[85] Allerdings bleibt es auch dann empfehlenswert, die Pflichten aus Art. 12ff. DSGVO in einer Betriebsvereinbarung zu dokumentieren und ggfs. zu konkretisieren.[86] Darüber hinaus kann diese Verlagerung auf den Arbeitgeber nur gelten, soweit es um Beschäftigtendaten geht, die der Arbeitgeber selbst generiert, nicht wenn der Betriebsrat eigene Beschäftigtendaten erhebt und verarbeitet.[87]

---

83 *Selk*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2017, Art. 45ff.

84 A.a.O.

85 *Dzida/Grau*, DB 2018, 189, 193; *Klösel/Mahnhold*, NZA 2017, 1428, 1431.

86 So auch *Dzida/Grau*, DB 2018, 189, 193, die an sich nur den Arbeitgeber in der Pflicht sehen.

87 Dazu unten G.II.

E. Zu regelnde Datenschutzinhalte in Betriebsvereinbarungen

Zwar ändert sich für Deutschland durch die DSGVO im materiellen Datenschutzrecht wenig, vor allem, was die Grundprinzipien des Datenschutzes angeht. Da aber die Informations- und Transparenzanforderungen deutlich zugenommen haben und die Betroffenenrechte ausgebaut worden sind, gibt es für Betriebsvereinbarungen zum Beschäftigtendatenschutz einiges neu zu beachten und das schon Bekannte klarer zu regeln. Grundsätzlich müssen alle Betriebsvereinbarungen zur Verarbeitung von Beschäftigtendaten den Definitionen und Begrifflichkeiten der DSGVO entsprechen. Das dürfte allerdings i.d.R. kein großes Problem sein, da vieles aus dem BDSG a.F. bereits bekannt und gewohnt ist.

Die Liste der in Betriebsvereinbarungen aufzunehmenden Datenschutzregelungen ist lang. Es kann jedoch danach unterschieden werden, ob die jeweilige Datenschutzregelung in jede einzelne Betriebsvereinbarung aufgenommen werden muss oder ob es ausreicht, pauschal in Rahmenbetriebsvereinbarungen zu regeln. Danach wird in der folgenden Darstellung unterschieden.

I. Notwendige Datenschutzinhalte in Einzelbetriebsvereinbarungen

Nicht alle unter D. genannten Aspekte müssen in allen Betriebsvereinbarungen zum Beschäftigtendatenschutz berücksichtigt werden. Es müssen nur die aufgenommen werden, die in der jeweiligen Betriebsvereinbarung eine Rolle spielen. Dazu gehört jedenfalls der Zweck der Verarbeitung i.S.v. § 26 Abs. 5 BDSG i.V.m. Art. 5 DSGVO, die Dauer der Verarbeitung, Löschungsregeln und die Zugriffsrechte.

Im Einzelnen sollte geregelt werden:

1. Hinweis in der Betriebsvereinbarung, dass es sich um eine eigenständige datenschutzrechtliche Rechtfertigungsgrundlage handelt. Das ist zwar nicht zwingend – alte Betriebsvereinbarungen müssen also darauf nicht angepasst werden –, aber empfehlenswert.

2. Vorgaben des Art. 88 Abs. 2 DSGVO, die im Wesentlichen § 75 BetrVG entsprechen, soweit für den konkreten datenschutzrechtlichen Regelungsinhalt der Betriebsvereinbarung relevant.

3. Grundsätze der DSGVO, soweit sie Mindeststandards darstellen und nicht gleichartig für alle Betriebsvereinbarungen im Unternehmen gelten (dann ggfs. Rahmenbetriebsvereinbarung, s.u.):

   - Zentral ist gemäß Art. 5 Abs. 1 lit. b DSGVO der Zweck der Datenverarbeitung, der nicht nur allgemein, sondern konkret beschrieben sein muss unter Nennung der für die Erfüllung des Zwecks benötigten Daten. Dabei dürfen nur für den Zweck erforderliche Daten erhoben werden und es ist dem Prinzip der Datenminimierung Rechnung zu tragen.
   - Zweckänderungen – können sich auch während der Laufzeit einer Betriebsvereinbarung ergeben. Ohne Regelung in einer Betriebsvereinbarung ergeben sich die gesetzlichen Voraussetzungen aus § 24 Abs. 1 BDSG n.F.
   - Sollen besondere Daten i.S.v. Art. 9 Abs. 1–3 DSGVO i.V.m. § 26 Abs. 3 BDSG verarbeitet werden, z.B. Gesundheitsdaten, sind die Voraussetzungen, die die Verarbeitung erlauben, zu benennen.[88] Hier sind spätere Zweckänderungen unter den Voraussetzungen von § 24 Abs. 2 BDSG n.F. zulässig und können in einer Betriebsvereinbarung auch strenger geregelt werden.
   - Beschreibung der von der Verarbeitung betroffenen Personen und der Empfänger der Daten.
   - Sofern Betriebsvereinbarungen Regelungen zur Einwilligung enthalten sollen, sind die Voraussetzungen von Art. 7 DSGVO zu beachten, insbesondere sind Hinweise auf das Widerrufsrecht aufzunehmen.
   - Zugriffsrechte des Betriebsrats bezüglich der Frage, ob eine Betriebsvereinbarung eingehalten worden ist.
   - Bei Datenverarbeitung des Betriebsrats müssen Zugriffsrechte in Verbindung zum Verarbeitungszweck geregelt werden: zu differenzieren nach Daten, auf die alle Betriebsratsmitglieder Zugriff haben sollen, und solchen, die nur für Ausschüsse bestimmt sind (z.B. Personalausschuss) oder nur für einzelne Funktionsträger (z.B. Mitglieder im BEM-Ausschuss).

---

88 Details in IGM, Handlungshilfe für Betriebsräte und Vertrauensleute Nr. 19: Datenschutz-Grundverordnung 4/2018, S. 19 ff.

- ... Löschfristen sind anzugeben; ggfs. Hinweis auf ein Löschkonzept mit Hilfe technischer Voreinstellungen.
- ... Ggfs. Schnittstellen zu anderen Systemen. Je nach konkreter Ausgestaltung kann dieser Punkt auch in einer Rahmenbetriebsvereinbarung geregelt werden.

II. Datenschutzregelungen in Rahmenbetriebsvereinbarungen[89]

Auch die folgenden Themen, insbesondere die Betroffenenrechte, sind in Betriebsvereinbarungen zu regeln. Da es sich dabei aber um Gegenstände handelt, die unabhängig vom jeweiligen konkreten Datenverarbeitungszweck immer gleich auszugestalten sind, müssen sie nicht in jeder Betriebsvereinbarung aufgeführt, sondern können als Allgemeiner Teil der betrieblichen Regelungen zur Datenverarbeitung von Beschäftigtendaten in einer Rahmenbetriebsvereinbarung zusammengefasst werden. Dazu gehören insbesondere:

1. Geltungsbereich der Rahmenbetriebsvereinbarung.
2. Hinweise auf Verantwortliche, betrieblichen Datenschutzbeauftragen und die zuständige staatliche Datenschutzbehörde.
3. Ggfs. klarstellender Hinweis darauf, dass die Zweckbestimmung für die konkrete Verarbeitung von Beschäftigtendaten jeweils in den einzelnen Betriebsvereinbarungen zu finden ist.
4. Die allgemeinen Verarbeitungsgrundsätze nach Art. 5 DSGVO.
5. Vor allem Beschäftigtenrechte, wie Informations- (Art. 13f. DSGVO) und Auskunftsrechte (Art. 15 DSGVO) sowie sonstige Betroffenenrechte (Art. 16–21). Diese Rechte sind ausführlicher als im BDSG a.F., z.B. die Mitteilungspflicht bei beabsichtigter Zweckänderung in Art. 13 Abs. 3 und Art. 14 Abs. 4 DSGVO.
6. Angaben zu den technischen Datenschutzmaßnahmen, Art. 25 DSGVO, d.h. Mindestanforderungen an jede IT-Anwendung (u.a. Anonymisierung, Pseudonymisierung, Verschlüsselung, Löschroutinen).[90]

---

89 Da Rahmenbetriebsvereinbarungen vor allem für die „Rettung" von alten Betriebsvereinbarungen eine große Rolle spielen, werden sie ausführlicher dort behandelt, vgl. unten F.IV.

90 Zum technischen Datenschutz auch noch im Folgenden unter IV.

7. Ggfs. Angaben zu den datenschützenden Voreinstellungen der IT-Systeme.
8. Anlage zur Systemdokumentation mit klar strukturierten Systemen, inkl. Zugriffsberechtigungen (wenn die nicht in der Einzelbetriebsvereinbarung geregelt werden muss) und System-Schnittstellen (ggfs. in Form von Steckbriefen[91]).
9. Regelung zur Datenübermittlung an Dritte sowie ggfs. zum internationalen Datentransfer.
10. Ggfs. Regelungen zur Datenschutzfolgenabschätzung.[92]
11. Regelung zu den Rechten des Betriebsrats, wie Einsichtsrechte in Unterlagen des Arbeitgebers, um die Einhaltung der Rahmenbetriebs- und anderer Betriebsvereinbarungen zum Beschäftigtendatenschutz zu überwachen.
12. Empfehlenswert ist auch eine Regelung zum Einsatz von IT-Sachverständigen i.S.v. § 80 Abs. 3 BetrVG, um Diskussionen in jedem Einzelfall zu vermeiden. Da der Streit i.d.R. um die Kosten kreist, wäre an die Festlegung eines Budgets zu denken.[93]
13. Ggfs. Zugriffsrechte: hier kommt es darauf an, ob die Zugriffsrechte allgemein für alle Verarbeitungssituationen einheitlich geregelt werden können oder sich, je nach Verarbeitungssituation, unterscheiden. Dass Letzteres häufig vorkommen wird, ist wahrscheinlich, da die Zugriffsberechtigungen so eng wie möglich gestaltet werden müssen und an den Verarbeitungszweck gebunden sind. Die müssen dann in der Einzelbetriebsvereinbarung geregelt werden.
14. Regelungen zu Korrekturmechanismen bei unrichtigen oder unrichtig gewordenen Daten. Je nach dem um welche Art von personenbezogenen Beschäftigtendaten es sich handelt, können Berichtigungsverfahren auch in die jeweilige Einzelbetriebsvereinbarung aufgenommen werden müssen.
15. Ggfs. Festlegung von technischen und organisatorischen Maßnahmen zur Datensicherheit als Konkretisierung von Art. 32 i.V.m. 5 Abs. 1 lit. f DSGVO.

---

91 Vgl. dazu unten F.V.

92 Zu Mitwirkungsmöglichkeiten des Betriebsrats an der Datenschutzfolgenabschätzung schon oben C.III.

93 *Schulze/Pfeffer*, ArbRAktuell 2017, 358ff., Nr. 8.

16. Verfahren bei Streitigkeiten: da es sich bei Rahmenbetriebsvereinbarungen um freiwillige Vereinbarungen nach § 88 BetrVG handelt, ist zu empfehlen, die Anrufung einer Einigungsstelle durch jede Seite und verbindliche Entscheidung derselben vorzusehen.

Insgesamt ist – auch im Hinblick auf alte Betriebsvereinbarungen,[94] für die es nahezu unmöglich sein wird, zeitnah eine perfekte Anpassung an die DSGVO zu gewährleisten – zu einem abgestimmten Gesamtkonzept zu raten mit Rahmenbetriebsvereinbarungen, Musterbetriebsvereinbarungen und ergänzenden betrieblichen Maßnahmen wie hinreichende Bekanntmachungen im Betrieb (z.B. Intranet, Mail an die einzelnen Beschäftigten o.Ä.) sowie der Etablierung eines Datenschutz-Management-Systems, nach dem die Datenverarbeitung regelmäßig zu überprüfen ist.[95] Für die Datenschutzfolgenabschätzung sieht die DSGVO eine derartige Überprüfung in Art. 35 Abs. 11 ohnehin vor. Zum Datenschutzmanagement könnten freiwillige Betriebsvereinbarungen abgeschlossen werden.

Angesichts der hohen Transparenzanforderungen, die nicht nur die Beschäftigten schützen, sondern auch für die Aufsichtsbehörden von großer Bedeutung sind, sollten jedenfalls Muster für die Gestaltung der IT-Systeme entwickelt werden, aus denen sich der Verarbeitungszweck, die Beschreibung der verarbeiteten Daten, Speicherorte und -dauer, Zugriffsrechte, Datensicherheitsmaßnahmen u.Ä. ergeben. Diese Muster können dann bei jeder neuen Verarbeitungsart von den IT-Fachleuten ausgefüllt werden.[96] In Gestalt von Steckbriefen gibt es diese Muster in der betrieblichen Praxis vereinzelt schon.[97]

III. Übersicht über Datenverarbeitungs-Regelungsgegenstände

Die potentiellen Regelungsgegenstände für Betriebsvereinbarungen zum Beschäftigtendatenschutz lassen sich nicht abschließend benennen. Daher ist die nachfolgende Aufzählung als beispielhafte Vorschlagsliste für Datenschutzthemen zu verstehen, die in Betriebsvereinbarungen geregelt werden können

---

94 Zu diesen noch unten F.

95 Auch empfohlen im Rundbrief Arbeitnehmeranwälte, 39/2018, S. 13.

96 *Klösel/Mahnhold*, Die Zukunft der datenschutzrechtlichen Betriebsvereinbarung, NZA 2017, 1428, 1433.

97 S.u. F.V.

und sollten. In Anlehnung an die technische Entwicklung handelt es sich dabei um eine „atmende“ Liste. Die Zulässigkeit ihrer Regelungsgegenstände ist an der Generalklausel des Art. 88 Abs. 1 DSGVO i.V.m. § 26 Abs. 4 BDSG n.F. zu messen, wonach die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses erforderlich sein muss.

Dazu gehören alt bekannte Themen wie u.a. Überwachung von E-Mail, Internet – bei beiden mit dem Problem der privaten Nutzung –, Videoüberwachung, GPS-Ortung, Zugangssysteme zum Arbeitsplatz mit Chipkarten oder biometrischen Daten, die Nutzung von Arbeitnehmerhardware (Bring your own device – BYOD) oder Wearables am Arbeitsplatz, elektronische Personalakte oder Veröffentlichung von Beschäftigtendaten auf der Homepage des Arbeitgebers.

Brisanter werden diese Datenverarbeitungsformen durch die große Menge an digitalen Spuren, die allein ihre Nutzung durch „intelligente“ Geräte sowie die Vernetzung der Datenbestände fast zwangsläufig hinterlässt. Ohne Vernetzung allerdings wäre etwa eine Arbeitsform wie das Home-Office nicht realisierbar. Abhilfe könnte hier nur deutlich mehr Anonymisierung und Verschlüsselung bringen, aber das ist – jedenfalls was das Surfen im Internet betrifft –, ein zweischneidiges Schwert, wie allein der negativ konnotierte Begriff „dark net“ zeigt.

Auch andere, neue Themen, die in der DSGVO nur punktuell Beachtung gefunden haben, werden in Zukunft beim Beschäftigtendatenschutz eine große Rolle spielen. Dazu gehören vor allem Big Data-Anwendungen, d.h. die Verarbeitung von sehr großen Datenmengen mit automatisierter Auswertung zum Zwecke der Vorhersage zukünftiger Entwicklungen, aber auch Verhaltensweisen Einzelner. Die DSGVO greift das zunächst in ihrer Definitionsnorm Art. 4 Nr. 4 als „Profiling“ auf, bei dem es darum geht, durch automatisierte Verarbeitung personenbezogener Daten Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel einer Person zu analysieren oder vorherzusagen. Zwar enthält die DSGVO keine ausdrückliche Erlaubnisnorm für Profiling. Der Umstand aber, dass das Verfahren überhaupt an mehreren Stellen angesprochen und genau beschrieben wird (auch bei den Betroffenenrechten in Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO), macht deutlich, dass der DSGVO-Gesetzgeber von der Möglichkeit eines rechtmäßigen Einsatzes derartiger Verfahren ausgeht, was gemäß Erwägungsgrund 71 durch „angemessene Garantien“ flankiert werden soll. Profiling ist längst Datenverarbeitungsrealität. Deshalb ist es auch zu kurz gegriffen, anzunehmen, im Beschäftigungskontext gäbe es nach (nicht

belegter) „verbreiteter Ansicht“ keine rechtmäßigen Zwecke, die ein Profiling rechtfertigen könnten.[98] Profiling wird möglicherweise im Beschäftigungsverhältnis gerade deshalb als problematisches Verfahren wahrgenommen, weil es – geeignete mathematische oder statistische Verfahren vorausgesetzt (so auch Erwägungsgrund 71) – in vielen Zusammenhängen nach Informatikeraussagen zumindest scheinbar treffsicherere Voraussagen erlaubt als subjektive menschliche Urteile. Da das Unbehagen über rein automatisierte Entscheidungen daher noch immer berechtigt ist, sieht Art. 22 Abs. 1 DSGVO vor, dass die betroffene Person das Recht hat, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden. Da Art. 22 Abs. 2 DSGVO aber leicht zu erfüllende Ausnahmen erlaubt, wird das Thema in Zukunft Gegenstand von Betriebsvereinbarungen werden (müssen). Das gilt auch für alle Verfahren, die unter dem Sammelbegriff „Künstliche Intelligenz“ die Vernetzung von Mensch und Maschine, RFID-Technik, Internet der Dinge, aber auch Robotik umfasst.

Es hilft den Betriebsparteien vor Ort zwar derzeit praktisch nicht weiter, muss aber dennoch immer wieder betont werden, dass die DSGVO mit ihren aus den 1970er Jahren stammenden Datenschutzkonzepten hier wenig Datenschutz-Hilfe bietet. Umso mehr kommt es auf zukunftsweisende Vereinbarungen auf der betrieblichen Ebene an. Die nutzen zwar zunächst nur Beschäftigten mit Betriebsrat, können aber ggfs. auch modellbildend für durch Art. 88 DSGVO weiterhin geöffnete nationale gesetzliche Regelung werden. Auf den Betriebsparteien ruht also insoweit eine höhere Verantwortung als bisher.

IV. Technische Maßnahmen

Die letzten Beispiele zeigen schon: die Konzeption eines wirkungsvollen Datenschutzes wandelt sich. Allein normative Vorgaben für Datenschutz sind nicht mehr ausreichend. Sie müssen durch technische Maßnahmen flankiert werden, durch die Hard- und Software so gestaltet werden, dass bestimmte Verarbeitungsformen entweder gar nicht erst bereitgestellt oder eingeschränkt werden. Diesen Gedanken greift Art. 25 DSGVO über Datenschutz durch Technikgestaltung („privacy by design“) und datenschutzfreundliche Voreinstellungen („privacy by default“) auf, der den Verantwortlichen verpflichtet, „geeignete techni-

98 So in IGM, Handlungshilfe für Betriebsräte und Vertrauensleute Nr. 19, Datenschutz-Grundverordnung 4/2018, S. 24.

sche und organisatorische Maßnahmen“ zu treffen (Abs. 1) und durch Voreinstellungen nur „erforderliche“ personenbezogene Daten zu erheben (Abs. 2). Die Vorschrift ist rechtsunsicher, da neben dem einzigen Beispiel Pseudonymisierung unklar bleibt, zu welchen technischen Maßnahmen der Verantwortliche verpflichtet ist, zumal die Pflicht auch noch durch Implementierungskosten, die Eintrittswahrscheinlichkeit und Schwere von Risiken sowie allgemein die Umstände der Verarbeitung relativiert wird.

Auch Art. 32 DSGVO über die Sicherheit der Verarbeitung personenbezogener (Beschäftigten-)Daten empfiehlt vor allem geeignete technische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Konkretes wird, außer wiederum Pseudonymisierung und zusätzlich Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO), auch bei Art. 32 DSGVO nicht geboten.

Da aber der Beschäftigtendatenschutz für nationale Regelungen geöffnet ist und darunter auch Betriebsvereinbarungen fallen, ist den Betriebsparteien ein weites Feld für technischen Datenschutz in Betriebsvereinbarungen eröffnet. Wo der sich ans Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG anknüpfen lässt, sind die Regelungen zwingend, ansonsten kann auf freiwillige Betriebsvereinbarungen gemäß § 88 BetrVG zurückgegriffen werden.

Die Möglichkeiten für technischen Datenschutz sind vielfältig: sie reichen neben Anonymisierung und Pseudonymisierung oder Löschroutinen für nicht mehr erforderliche Daten, und automatische Verfallstermine für gespeicherte Daten über Verschlüsselung bis zu restriktiven Zugriffsmechanismen. Auch die technische Trennung von Beschäftigtendaten, die zu unterschiedlichen Zwecken verarbeitet werden, wie Personalverwaltung, Telefon- und Smartphone-Nutzung, Zugangssysteme, interne soziale Netzwerke oder Ortungssysteme, ist vorzunehmen.[99] Um wirksame Standards für technische Voreinstellungen für die Verarbeitung von Beschäftigtendaten zu definieren, müssen allerdings die z.T. hochkomplexen Verarbeitungszusammenhänge verstanden werden. Damit sind vor allem Betriebsräte in kleineren Unternehmen häufig überfordert. Daher bedarf es hier ausreichender IT-Beratung von außen, um geeignete technische Voreinstellungen zu wählen. Hier bieten das Bundesamt für Sicherheit in der Informationstechnologie (BSI)[100] und das Standard-Datenschutzmodell der

---

99 Umfangreiche Vorschläge finden sich in: *Maas*/*Schmitz*/*Wedde*, Datenschutz 2014 – Probleme und Lösungsmöglichkeiten, 2014, u.a. S. 56ff., 93ff.

100 BSI, BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise, bsi.bund.de/gshb

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder[101] Unterstützung.[102]

Betriebsräten ist dringend anzuraten, in Verhandlungen mit dem Arbeitgeber auf das Instrument des Datenschutzes durch Technik zu pochen. Einmal installiert, kann es Entlastung für die Datenschutzpflichten des Betriebsrats bringen. Der Weg dahin aber führt über externen Sachverstand, der dem Arbeitgeber gegenüber geltend gemacht werden sollte und zwar nicht nur einmalig, sondern fortlaufend, da auch der Datenschutz durch Technik ständig an die IT-Entwicklung angepasst werden muss.

Für die Einschaltung von Sachverständigen durch den Betriebsrat hat sich durch die DSGVO nichts Grundsätzliches geändert. Der Betriebsrat kann weiterhin gemäß § 80 Abs. 3 BetrVG Sachverständige hinzuziehen, soweit dies zur ordnungsgemäßen Erfüllung seiner Aufgaben erforderlich ist und eine entsprechende Vereinbarung mit dem Arbeitgeber vorliegt. Angesichts der Komplexität der IT-bezogenen Fragestellungen ist beim 71. Deutschen Juristentag 2016 vorgeschlagen worden, das Erfordernis des Arbeitgebereinverständnisses entfallen zu lassen und nur noch auf die Erforderlichkeit für die Betriebsratsaufgaben abzustellen.[103] Bislang hat der deutsche Gesetzgeber daraus keine Konsequenzen gezogen. Ggfs. könnte aber im IT-Kontext § 80 Abs. 3 BetrVG teleologisch reduziert werden. Jedenfalls wäre an eine nachträgliche gerichtliche Ersetzung zu denken.[104]

Bei der Beurteilung der Erforderlichkeit verfolgte das BAG bislang eher eine restriktive Linie und verlangt, dass der Betriebsrat versuchen muss, die erforderliche Information zunächst vom Arbeitgeber, von sachkundigen Mitarbeitern der EDV-Abteilung oder durch eigene Recherchen zu erlangen. Das sind

---

101 Das Standard-Datenschutzmodell – eine Methode zur Datenschutzberatung und -prüfung auf Basis einheitlicher Gewährleistungsziele. Empfohlen von der 90. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 30.9./1.10.2015 in Darmstadt, mittlerweile in Version 1.1. – Erprobungsfassung, von der 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 25./26. April 2018 in Düsseldorf einstimmig beschlossen.

102 Darauf verweist auch IGM, Handlungshilfe für Betriebsräte und Vertrauensleute Nr. 19, Datenschutz-Grundverordnung, 4/2018, S. 45.

103 *Krause*, Digitalisierung der Arbeitswelt, Gutachten B zum 71. Deutschen Juristentag, 2016, S. 98, bezieht diesen Vorschlag nicht nur auf die in der DSGVO angesprochenen Verarbeitungsvorgänge, sondern auf die Digitalisierung im Arbeitsleben insgesamt.

104 Vgl. DKKW, § 80 Rn 155.

allerdings bei hochkomplexer Datenverarbeitung überzogene Anforderungen.[105] Solange der deutsche Gesetzgeber zu dieser Frage nicht handelt, ist Betriebsräten zu empfehlen, besonders in DV-Rahmenbetriebsvereinbarungen die nötige Beratung gleich mit vorzusehen, schon um seine Überwachungspflicht gemäß § 80 BetrVG erfüllen zu können.

V. Konzerndatenverarbeitung

Nach dem BDSG a.F. gab es kein Konzernprivileg für die Verarbeitung von Beschäftigtendaten, d.h. der Datenaustausch zwischen konzernangehörigen Unternehmen wurde behandelt wie der Datenaustausch zwischen Unternehmen, die voneinander unabhängig sind, also nach den Regeln der Auftragsdatenverarbeitung, da die Konzernunternehmen datenschutzrechtlich als Dritte galten.

Auch das neue Datenschutzrecht hat nicht ausdrücklich ein Konzernprivileg eingeführt, obwohl das im Gesetzgebungsprozess diskutiert worden war. Datenflüsse zwischen konzernverbundenen Unternehmen benötigen also eine eigene Rechtfertigung, die der DSGVO entsprechen muss. Art. 4 Abs. 19 DSGVO definiert den Konzern nur. Dagegen hält Erwägungsgrund 48 fest, dass die zentrale Verarbeitung von Beschäftigtendaten ein berechtigtes Interesse für eine Verarbeitung auf Konzernebene für interne Verwaltungszwecke darstellen kann. Darin ist kein „verstecktes Konzernprivileg" zu sehen. Ein Erwägungsgrund hat schon keine Rechtswirkung. Die Formulierung ist nur als Hinweis zu verstehen, dass bei der Interessenabwägung zwischen Datenverwender und geschützter Person auch aus internen Verwaltungsgründen ein Unternehmensinteresse an einer konzernweiten Datenverarbeitung zu berücksichtigen sein kann. Hätte ein Konzernprivileg eingeführt werden sollen, wäre das ohne weiteres in Art. 88 Abs. 2 DSGVO möglich und Erwägungsgrund 48 gar nicht nötig gewesen.

Auch wenn also die DSGVO kein datenschutzrechtliches Konzernprivileg enthält und für konzerninterne Übermittlung von Beschäftigtendaten eine Befugnis i.S.v. Art. 6 DSGVO vorliegen muss,[106] ermöglicht Art. 47 DSGVO die Datenübermittlung im Konzern auf der Basis von Binding Corporate Rules. Die sind

---

105 *Däubler*, Gläserne Belegschaften, 2017, 7. Aufl., § 13 Rn. 643ff.

106 So auch *Maschmann*, in: Kühling/Buchner, DSGVO, 2018, 2. Aufl., Art. 88 Rn. 53 m.w.N. in Anm. 123.

allerdings an eine Genehmigung der Aufsichtsbehörde gebunden und dann eine Befugnis i.S.v. Art. 6 DSGVO.

Das gilt auch für Konzernbetriebsvereinbarungen, die den Austausch von Beschäftigtendaten im Konzern regeln können,[107] aber als „spezifischere" nationale Regelungen i.S.v. Art. 88 Abs. 1 DSGVO den o.a. Voraussetzungen aus Art. 88 Abs. 2 DSGVO und den allgemeinen Regeln[108] entsprechen müssen. Da jedenfalls Abweichungen vom Standard der DSGVO nach unten unzulässig sind,[109] könnte ein generelles Konzernprivileg durch nationales Recht und daher auch durch Betriebsvereinbarungen nicht eingeführt werden.[110] Allerdings zeigt Erwägungsgrund 48, dass auch ein generelles Verbot einer Übermittlung von Beschäftigtendaten i.d.R. nicht wirksam sein wird, jedenfalls die im Erwägungsgrund 48 vorgesehene Interessenabwägung stattfinden muss.

Dennoch bleibt abzuwarten, wie die Aufsichtsbehörden und Gerichte mit der Möglichkeit eines privilegierten Datentransfers im Konzern umgehen werden. Erwägungsgrund 48 wäre nicht der erste Fall, in dem die Gerichte sog. Soft Law eine quasi-Rechtswirkung zumessen.

---

107 *Wybitul*, ZD 2016, 203, 208.

108 Vgl. oben Kapitel D.

109 U.a. *Maschmann*, in: Kühling/Buchner, DSGVO, 2018, 2. Aufl., Art. 88 Rn. 54; *Pauly*, in: Paal/Pauly, DSGVO, 2017, Art. 88 Rn. 12.

110 *Maschmann*, a.a.O.

F. Umgang mit alten Betriebsvereinbarungen

I. Grundsätzliche Überlegungen

Das Archiv der Hans-Böckler-Stiftung weist für das Jahr 2015 einen Bestand von 2.472 Betriebsvereinbarungen zu den Themen „Technologie und IT" aus.[111] Zwar ist daraus nicht zu ersehen, wie viele davon Beschäftigtendatenschutz betreffen. Wenn man aber berücksichtigt, dass auch in Betriebsvereinbarungen, die anderen Themenkomplexen zugeordnet werden (z.B. Personalpolitik mit 2.042, Arbeitsorganisation mit 1.670 oder Arbeitszeit mit 3.946), zahlreiche Regelungen zum Beschäftigtendatenschutz enthalten sein können, ist der Bestand an Betriebsvereinbarungen, die nun an der DSGVO zu messen sind, erheblich. Verstoßen Betriebsvereinbarungen gegen die DSGVO, kann das dazu führen, dass sie unwirksam bzw. unanwendbar sind, wenn der verbleibende Teil ohne die unzulässigen Bestimmungen keine sinnvolle, in sich geschlossene Regelung mehr ergibt.[112]

Weder die DSGVO noch das BDSG 2018 enthalten Ausnahme- oder Übergangsregelungen für bestehende Kollektivvereinbarungen oder Vorschriften, die Altverhältnisse regeln. Allerdings befasst sich Erwägungsgrund 171 mit der Thematik und stellt klar, dass bei Verarbeitungen, die auf einer Einwilligung gemäß der EU-Datenschutz-Richtlinie 95/46/EG beruhen, die Einwilligung nicht erneut eingeholt werden muss, wenn sie den Erfordernissen der DSGVO entspricht. Da die Fortgeltung der Wirkung der Einwilligung in der DSGVO angesprochen wird, kann im Umkehrschluss angenommen werden, dass Betriebsvereinbarungen, die nicht der DSGVO entsprechen, auch nicht fortgelten.

Verstoßen Betriebsvereinbarungen gegen höherrangiges Recht, wie die DSGVO, wird z.T. die Nichtigkeit der Betriebsvereinbarung aus § 134 BGB angenommen.[113] Z.T. wird zwar von deren Fortgeltung ausgegangen, kann aber nur dann

---

111 HBS – Archiv Betriebliche Vereinbarungen 2015.
112 BAG, Beschl. v. 9.7.2013 – 1 ABR 19/12, NZA 2014, 99.
113 *Franck*, ZD 2017, 509, 511.

weiter als Rechtfertigung für die Verarbeitung von Beschäftigtendaten herangezogen werden, wenn sie der DSGVO entspricht.[114]

In beiden Fällen stellt sich die Frage, inwieweit alte Betriebsvereinbarungen an Art. 88 Abs. 2 DSGVO und die allgemeinen Regeln in Art. 5ff. DSGVO angepasst werden müssen, d.h. ob diese Grundsätze ausdrücklich in alle alten Betriebsvereinbarungen aufgenommen werden müssen oder ob es reicht, dass die alten Betriebsvereinbarungen Art. 88 Abs. 2 DSGVO und die Grundsätze aus Art. 5ff. DSGVO nicht verletzten. Diese Frage kann mit letzter Verbindlichkeit nur der Europäische Gerichtshof beantworten.[115] Für Letzteres spricht § 26 Abs. 4 S. 2 BDSG n.F., wonach § 88 Abs. 2 DSGVO nur „zu beachten" ist. Art. 88 Abs. 2 DSGVO allerdings als die verbindliche europäische Norm, an der § 26 BDSG zu messen ist, formuliert, dass die Betriebsvereinbarung dessen Inhalte „umfassen" muss. Das spricht für eine ausdrückliche Regelung. Jedoch kann nach Sinn und Zweck der Regelung nicht gemeint sein, dass schematisch der Inhalt von Art. 88 Abs. 2 DSGVO in jeder Betriebsvereinbarung wiedergegeben werden muss. Vielmehr ist das Erfordernis kontextabhängig,[116] d.h. es müssen in der Betriebsvereinbarung nur die Aspekte aus Art. 88 Abs. 2 DSGVO aufgegriffen werden, um die es in der konkreten Betriebsvereinbarung auch tatsächlich geht. So muss etwa in einer Betriebsvereinbarung zu den besonderen Anforderungen bei der Übermittlung personenbezogener Daten im Konzern nur dann etwas geregelt werden, wenn es um Konzerndatenverarbeitung geht. Ebenso werden sich in vielen Betriebsvereinbarungen bereits Regelungen finden, die Art. 88 Abs. 2 DSGVO erfüllen, so z.B. wenn bei der Videoüberwachung im Betrieb Sanitäreinrichtungen und Umkleideräume von der Überwachung ausgeschlossen werden. Dabei handelt es sich dann um eine „Maßnahme zur Wahrung der menschlichen Würde",[117] ohne dass diese Formulierung in der Betriebsvereinbarung ausdrücklich aufgegriffen werden muss.

Auch die in Art. 88 Abs. 2 DSGVO genannten „berechtigten Interessen und der Grundrechte der betroffenen Personen" dürften wegen § 75 Abs. 1 und 2 sowie § 80 Abs. 1 Nr. 1 BetrVG i.d.R. in bestehenden Betriebsvereinbarungen bereits Beachtung gefunden haben. Auch wenn etliche der Anforderungen in Art. 88 Abs. 2 DSGVO schon in alten Betriebsvereinbarungen erfüllt sein mögen, dürfte

---

114 *Maschmann*, DB 2016, 2480, 2485.

115 *Kiesche/Wilke/Berger*, AiB 2018, 15, 16.

116 So auch *Dzida/Grau*, DB 2018, 189, 191; *Wybitul*, NZA 2017, 413, 419; *Wurzberger*, ZD 2017, 258, 259.

117 *Dzida/Grau*, a.a.O.

jedenfalls Anpassungsbedarf bei den viel dezidierter als nach altem Datenschutzrecht in der DSGVO geforderten Transparenzanforderungen bestehen. Dass die Transparenz der Verarbeitung von Beschäftigtendaten derzeit im Fokus der datenschutzrechtlichen Diskussion steht,[118] zeigt auch die jüngste Datenschutz-Rechtsprechung des EGMR.[119]

Aber auch wenn in vielen Alt-Betriebsvereinbarungen zur Verarbeitung von Beschäftigtendaten schon etliche der Anforderungen aus Art. 88 Abs. 2 DSGVO erfüllt sein werden, kann nicht pauschal davon ausgegangen werden, dass nichts zu tun ist, sondern müssen die alten Betriebsvereinbarungen daraufhin überprüft und ggfs. angepasst werden. Häufig wird sich nur eine knappe Dokumentation finden und werden die Datenverarbeitungsvorgänge nur abstrakt umschrieben sein. Das reicht nach neuem Recht nicht mehr.

Die Gewerkschaftssicht darauf ist sogar z.T. besonders streng: so wird gefordert, dass wegen der Pflicht des Betriebsrats gemäß § 80 Abs. 1 Nr. 1 BetrVG die Einhaltung der DSGVO im Betrieb zu überwachen, „alle Betriebsvereinbarungen, die die Verarbeitung personenbezogener Beschäftigtendaten regeln, durchgesehen und dahingehend geprüft werden müssen, ob sie den neuen Anforderungen entsprechen".[120]

Dafür kommen mehrere Wege in Betracht. Bei denen ist zu beachten, dass das Gesetz in Art. 88 Abs. 2 DSGVO nur „angemessene" Regelungen verlangt, so dass es auf die Situation ankommt, mit welchem Umfang und in welcher Detailtiefe die Voraussetzungen der DSGVO in den Betriebsvereinbarungen erscheinen müssen.[121]

II. Einzelprüfung

Zunächst könnte man fordern, jede einzelne Betriebsvereinbarung zur Beschäftigtendatenverarbeitung auf ihre Kompatibilität mit der DSGVO zu überprüfen. Das drängt sich vor allem dann auf, wenn gefordert wird, dass die allgemeinen Datenschutz-Grundsätze aus Art. 5 Abs. 1 DSGVO ausdrücklich in Bezug zu

---

118 So auch *Dzida/Grau*, a.a.O.

119 Dazu schon oben D.II.4.

120 IGM, Handlungshilfe für Betriebsräte und Vertrauensleute Nr. 19, Datenschutzgrundverordnung, 4/2018, S. 36.

121 So auch *Klösel/Mahnhold*, NZA 2017, 1428, 1432.

nehmen sind.[122] Dann nämlich könnten alte Betriebsvereinbarungen im Grunde nie der DSGVO entsprechen.

Bei der großen Zahl an Betriebsvereinbarungen zu dieser Materie ist das nicht nur ein erheblicher Aufwand, dessen Verhältnismäßigkeit fraglich ist, sondern auch zu bedenken, dass es nicht nur „reine" Datenverarbeitungsbetriebsvereinbarungen gibt, sondern diese Materie auch bei anderen Aufhängern einer Betriebsvereinbarung mitgeregelt sein kann.

Daher bietet sich gerade für die allgemeinen Grundsätze eine Lösung an, die diese Grundsätze pauschal für alle betroffenen Betriebsvereinbarungen regelt.

III. FAQ

Es kann auch den Anforderungen der Transparenz genügen, wenn die Betriebsparteien alte Betriebsvereinbarungen um eine Anlage sowie durch Mitarbeiterinformation im Intranet, etwa in Gestalt von Frequently asked questions (FAQ), zu häufig gestellten Fragen ergänzen.[123]

Hierbei stellt sich die Frage, ob eine entsprechende einseitige Ergänzung des Arbeitgebers reicht oder die Anlage zwischen den Betriebsparteien vereinbart werden muss. Da primär der Arbeitgeber den Beschäftigten die datenschutzrechtliche Information und Aufklärung schuldet, kann er die FAQ im Prinzip alleine erstellen, denn er haftet auch, wenn die Betroffenenrechte nicht verordnungskonform gewährt werden. Allerdings ist es auch hier empfehlenswert, dass sich die Betriebsparteien auf ein gemeinsames Papier einigen.

Um die Anforderungen von Art. 5 DSGVO zu erfüllen, dürfte dieser Weg allerdings ohnehin nicht ausreichen. Er ist eher ein zusätzliches – sinnvolles und empfehlenswertes – Hilfsmittel, um die Datenschutzregeln für die Beschäftigten „griffiger" zu machen. Das ist auch deshalb wichtig, um die Beschäftigten nicht allzu lange im Unklaren darüber zu lassen, wie die Datenschutzregeln in Betriebsvereinbarungen nach der neuen Rechtslage zu verstehen sind.[124]

---

122 So *Grimm*, ArbRB 2018, 78.
123 *Wibytul/Sörup/Pötters*, ZD 2015, 559, 561.
124 Rundbrief Arbeitnehmeranwälte, 39/2018, S. 6.

IV. Rahmenbetriebsvereinbarungen

Rechtssicherer ist aber eine grundlegende Rahmenbetriebsvereinbarung. Dadurch könnten bestehende Betriebsvereinbarungen durch datenschutzrechtliche Klarstellungen und Ergänzungen „gerettet" werden.[125] Rahmenbetriebsvereinbarungen sind, was die allgemeinen Datenschutz-Grundsätze angeht, aber auch für neue Betriebsvereinbarungen sinnvoll[126] und sollten vorsehen, dass die Datenschutz-Grundsätze des Art. 5 DSGVO und anderer zwingender Regeln der DSGVO auch für zum Zeitpunkt des Wirksamwerdens der DSGVO schon bestehende Betriebsvereinbarungen gelten sollen und eventuell entgegenstehende Regelungen in den alten Betriebsvereinbarungen ersetzen.[127] So lassen sich auch die Folgen von salvatorischen Klauseln, die oft in Betriebsvereinbarungen zu finden sind, abfedern. Keinesfalls können Rahmenbetriebsvereinbarungen aber die oben dargestellten Pflichtinhalte, die jede einzelne Betriebsvereinbarung enthalten muss, durch pauschale Regelungen ersetzen, da diese Inhalte je nach Betriebsvereinbarung unterschiedlich sind. Dazu gehören jedenfalls der Verarbeitungszweck und alle an ihn gebundenen Faktoren, wie die zulässige Speicherdauer oder die zugriffsberechtigten Personen. Dagegen dürfen Datenschutzregeln, die unabhängig vom jeweiligen Verarbeitungszweck immer gleich sind, wie etwa die Betroffenenrechte, pauschal in einer Rahmenbetriebsvereinbarung geregelt werden, die damit eine übersichtliche Zusammenfassung der Regelungen sein kann, die für alle Anwendungen gelten. Das fördert sogar die Transparenz, weil die Aufnahme aller unter D. darstellten Punkte in jede einzelne Betriebsvereinbarung die Übersichtlichkeit und Klarheit der Regelung beeinträchtigen würde. Allerdings enthebt dieser Ansatz Betriebsrat und Arbeitgeber nicht der Mühe, alte Betriebsvereinbarungen auf die Kompatibilität mit den Pflichtinhalten zu überprüfen.

Die möglichen Regelungsgegenstände für Rahmenbetriebsvereinbarungen sind nicht abschließend zu bestimmen und entsprechen dem unter E.II. Dargestellten.

Rahmenbetriebsvereinbarungen können, wo es sinnvoll erscheint, z.B. wenn sie sehr umfangreich sind, um eine FAQ-Liste[128] ergänzt werden, in der die Beschäftigten leichter Zugriff auf die wichtigsten Datenschutzregeln erhalten.

---

125 So u.a. *Wybitul*, NZA 2017, 1488, 1490.
126 So schon oben E.II.
127 A.a.O.
128 Dazu schon oben III.

An sich sind Rahmenbetriebsvereinbarungen für den Beschäftigtendatenschutz nichts Neues. Schon seit Jahrzehnten werden in den Betrieben auf freiwilliger Basis EDV-Rahmenbetriebsvereinbarungen abgeschlossen,[129] die allgemeine Aspekte des Beschäftigtendatenschutzes, eben einen Rahmen dafür, regeln. Dabei bleibt es auch unter der DSGVO. Für die Regelung konkreter Überwachungssituationen sind sie aber nicht geeignet.[130]

V. Steckbriefe

In der arbeitsrechtlichen Praxis wurde auch bereits erfolgreich mit sog. Steckbriefen gearbeitet. Der Begriff ist nicht eindeutig. Zunächst ist der Datenschutz-Steckbrief ein Begriff der Kanzlei- und Steuerberater-Software DATEV,[131] an dem Verantwortliche ihre Datenverarbeitung ausrichten können, um sicherzugehen, mit der DSGVO konform zu sein. Im kollektiven Arbeitsrecht beschreibt „Steckbrief" einerseits Grundlagenvereinbarungen zwischen Arbeitgeber und (Gesamt- oder Konzern-)Betriebsrat über die Konfiguration von IT-Systemen und den damit verbundenen Datenschutz, andererseits die entsprechenden Anlagen zu (Konzern-)Betriebsvereinbarungen über IT-Systeme und Datenschutz. In beiden Fällen handelt es sich um ausgehandelte Vereinbarungen zwischen Arbeitgeber und Betriebsrat zu den DSGVO-konformen Details der Datenverarbeitungssysteme. Da es um die systemische Beschreibung geht, sind Steckbriefe keine Alternative zu Rahmenbetriebsvereinbarungen, sondern können und sollen diese sinnvoll dergestalt ergänzen, dass Rahmenbetriebsvereinbarungen systemübergreifende Regelungen enthalten und für das konkrete Datenverarbeitungssystem die Spezifizierung in einem Steckbrief erfolgt, wobei die Gesamtkonstruktion die Anforderungen der DSGVO erfüllen muss.

Für die Frage, welche dieser Varianten nun tatsächlich die Anforderungen der generalklauselartig formulierten DSGVO am besten erfüllt, besteht Spielraum und ist noch nicht sicher, wie sich die Aufsichtsbehörden und Gerichte positionieren werden. Daher ist Betriebsräten zu empfehlen, eine pragmatische, verhältnismäßige Lösung zu wählen, die das ernsthafte Bemühen erkennen lässt, den Anforderungen der DSGVO gerecht zu werden und ggfs. später bei der Neuverhandlung von Betriebsvereinbarungen nachzujustieren. Rahmenbetriebsvereinbarungen mit Steckbriefen weisen daher für alte Betriebsvereinba-

---

129 *Schapper*, AuR 1988, 97.
130 *Däubler*, Gläserne Belegschaften, 2017, 7. Aufl., Rn. 817.
131 www.datev.de/datenschutz-steckbrief

rungen in die richtige Richtung. Strenger wird man – im Prinzip – bei neuen Betriebsvereinbarungen sein müssen, die in Kenntnis der DSGVO abgeschlossen werden und bei denen daher zumutbar ist, die Kern-Anforderungen der DSGVO in jeder einzelnen Betriebsvereinbarung zu erfüllen. Je nach Regelungsmaterie lassen sich aber auch dafür Muster entwickeln, sodass nicht jeder Betriebsrat das Rad neu erfinden muss. Darüber hinaus können auch bei neuen Betriebsvereinbarungen Datenschutzregeln, die für alle Verarbeitungszusammenhänge gleichermaßen gelten, wie z.B. die Informations- und Betroffenenrechte, in einer Rahmenbetriebsvereinbarung geregelt werden.[132]

132 S.o. E.II.

G. Eigene Datenverarbeitung des Betriebsrats

I. Betriebsrat als verarbeitende Stelle

Der Betriebsrat nimmt datenschutzrechtlich zwei Positionen ein[133]: Einerseits überwacht er nach § 80 Abs. 1 Nr. 1 BetrVG die Einhaltung der zugunsten der Beschäftigten geltenden Datenschutzgesetze im Betrieb. Andererseits arbeitet er selbst in erheblichem Umfang mit Beschäftigtendaten.

Betriebsratstätigkeit ohne die (umfangreiche) Verarbeitung personenbezogener Beschäftigtendaten ist nicht denkbar. Für fast alle Aufgaben benötigt der Betriebsrat diese Daten. Das beginnt mit Dokumenten zu Personalvorgängen, wie Einstellungen, Versetzungen, Kündigungen oder Leistungsbeurteilungen und seinen Stellungnahmen dazu – Daten, die Betriebsräte i.d.R. in eigenen automatisierten Dateien ablegen, aber auch nicht automatisierte Dateien fallen gemäß Art. 2 Abs. 1 DSGVO unter die Verordnung, so dass die DSGVO i.V.m. § 26 BDSG für jede Art von Umgang mit Beschäftigtendaten beim Betriebsrat Anwendung findet.

Auch bei der Arbeitszeitkontrolle, um ein weiteres Beispiel zu nennen, will der Betriebsrat etwa Auf- und Abbau von Gleitzeitkonten oder die Rechtmäßigkeit der Anordnung von Mehrarbeit in Bezug auf bestimmte Personen überprüfen können, was nur mit der Erfassung, Speicherung und Auswertung der entsprechenden Beschäftigtendaten möglich ist.

Ähnliches gilt bei Altersteilzeitprogrammen, bei denen Listen der altersteilzeitgeeigneten Personen sowie deren Daten im Detail erstellt werden müssen, um überhaupt mit den Betroffenen und der Personalabteilung reden zu können. Allein die Liste der personenbezogenen Beschäftigtendaten, die der Betriebsrat im Zusammenhang mit personellen Einzelmaßnahmen nach § 99 BetrVG benötigt und verarbeitet, ließe sich endlos fortsetzen, aber auch etwa das BEM ist ein Beispiel.

§ 26 Abs. 1 S. 1 BDSG n.F. trägt dem Rechnung. Nach dieser Vorschrift hat der Betriebsrat ein „Recht auf personenbezogene Daten“, die für die Ausübung

---

133 So auch Rundbrief Arbeitnehmeranwälte Nr. 39, 5/2018, S. 17.

seiner Aufgaben nötig sind. Die ergeben sich u.a. aus § 87 Abs. 1 Nr. 6 BetrVG in Bezug auf Beschäftigtendaten zur Verhaltens- und Leistungskontrolle, aus § 87 Abs. 1 Nr. 10 BetrVG für Entgeltdaten, aus § 102 BetrVG für Kündigungsdaten, aus §§ 112f. BetrVG für Sozialplandaten oder beim betrieblichen Eingliederungsmanagement für sensible Daten i.S.v. Art. 9 DSGVO. Aus diesen Aufgaben wird das Recht des Betriebsrats abgeleitet, sich für die Erfüllung seiner betriebsverfassungsrechtlichen Aufgaben im erforderlichen Umfang eigene Dateien aufzubauen.[134]

Obwohl der Betriebsrat neben dem Arbeitgeber also selbst in erheblichem Umfang personenbezogene Beschäftigtendaten verarbeitet und daher die DSGVO gemäß Art. 2 auf Beschäftigtendaten auf Betriebsrats-PCs anwendbar ist, ist nach wie vor umstritten, ob er eine eigene verantwortliche Stelle ist.[135] Nach h.M. und BAG soll das nicht der Fall sein.[136] Für die Beibehaltung der bisherigen Sicht[137] spricht u.a., dass Art. 4 Nr. 7 DSGVO nicht ausreichend vom Verantwortlichen-Begriff im alten BDSG (§ 3 Abs. 7 BDSG a.F.) abweicht.[138]

Weder die DSGVO noch das BDSG n.F. beantworten die Frage, ob es sich beim Betriebsrat um einen eigenständigen Verantwortlichen gemäß Art. 4 Nr. 7 DSGVO handelt. Dass sich der europäische Gesetzgeber bei einer europaweiten Datenschutzregelung über Besonderheiten der deutschen Betriebsverfassung keine Gedanken gemacht hat, ist nachvollziehbar. Der deutsche Gesetzgeber jedoch hätte in § 26 BDSG n.F. die Frage aufgreifen können. Immerhin definiert Art. 4 Nr. 7 DSGVO den „Verantwortlichen" – nicht mehr die „verantwortliche Stelle", wie in § 3 Abs. 7 BDSG – aber als ein Subjekt, das „allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von Personen entscheidet". Wenn man sich vor dem Hintergrund dieser Formulierung die Rechtsprechung des BAG zur Eigenständigkeit des Betriebsrats bei der Bestimmung von Datenverarbeitung und Datenschutz vergegenwärtigt, scheint die DSGVO-Regelung die Konstellation zwischen Arbeitgeber und Betriebsrat zu

---

134 Simitis-*Seifert*, § 32 Rn. 169ff.; *Klebe*, in: DKKW, § 94 Rn. 53.

135 Das ist z.T. auch schon nach der alten Rechtslage einschränkend auf die Fälle der aufgabenbezogenen Verarbeitungen verstanden worden: *Kort*, NZA 2010, 1267, 1268.

136 BAG v. 18.7.2012 – 7 ABR 23/11, NZA 2012, 764.

137 *Hartung*, in: Kühling/Buchner, DSGVO 2018, 2. Aufl., § 4 Abs. 7 Rn. 11; *Gola*, ZBVR online 7-8/2017, 31, 32. Im Übrigen äußert sich die inzwischen umfangreiche Kommentarliteratur zur DSGVO nur teilweise zu dieser Fragestellung.

138 So Rundbrief Arbeitnehmeranwälte Nr. 39, 5/2018, S. 17.

treffen.[139] So hat das BAG etwa entschieden, dass der Betriebsrat die für seine Datenverarbeitung benötigte Technik soweit erforderlich selbständig bestimmen darf.[140] Auch über die Frage, wie der Zugang zum Internet organisiert wird – nur über einen zentralen PC im Betriebsratsbüro oder am Arbeitsplatz des einzelnen Betriebsratsmitglieds – befindet der Betriebsrat allein.[141] Datenschutzrechtlich besonders problematisch ist die BAG-Entscheidung, dass jedes Betriebsratsmitglied nach § 34 Abs. 3 BetrVG das Recht hat, alle Dateien und E-Mails des Betriebsrats auf elektronischem Wege zu lesen.[142]

Aus dieser Rechtsprechungslinie lässt sich aber keine eigenständige datenschutzrechtliche Verantwortung des Betriebsrats ableiten. Zunächst hat sich am materiellen Datenschutzrecht kaum etwas geändert, so dass zunächst auch die bisherige Beurteilung, dass der Betriebsrat nicht selbst verantwortliche Stelle ist, beibehalten werden kann. Vor allem aber handelt der Betriebsrat nur im Rahmen der ihm zugewiesenen Aufgaben. Zwecke für eine Datenverarbeitung des Betriebsrats können sich nur daraus ergeben.[143] Zusätzliche eigene Verarbeitungszwecke kann der Betriebsrat nicht definieren. Auch über die Sachmittel für die Datenverarbeitung kann der Betriebsrat nicht frei entscheiden.[144] Diese Faktoren sprechen dagegen, dass der Betriebsrat eine eigene verantwortliche Stelle ist. Diese Sicht wird auch dadurch erhärtet, dass der europäische Gesetzgeber bei der verantwortlichen Stelle einen solventen, eigenständigen und unabhängigen Schuldner vor Augen hatte, dem strenge Haftung auferlegt und hohe Bußgelder abverlangt werden können. Die Haftungsregeln laufen aber beim nicht rechtsfähigen Betriebsrat ins Leere und eine persönliche Haftung einzelner Betriebsratsmitglieder[145] würde die Unabhängigkeit des Betriebsrats unterminieren.

Es bleibt also auch unter der DSGVO dabei, dass der Betriebsrat keine eigene datenverantwortliche Stelle ist, sondern Teil der Arbeitgeberdatenverarbeitung, der allein nach außen als Verantwortlicher auftritt.

Damit soll aber nicht der Umstand übergangen werden, dass in der Praxis bei vielen Betriebsräten die Transparenz der Datenverarbeitung verbesserungsbe-

---

139 So auch *Gola*, ZBVRonline 7-8/2017, 31, 32.
140 BAG v. 20.4.2016 – 7 ABR 50/14, juris; kritisch dazu *Middel*, AuR 2018, 411.
141 BAG v. 18.7.2012 – 7 ABR 23/11, RDV 2012, 295.
142 BAG v. 12.8.2009 – 7 ABR 15/08, juris.
143 *Middel*, AuR 2018, 411, 417.
144 Vgl. z.B. HessLAG 25.7.2016 – 16 TaBV 219/1, FA 2017, 17.
145 Vom BGH bei kartellrechtlichen Verstößen allerdings bejaht: BGH, Urt. v. 1.6.1989 – ZR 81/87, NJW-RR 1989, 1312.

dürftig ist.[146] Häufig werden eigene Tabellen und Sammlungen erstellt und entsteht so ggfs. eine zweite Personalakte – nicht nur beim Betriebsrat als Organ, sondern auch bei einzelnen Betriebsratsmitgliedern auf deren PCs –, was nach § 83 Abs. 2 S. 2 BetrVG gar nicht zulässig ist, und nicht immer kann sicher angegeben werden, wer was wo mit welchen Zugriffsbefugnissen wie lange speichert, weiterleitet und auswertet – von der Datensicherheit ganz zu schweigen. Man denke etwa an Beschäftigtendaten auf privater Hardware von Betriebsratsmitgliedern. Auch das E-Mail-Postfach von Betriebsratsmitgliedern kann zum eigenen Archiv werden, obwohl eine derartige Archivierung vom BetrVG nicht vorgesehen ist. Nach § 34 Abs. 3 BetrVG haben die Betriebsratsmitglieder das Recht, Unterlagen des Betriebsrats und seiner Ausschüsse einzusehen. Die IT-Technik macht es aber möglich, dass dieses Prinzip leicht ausgehebelt werden kann.

Diesen oft unbewussten Datenschutzverstößen muss natürlich begegnet werden, wenn sie auch nichts damit zu tun haben, ob der Betriebsrat eine eigene verantwortliche Stelle ist. Daher wird auch aus gewerkschaftlicher Sicht vertreten, dass der Betriebsrat „für die von ihm durchgeführte Datenverarbeitung verantwortlich ist", obwohl er nur Teil der verantwortlichen Stellen im Sinne der DSGVO ist.[147]

Hier ist neben – zugegebenermaßen nicht immer effizienter – Selbstkontrolle an einen externen Datenschutzbeauftragten für den Betriebsrat zu denken.[148] Der kann angesichts der Komplexität der Datenverarbeitung und Einhaltung der Datenschutz- sowie Datensicherheitsvorschriften gemäß § 40 Abs. 2 und § 80 Abs. 3 BetrVG als erforderliches Mittel für die Sicherung des Beschäftigtendatenschutzes bei der Betriebsratsarbeit eingesetzt werden, könnte aber auch unabhängig von konkreter Erforderlichkeit im Einzelfall in einer freiwilligen Betriebsvereinbarung vorgesehen werden.

---

146 So auch Rundbrief Arbeitnehmeranwälte Nr. 39, 5/2018, S. 16.

147 IGM, Handlungshilfe für Betriebsräte und Vertrauensleute Nr. 19, Datenschutz-Grundverordnung, 4/2018, S. 62.

148 Dazu auch unten G.IV.3.

II. Zulässigkeit von Datenverarbeitung durch den Betriebsrat

Auch wenn der Betriebsrat nur Teil der an den Arbeitgeber anknüpfenden verantwortlichen Stelle ist, muss auch die Datenverarbeitung durch den Betriebsrat zulässig sein, also Art. 5 DSGVO i.V.m. § 26 BDSG entsprechen.[149] Zunächst muss der Zweck der Datenverarbeitung beim Betriebsrat definiert und festgehalten (s.u. III.) werden und sich aus einer konkreten Aufgabe des BetrVG ergeben. Darüber hinaus dürfen nur Daten verarbeitet werden, die für den zuvor definierten Zweck erforderlich sind. Zugang zu diesen Daten dürfen nur Berechtigte haben, die ihrerseits klar benannt sein müssen. Schließlich müssen Daten nach Erreichen des Zwecks gelöscht werden. Ggfs. sind hierfür Löschroutinen vorzusehen (vgl. auch zum technischen Datenschutz E.IV.). Es reicht allerdings rechtlich nicht, dass der Betriebsrat „im Idealfall" die gleichen Datenschutzanforderungen an sich selbst stellt, wie an den Arbeitgeber.[150] Bei den Datenschutzanforderungen handelt es sich um eine Rechtspflicht aus der DSGVO, die für alle gleichermaßen gilt, die personenbezogene Daten verarbeiten.

Daraus folgt auch, dass der Betriebsrat den Auskunftsansprüchen der Betroffenen aus der DSGVO unterliegt,[151] denn der Arbeitgeber ist zu umfassenden Auskünften über die Datenverarbeitung des Betriebsrats gar nicht in der Lage. Die Ausgestaltung dieser Auskunftsansprüche müsste in einer Betriebsvereinbarung geregelt werden.

III. Verzeichnis der Verarbeitungstätigkeiten, Art. 30 DSGVO

Obwohl der Betriebsrat nach wie vor nicht als eigene verantwortlichen Stelle anzusehen ist, stellt sich die Frage, ob und wie der Betriebsrat über seine eigenen Verarbeitungstätigkeiten von personenbezogenen Daten Verzeichnisse i.S.v. Art. 30 DSGVO erstellen muss. Gleich, ob sich die Aufsichtsbehörde an den Betriebsrat selbst wendet oder an den Arbeitgeber – es muss die Frage beantwortet werden können, was der Betriebsrat mit den Beschäftigtendaten macht. Das ist aber nur möglich, wenn eine ausreichende Dokumentation vorliegt,

---

149 Siehe zu den Anforderungen aus Art. 5 DSGVO im Einzelnen oben D.II.3.

150 So Rundbrief Arbeitnehmeranwälte, 39/2018, S. 18.

151 *Gola*, ZBVR online 7-8/2017, 31, 32.

denn nur derjenige kann die Datenschutzvorgaben einhalten, der die eigenen Verarbeitungsprozesse kennt.[152]

Daher sieht Art. 30 DSGVO eine Verzeichnispflicht für alle Verarbeitungstätigkeiten vor. Diese Pflicht richtet sich zunächst an den Verantwortlichen, aber gemäß Abs. 2 auch an Auftragsverarbeiter und in Art. 30 Abs. 1 S. 2 lit. a DSGVO ist von einem „gemeinsam mit ihm Verantwortlichen" die Rede. Nach Sinn und Zweck der Norm soll also diejenige Stelle das Verzeichnis erstellen, die selbst Daten verarbeitet. Darunter fällt auch der Betriebsrat.

Die DSGVO enthält im Rahmen des Art. 30 schon deshalb nichts Ausdrückliches zum Betriebsrat, weil der überhaupt erst in einem weit fortgeschrittenen Stadium der DSGVO-Entwürfe in die DSGVO aufgenommen wurde – ausdrücklich auch nur in die nicht rechtlich bindenden Erwägungsgründe (EW 155) – und, da eine deutsche Besonderheit, in der DSGVO ein Fremdkörper bleibt. Daher ist die DSGVO insgesamt nicht auf den spät ergänzten Art. 88 angepasst worden.

Ein unüberwindliches Problem ist die Dokumentationspflicht ohnehin nicht. Die Pflichtenliste in Art. 30 Abs. 1 S. 2 DSGVO ist überschaubar. Zwingend aufzunehmen sind nur der Verarbeitungszweck, die Kategorien der betroffenen Personen und Daten sowie die Kategorien von Empfängern. Da der Zweckbindungsgrundsatz die wesentlichste Voraussetzung für rechtmäßige Verarbeitung personenbezogener Daten ist und das beim Betriebsrat bedeutet, dass sich die Datenverarbeitung immer aus Betriebsratsaufgaben ergeben muss – etwa aus § 87 Abs. 1 Nr. 3, § 99, § 102 BetrVG oder aus § 10 EntgTranspG –, dürfte die Formulierung des Verarbeitungszwecks nie Schwierigkeiten machen. Löschungsfristen und technische und organisatorische Maßnahmen i.S.v. Art. 32 DSGVO sollen nur „wenn möglich" aufgenommen werden. Hier regelt allerdings § 70 Abs. 1 BDSG n.F. etwas strenger: Löschungsfristen müssen aufgenommen werden, was für den Persönlichkeitsschutz der Betroffenen sinnvoll ist, wenn auch für den, der die Daten gerne länger nutzen würde, lästig, da man sich vorab Gedanken machen muss, welche Daten wie lange aus sachlichen Gründen aufbewahrt werden müssen. Es ist gerade der Kern jeden Datenschutzes, dass personenbezogene Information nur so lange aufgehoben werden darf, wie sie rechtlich erforderlich ist. Ob sie darüber hinaus auch später noch einmal nützlich sein könnte, ist gerade kein rechtlich relevanter Zweck. Es gibt keine Begründung dafür, warum dabei beim Betriebsrat andere Maßstäbe gelten soll-

152 *Imping*, CR 2017, 378, 381.

ten als beim Arbeitgeber. Bei den technischen und organisatorischen Maßnahmen reicht „eine allgemeine Beschreibung“. Auch das ist leistbar und zwar in jedem Einzelfall.

Dennoch wäre es für Betriebsräte hilfreich, wenn etwa Gewerkschaften ausformulierte Vorlagen an die Hand geben würden, die dann vor Ort angepasst werden können. Derartige Vorlagen – wenn auch nicht spezifisch für den Beschäftigtendatenschutz – finden sich z.T. schon bei den Aufsichtsbehörden.[153]

Zwar schränkt Art. 30 Abs. 5 DSGVO die Pflicht, ein Verzeichnis für die Verarbeitungstätigkeiten zu erstellen, auf Unternehmen oder Einrichtungen mit mindestens 250 Mitarbeitern ein. Die Ausnahmen sind aber umfangreich: sie sollen schon gelten, wenn die Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen bergen – welche Datenverarbeitung von Beschäftigtendaten täte das nicht? –, die Verarbeitung nicht nur gelegentlich erfolgt oder eine Verarbeitung besonders sensibler Daten i.S.v. Art. 9 Abs. 1 DSGVO erfolgt. Da es angesichts der Vielfalt von Verarbeitungssituationen für Beschäftigtendaten unwahrscheinlich ist, dass in einem Unternehmen bzw. beim Betriebsrat nur Beschäftigtendaten verarbeitet werden, die unter keine der Ausnahmetatbestände des Art. 30 Abs. 5 DSGVO fallen, ist zu empfehlen, dass für alle Verarbeitungstätigkeiten Verzeichnisse erstellt werden.

IV. Überwachung der Datenverarbeitung des Betriebsrats

Da der Betriebsrat auch weiterhin nicht selbst verantwortliche Stelle für die Verarbeitung von Beschäftigtendaten ist, sondern insoweit Teil des Arbeitgebers als verantwortliche Stelle für die gesamte Datenverarbeitung im Unternehmen, auch die beim Betriebsrat, stellt sich die Frage, wie in Zukunft mit der Überwachung der Datenverarbeitung des Betriebsrats umzugehen ist.

Das BAG hat schon vor 20 Jahren mit dem Argument der Gegnerfreiheit sowohl die Kontrolle durch den Arbeitgeber wie durch den betrieblichen Datenschutzbeauftragten ausgeschlossen.[154] Es ist fraglich, ob diese Linie aufrechterhalten werden kann.[155]

---

153 Vgl. deren Homepages.

154 BAG, Beschl. v. 11.11.1997 – 1 ABR 21/97, BAGE 87, 64ff.

155 Verneinend: *Kurzböck/Weinbeck*, BB 2018, 1652; *Wybitul*, NZA 2017, 1488, 1490.

1. Kontrolle durch den Arbeitgeber

Mit Datenschutzargumenten soll die Mitbestimmungsbefugnis des Betriebsrats nicht ausgehebelt werden können,[156] etwa dergestalt, dass der Betriebsrat die für die Ausübung seiner Befugnisse erforderlichen personenbezogenen Beschäftigtendaten nicht oder nur eingeschränkt erheben darf. Ebenso wenig darf der Arbeitgeber bisher die Datenverarbeitung des Betriebsrats unter datenschutzrechtlichen Gesichtspunkten kontrollieren. Ist der Arbeitgeber der Gesamtverantwortliche, und damit rechenschaftspflichtig und Haftungsschuldner[157] mit gemäß Art. 82 DSGVO verschärfter zivilrechtlicher Haftung und gemäß Art. 83 DSGVO erheblichen Geldbußen für alle Verarbeitungen personenbezogener Daten in seinem Unternehmen, also auch für die beim Betriebsrat, hat er natürlich ein Interesse sicherzustellen, dass auch beim Betriebsrat der Umgang mit Beschäftigtendaten rechtmäßig erfolgt. Anders kann er kaum sicherstellen und eigene Haftung vermeiden, dass die DSGVO und weitere Datenschutzregeln eingehalten werden. Die bisherige Sicht des BAG, die zur unternehmensinternen Kontrollfreiheit der Betriebsrats-Datenverarbeitung führt, mag umso einfacher einzunehmen gewesen sein als wie bisher Datenschutzverstöße eher milde geahndet wurden[158] und sich also das Haftungsrisiko des Arbeitgebers für Datenschutzverstöße des Betriebsrats in Grenzen hielt.[159]

Allerdings ist zu berücksichtigen, dass der europäische Gesetzgeber bei der spät aufgenommenen Regelung, dass auch weiterhin Betriebsvereinbarungen Datenschutzrecht regeln dürfen, die möglichen Friktionen zwischen Datenschutzrecht und deutschen betriebsverfassungsrechtlichen Garantien für die Unabhängigkeit des Betriebsrats nicht in den Blick genommen hat und deshalb nicht bewusst eine Schlechterstellung des Betriebsrats regeln wollte. Der Arbeitgeber hat daher wie bisher aus betriebsverfassungsrechtlichen Gründen keine umfassenden Kontrollbefugnisse für die Betriebsratsdaten, weil dadurch dessen Rechte unverhältnismäßig eingeschränkt würden. Schon gar nicht ist Datenschutz ein Grund, dem Betriebsrat die personenbezogenen Informationen vorzuenthalten, die er für seine Aufgabenerfüllung braucht.[160] Allerdings reicht es auch nicht, dass der Betriebsrat die Grundsätze des Datenschutzes „in vorbildlicher

156 Dazu auch schon oben C.II.
157 *Wybitul/Neu/Strauch*, ZD 2018, 202.
158 *Simitis*, in: Simitis, BDSG 2014, 8. Aufl., § 43 Rn. 79ff.
159 *Rost*, RDV 2017, 13, 16.
160 Rundbrief Arbeitnehmeranwälte, 39/2018, S. 16.

Weise einhalten“ sollte,[161] denn wie meistens bei Selbstkontrolle ist sie auch hier nicht immer sicher und daher nicht ausreichend.

Um eine rechtmäßige Verarbeitung von Beschäftigtendaten beim Betriebsrat zu gewährleisten, liegt es auch im Interesse des Arbeitgebers, den o.a. Vorschlag[162] aufzugreifen und in einer freiwilligen Betriebsvereinbarung einen externen Datenschutzbeauftragten für den Betriebsrat vorzusehen.

2. Betrieblicher Datenschutzbeauftragter

Der betriebliche Datenschutzbeauftragte ist als Kontrollorgan nach zunächst im Gesetzgebungsprozess einschränkenden Plänen, schließlich doch in einer Version in Art. 37ff. DSGVO aufgenommen worden, die im Großen und Ganzen der bisherigen deutschen Rechtslage entspricht. Die war allerdings auch bislang schon in Bezug auf Beschäftigtendaten und deren Verarbeitung durch den Betriebsrat problematisch, da der vom Arbeitgeber allein ausgewählte betriebliche Datenschutzbeauftragte als nicht unabhängig gilt. Dabei bleibt es nach der neuen Rechtslage, denn auch nach der DSGVO wird er – ob intern oder extern rekrutiert – allein vom Unternehmen bestellt. Der Kommissionsentwurf der DSGVO hatte das Problem noch adressiert und die Unabhängigkeit des betrieblichen Datenschutzbeauftragten ausdrücklich im Gesetzestext verankert.[163] In der nun geltenden Fassung ist sie nur noch in Erwägungsgrund 97 erwähnt. Art. 38 Abs. 3 DSGVO geht nicht über die bisherige Rechtslage in Deutschland hinaus: der betriebliche Datenschutzbeauftragte ist zwar gemäß Art. 38 Abs. 3 DSGVO nicht weisungsgebunden, bleibt aber der Unternehmensleitung unterstellt und am Unternehmensinteresse ausgerichtet.[164] Daher hatte das BAG schon vor 20 Jahren zu §§ 36 und 37 BDSG a.F. festgestellt,[165] dass der betriebliche Datenschutzbeauftragte die Datenverarbeitung des Betriebsrats nicht kontrollieren darf, da der Betriebsrat bei seiner Bestellung kein ausdrückliches Mitbestimmungsrecht hatte.[166]

---

161 *Klebe*, in: DKKW, 16. Aufl., § 94 Rn. 53.

162 S.o. G.I.

163 Art. 36 DSGVO-E.

164 Vgl. auch *Körner*, a.a.O, S. 61; *Kort*, NZA 2015, 1345, 1348 sieht – etwas zweifelhaft – das Arbeitnehmerinteresse vom Unternehmensinteresse umfasst.

165 BAG, Beschl. v. 11.11.1997 – 1 ABR 21/97, BAGE 87, 64ff.

166 So auch *Klebe,* in: DKKW, § 94; für ein Kontrollrecht schon nach alter Rechtslage aus datenschutzrechtlicher Sicht: *Dammann*, in: Simitis, BDSG 2014, 8. Aufl., § 3 Rn. 240.

Gemäß Art. 38 Abs. 2 DSGVO hat der betriebliche Datenschutzbeauftragte zur Sicherstellung seiner Überwachungsaufgaben nach Art. 39 DSGVO ein Zugangsrecht zu allen Verarbeitungsvorgängen. Ausnahmen sind nicht vorgesehen, auch nicht in Bezug auf den Betriebsrat.[167] Daraus wird z.T. geschlossen, dass „die insoweit vom Bundesarbeitsgericht aus der betriebsverfassungsrechtlichen Unabhängigkeit der Mitarbeitervertretung herausgelesene Einschränkung der Befugnisse des Datenschutzbeauftragten mit der DSGVO nicht vereinbar ist".[168] Den betroffenen Personen wären ansonsten die Rechte aus Art. 38 Abs. 4 DSGVO genommen.

Aus dem Wortlaut von Art. 39 DSGVO ließen sich also ggfs. Überwachungsrechte des betrieblichen Datenschutzbeauftragten gegenüber dem Betriebsrat ableiten, insbesondere da dieser der Datenverarbeitung des Arbeitgebers zugerechnet wird. Allerdings ist zu berücksichtigen, dass auch an dieser Stelle der DSGVO die Friktionen zwischen Datenschutz und Unabhängigkeit der Betriebsratsarbeit verkannt wurden, zumal der deutsche Betriebsrat eine singuläre Stellung im Vergleich zu anderen Interessenvertretungsstrukturen in EU-Mitgliedstaaten einnimmt. Man kann also nicht davon ausgehen, dass der europäische Gesetzgeber den Betriebsrat bewusst der Kontrolle des allein vom Arbeitgeber bestellten betrieblichen Datenschutzbeauftragten unterstellen wollte. Vielmehr ist das Kollisionsproblem übersehen worden – allerdings auch von der deutschen Regierung, die nicht nur die Datenschutzbefugnisse des Betriebsrats, sondern auch den betrieblichen Datenschutzbeauftragten als zwei deutsche Besonderheiten in einem späten Stadium der Verhandlungen in der DSGVO durchsetzen konnte.

Zieht man sonstiges EU-Recht heran, so wird man aus dem Unterrichtungs- und Anhörungsrecht von Arbeitnehmervertretungsorganen in Art. 27 GR-Charta, das in der Richtlinie 2002/14/EG konkretisiert wird, ableiten können, dass diese Rechte ohne Unabhängigkeit der Vertretungsorgane nicht viel wert sind.

Auch das BDSG n.F. regelt nach wie vor nichts zum Verhältnis zwischen Betriebsrat und betrieblichem Datenschutzbeauftragten. Da die Frage seit langem

---

167 *Bergt*, in: Kühling/Buchner, DSGVO, 2018, 2. Aufl., § 38 Rn. 18; *Kort*, ZD 2017, 3, 6; *Wybitul/von Gierke*, BB 2017, 181, 184. *Däubler* bestätigt in Däubler/Wedde/Weichert/Sommer, EU-Datenschutzgrundverordnung und BDSG-neu, 2018, § 38 Rn. 5, dass es keine kontrollfreie Datenverarbeitung geben darf und der betriebliche Datenschutzbeauftragte „muss Zutritt zu allen Räumlichkeiten haben, in denen Daten verarbeitet werden", erwähnt in diesem Zusammenhang die Datenverarbeitung des Betriebsrats aber nicht.

168 *Gola*, ZBVRonline 7-8/2017, 31, 33; *Bergt*, a.a.O.

streitig ist, wäre es Aufgabe des Gesetzgebers, hier Klarheit zu schaffen. Trotz der Öffnung für nationalen Beschäftigungsdatenschutz in Art. 88 DSGVO hat aber der deutsche Gesetzgeber mit § 26 BDSG n.F. – wenn auch etwas mehr als in § 32 BDSG a.F. – mitnichten alle zentralen beschäftigtendatenschutzrechtlichen Fragen beantwortet. Das ist keine seltene Strategie des Gesetzgebers, die es im Ergebnis beim jeweiligen Stand der Rechtsprechung belassen soll. Davon ist auch hier auszugehen, da sich materiell-rechtlich bei der Bestellung des betrieblichen Datenschutzbeauftragten nichts geändert hat, vor allem das Problem von dessen mangelnder Unabhängigkeit nicht angegangen wurde. Daher kann es bei der bisherigen Linie des BAG bleiben, wonach der betriebliche Datenschutzbeauftragte die Datenverarbeitung beim Betriebsrat nicht kontrollieren darf. Dieser Linie könnte auch der EuGH folgen, sollte er mit der Materie befasst werden. Zwar legt die DSGVO großen Wert auf effiziente Kontrolle, aber die muss gerade unabhängig sein. Hier hatte der EuGH bereits 2010 sogar bei den deutschen Aufsichtsbehörden nicht genug Unabhängigkeit gesehen.[169] Kontrolle der Datenverarbeitung, auch der beim Betriebsrat, ist also europarechtlich wichtig, aber nur durch unabhängige Stellen und das ist bei der heutigen Konstruktion des betrieblichen Datenschutzbeauftragten nicht gewährleistet.

Dagegen ist es unproblematisch, wenn der Betriebsrat beschließt, sich vom betrieblichen Datenschutzbeauftragten zum datenschutzkonformen Umgang mit Beschäftigtendaten beraten zu lassen, denn oft basieren Datenschutzverstöße auf fehlender Information.

3. Eigener DSB des Betriebsrats

Da die staatliche Kontrolle von Datenverarbeitung beim Betriebsrat bisher aus Kapazitätsgründen zu wünschen übrig lässt[170] und § 23 BetrVG häufig ein zu grobes Sanktionsmittel darstellt, schlagen auch z.T. diejenigen, die die Position des BAG von 1997 unverändert fortschreiben wollen, jedenfalls für große Betriebsratsgremien einen eigenen Datenschutzbeauftragten vor.[171] Der müsste dann, um die Unabhängigkeit der Kontrolle zu wahren, zwar mit Zustimmung des Betriebsrats bestellt werden, dürfte aber nicht aus dessen eigenen Reihen kommen.

---

169 EuGH, Urt. v. 9.3.2010 – C-518/07 (Kommission/Deutschland), NJW 2010, 1265.

170 Dazu näher unten H.I.

171 *Däubler*, Gläserne Belegschaften, 2017, 7. Aufl., Rn. 641, 687; ähnlich *Klebe*, in: DKKW, § 94 Rn. 54: „einverständliche Regelung mit dem Arbeitgeber".

Auch die Ausarbeitung eigener Datenschutzkonzepte ist zu empfehlen.[172] So könnten in einer freiwilligen Betriebsvereinbarung, in der die Datenschutzgrundsätze niedergelegt sind, auch die Erfüllung der Betroffenenrechte durch den Betriebsrat geregelt werden. Darüber hinaus kann ein eigener externer Datenschutzbeauftragter für den Betriebsrat über § 80 Abs. 3 und § 40 Abs. 2 BetrVG erforderlich sein.

4. Staatliche Aufsichtsbehörden

Dreh- und Angelpunkt für die Überwachung der Datenverarbeitung beim Betriebsrat sind aber die staatlichen Aufsichtsbehörden. Auf die Komplexität der Aufsicht nach der DSGVO soll an dieser Stelle nicht näher eingegangen werden,[173] da sie nur bei grenzüberschreitenden Sachverhalten relevant wird. Jedenfalls sind zunächst die bereits bekannten Aufsichtsorgane für den Betriebsrat zuständig. Hier ist der Staat gefordert, die nötige Infrastruktur und vor allem eine ausreichende personelle Ausstattung sicherzustellen.

172 *Kiesche/Wilke*, AiB 2017, 40, 41ff.; vgl. auch *Klebe*, in: DKKW, § 94 Rn. 53.
173 Vgl. dazu *Körner*, a.a.O., S. 31ff. m.w.N.

H. Aufsichtsbehörden und Betriebsrat

I. Überwachung des Betriebsrats

Sofern der Betriebsrat selbst personenbezogene Beschäftigtendaten verarbeitet, muss er, wie oben dargelegt, die DSGVO einhalten, was durch die Aufsichtsbehörden gemäß § 40 BDSG überwacht wird. Die jeweiligen Landesbehörden sind nach § 40 Abs. 5 BDSG befugt, ein Betriebsratsbüro zu betreten, um dort Prüfungen vorzunehmen, vor allem die Anlagen und Geräte für die Datenverarbeitung zu überprüfen und gemäß § 80 Abs. 4 BDSG erforderliche Auskünfte zu verlangen. Stellt die Aufsichtsbehörde Verstöße fest, kann sie gemäß § 80 Abs. 3 BDSG den Verstoß anderen für die Verfolgung oder Ahndung zuständigen Stellen anzeigen.

Allerdings laufen diese Befugnisse bei der Überprüfung der Betriebsräte in Deutschland in der Praxis häufig aus Kapazitätsgründen[174] ins Leere. Das führt faktisch zu einer zu geringen Kontrolldichte der Verarbeitung von Beschäftigtendaten beim Betriebsrat.[175] Dieser Umstand wird schon deutlich, wenn man sich die einschlägigen Zahlen nur kursorisch vor Augen hält: nach dem IAB-Betriebspanel von 2016 haben 9 % aller Betriebe ab 5 Mitarbeitern einen Betriebsrat.[176] Der Anteil der ca. 35 Millionen Arbeitnehmer, die in diesen 9 % der Betriebe arbeiten, wird von der Hans Böckler-Stiftung, ebenfalls auf der Basis des IAB-Betriebspanels 2016, auf ca. 41 % geschätzt.[177] Die genaue Anzahl der Betriebsräte in Deutschland ist nach wie vor nicht bekannt. Die Frage nach der absoluten Anzahl der Betriebsräte in Deutschland war kürzlich Gegenstand einer kleinen Anfrage der Fraktion der Linken im Bundestag. Auch die Bundes-

---

174 FAZ 25.6.2018: „Behörden verzweifeln am neuen Datenschutz".

175 So auch *Brandt*, Datenschutz im Betriebsrat, AiB 2016, 16, der ausführt, „wegen dieser Kontrollfreiheit sollte der Betriebsrat den Datenschutz ernst nehmen" – aber nicht etwa aus rechtlichen Gründen, sondern „um Kolleginnen und Kollegen nicht zu enttäuschen".

176 *Ellguth/Kohaut*, Tarifbindung und betriebliche Interessenvertretung, Ergebnisse aus dem IAB-Betriebspanel 2016, WSI Mitteilungen 4/2017, S. 278.

177 https://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/themen_showpicture.htm?id=112635&chunk=2

regierung konnte die Frage am 29.6.2018 nicht genau beantworten und stützte sich ihrerseits auf die Ergebnisse des IAB-Betriebspanels von 2016.[178]

Dem stehen bei den Aufsichtsbehörden sehr wenige Mitarbeiter gegenüber. Beim Hessischen Datenschutzbeauftragten etwa sind insgesamt (inklusive des Beauftragten und der Verwaltungsmitarbeiter) 46 Mitarbeiter beschäftigt, vier davon im Bereich Beschäftigtendatenschutz.[179] Das Amt des Bayerischen Datenschutzbeauftragten hat sogar nur 22 Mitarbeiter, einer davon für den Beschäftigtendatenschutz.[180] In den anderen Bundesländern sieht es ähnlich aus.

Nur der Gesetzgeber kann und muss für eine wirksame Kontrollinstanz sorgen, die die Wertungswidersprüche zwischen Datenschutz und Betriebsverfassungsrecht auflöst und dafür wäre neben mehr Personal für die Aufsichtsbehörden auch ein wichtiger Schritt, dass der Betriebsrat bei der Bestellung des betrieblichen Datenschutzbeauftragten ein Mitwirkungsrecht hätte. Da, wo es das schon gibt, etwa in § 74 Abs. 1 Nr. 3 des Hessischen Personalvertretungsgesetzes, bleibt aber dennoch umstritten, ob dann Datenschutzkontrolle beim Betriebsrat möglich wäre.[181]

Treten Datenschutzverstöße beim Betriebsrat zutage, funktioniert aber zumindest die gerichtliche Kontrolle im Einzelfall. So sind etwa Beweismittel, die ein Betriebsrat unter Verstoß gegen Datenschutzrecht erlangt hat, nicht verwertbar[182] oder können Betriebsratsmitglieder, die wiederholt datenschutzrechtswidrig in elektronische Personalakten Einsicht nehmen, aus dem Betriebsrat ausgeschlossen werden.[183] Der Betriebsrat hat auch kein uneingeschränktes Recht zur Weitergabe elektronisch erfasster, namensbezogener Arbeitszeiten an Aufsichtsbehörden.[184] Punktuelle gerichtliche Kontrolle ersetzt aber nicht eine wirksame Kontrollinstanz.

---

178 BT-Drs. 19/2778.

179 https://datenschutz.hessen.de/ueber-uns/aufgaben-und-organisation/aufgabengebiete-und-zust%C3%A4ndige-ansprechpartner

180 https://www.lda.bayern.de/de/organisation.html

181 *Kramer*, Datenschutz-Berater, Nr. 12/2016, 265; *Gola*, ZBVRonline 7-8/2017, S. 31, 32.

182 LAG Berlin-Brandenburg, Beschl. v. 15.5.2014 – 18 TaBV 828/12, juris.

183 LAG Berlin-Brandenburg, ZD 2013, 239. Einen wichtigen Grund für eine außerordentliche Kündigung des Betriebsratsmitglieds hat das LAG dagegen nicht angenommen.

184 BAG, NZA 2009, 1218; BAG, DB 2003, 2496.

II. Einschaltung der Aufsichtsbehörden durch den Betriebsrat

Vor diesem Hintergrund stellt sich die Frage, ob und inwieweit der Betriebsrat die Datenschutz-Aufsichtsbehörden von sich aus einschalten kann.

1. Beratung durch die Aufsichtsbehörde

Zunächst ist an Beratung des Betriebsrats im Zusammenhang mit seinen Aufgaben zum Beschäftigtendatenschutz durch die Aufsichtsbehörde im Rahmen von § 80 Abs. 3 BetrVG zu denken, wenn man die Aufsichtsbehörde für einen Sachverständigen hält und die sonstigen Voraussetzungen des § 80 Abs. 3 BetrVG erfüllt sind. Danach kann der Betriebsrat zur Erfüllung seiner Aufgaben Sachverständige heranziehen, aber nur nach „näherer Vereinbarung mit dem Arbeitgeber". Allerdings hängt das mit der Kostenerstattungspflicht für Sachverständige durch den Arbeitgeber zusammen.[185] Daher ist § 80 Abs. 3 BetrVG nicht einschlägig, wenn die Auskunftsperson unentgeltlich informiert.[186]

Art. 57 Abs. 1 lit. c i.V.m. Abs. 3 DSGVO sieht das sogar ausdrücklich vor. Danach muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet neben dem Parlament und der Regierung auch „andere Einrichtungen und Gremien" über legislative und administrative Maßnahmen zu Datenschutzfragen beraten. Diese Beratung erfolgt gemäß Art. 57 Abs. 3 DSGVO unentgeltlich. Sinn der Norm ist, dass die „anderen Einrichtungen oder Gremien" vom Expertenwissen der Aufsichtsbehörden profitieren sollen.[187] Daher fällt auch der Betriebsrat darunter und kann die unentgeltliche Expertise der Aufsichtsbehörden jederzeit in Anspruch nehmen.

Beratungsfunktionen schreibt den Aufsichtsbehörden auch Art. 36 DSGVO zu. Allerdings bezieht sich Art. 36 DSGVO nur auf die in Art. 35 DSGVO geregelte Datenschutzfolgenabschätzung, d.h. riskante Datenverarbeitung mit hohem Risikopotential für die Betroffenen. Konsultationspflichtig[188] ist dann der Verantwortliche, d.h. je nach Sichtweise entweder nur der Arbeitgeber oder auch der Betriebsrat.

---

185 Vgl. BAG, Beschl. v. 19.4.1989 – 7 ABR 87/87, BAGE 61, 333.

186 ErfK-*Kania*, 2018, 18. Aufl., § 80 BetrVG Rn. 33; GK-BetrVG/*Weber*, § 80 Rn. 139 zu unentgeltlicher Information durch Beamte der Gewerbeaufsicht.

187 *Boehm*, in: Kühling/Buchner, DSGVO, 2018, 2. Aufl., Rn. 15.

188 In der englischen Version der DSGVO ist die Pflicht eindeutig, in der deutschen nicht, *Jandt*, in: Kühling/Buchner, DSGVO, 2018, 2. Aufl., Art. 36 Rn. 6.

Weiter ist die Beratungsfunktion der Aufsichtsbehörden nach Art. 36 Abs. 4 DSGVO. Hier geht es um den neuen Ansatz, dass die Aufsichtsbehörden frühzeitig bei nationalen Gesetzgebungs- und Regelungsverfahren zum Datenschutz als Berater einbezogen werden, die dadurch nicht erst repressiv tätig werden müssen, sondern schon im Vorfeld neuer Regulierung präventiv tätig werden können.[189] Der Betriebsrat und seine normativ wirkenden Betriebsvereinbarungen sind zwar nicht genannt, da sich die DSGVO nicht mit den nationalen Besonderheiten der Arbeitnehmermitwirkung befasst, sondern nur in Art. 88 DSGVO die Öffnung für nationale Regelung in diesem Bereich enthält. Das BDSG n.F. regelt zur Beratung von Betriebsräten durch die Aufsichtsbehörden zwar auch nichts, ist aber sogar hinsichtlich der in Art. 36 DSGVO ausdrücklich gemeinten Bereiche restriktiver als die DSGVO.[190] Nach Sinn und Zweck des Abs. 4 in Art. 36 DSGVO geht es darum, vor gesetzlichen Regelungen Datenschutzberatung zu erhalten. Daher kann auch der Betriebsrat um derartige Beratung vor dem Abschluss von Betriebsvereinbarungen nachsuchen.

2. Initiativrecht des Betriebsrats?

Fraglich ist jedoch, ob der Betriebsrat die Aufsichtsbehörden auch auffordern kann, vermutete Datenschutzverstöße beim Arbeitgeber zu überprüfen.

Europarechtlich sieht Art. 77 DSGVO vor, dass jede betroffene Person ein Beschwerderecht bei einer Aufsichtsbehörde hat, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt. Gemäß Art. 80 Abs. 1 DSGVO darf sich die betroffene Person dabei vertreten lassen. Es muss also immer eine Beauftragung vorausgehen und es dürfen nur die in Art. 80 Abs. 1 DSGVO genannten Einrichtungen beauftragt werden. Allerdings ist der Betriebsrat keine Einrichtung im Sinne des Art. 80 Abs. 1 DSGVO, da es nicht, wie die Norm verlangt, seine hauptsächliche Zielsetzung ist, im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf deren personenbezogene Daten tätig zu werden.

Auch ein Verbandsklagerecht für den Betriebsrat kommt nicht in Betracht, da der deutsche Gesetzgeber von Art. 80 Abs. 2 DSGVO, wonach der nationale Gesetzgeber vorsehen kann, dass die in Abs. 1 genannte Einrichtung auch ohne Auftrag der betroffenen Person die Aufsichtsbehörden einschalten kann – wobei

---

189 *Jandt*, in: Kühling/Buchner, DSGVO 2018, 2. Aufl., § 36 Rn. 13.

190 § 69 BDSG n.F. regelt Beratungspflichten nur in Bezug auf die zusammen mit der DSGVO in Kraft gesetzte Datenschutzrichtlinie für Strafjustiz 2016/679.

auch die „Einrichtung“ näher hätte definiert werden können – keinen Gebrauch gemacht hat.

Schließlich könnte man noch ein „Recht auf Whistleblowing“ des Betriebsrats in Betracht ziehen. Beschwerdemöglichkeiten des Betriebsrats bei Verstößen gegen Datenschutzbestimmungen gegenüber der Aufsichtsbehörde ergeben sich weder aus Datenschutzrecht noch aus dem BetrVG. Auch entsprechende höchstrichterliche Entscheidungen liegen nicht vor. Ableitbar wäre ein solches Recht ggfs. aus der Überwachungspflicht des Betriebsrats gemäß § 80 Abs. 1 Nr. 1 BetrVG. In der Literatur wird ein derartiges Whistleblowing für denkbar gehalten, wenn vorherige Abhilfeersuchen des Betriebsrats an den Arbeitgeber und den betrieblichen Datenschutzbeauftragten ohne Ergebnis geblieben sind.[191] Dem ist zuzustimmen. Ein voraussetzungsloses Recht des Betriebsrats zum Whistleblowing kollidiert dagegen mit dem Grundsatz auf vertrauensvolle Zusammenarbeit zwischen Betriebsrat und Arbeitgeber gemäß § 2 Abs. 1 i.V.m. § 74 Abs. 1 BetrVG.[192] In diese Richtung tendiert auch das BAG in seiner Entscheidung zu § 89 BetrVG, wo ausgeführt wird, dass einiges dafür spricht, *„dass der Betriebsrat wegen des Grundsatzes der vertrauensvollen Zusammenarbeit der Betriebsparteien jedenfalls vor der unaufgeforderten Unterrichtung einer Überwachungsbehörde erfolglos den Versuch unternommen haben muß, den Arbeitgeber zur Abhilfe der Mängel zu bewegen“*.[193] Im Ergebnis darf also der Betriebsrat die Aufsichtsbehörde zur Meldung von Datenschutzverstößen einschalten, wenn seine Konsultation mit dem Arbeitgeber und dem betrieblichen Datenschutzbeauftragten zu keinem Ergebnis geführt hat.

---

191 *Kort*, NZA 2015, 1345, 1351 f.; *ders.*, ZD 2017, 3, 6.

192 *Kort*, ZD 2017, 3, 6; *Gola/Pötters/Wronka*, Handbuch Arbeitnehmerdatenschutz, 2016, 6. Aufl., Rn. 1771; a.A. *Buschmann*, in: DKKW, § 80 Rn. 15.

193 BAG, Beschl. v. 3.6.2003 – 1 ABR 19/02, RDV 2004, 24.

J. Ergebnisse

1. Der Betriebsrat bleibt auch unter der DSGVO zentraler Akteur für die Ausgestaltung des Beschäftigtendatenschutzes (C.).
2. Betriebsvereinbarungen zur Verarbeitung von Beschäftigtendaten unterliegen aber z.T. neuen Anforderungen:
   a) Art. 88 Abs. 2 DSGVO i.V.m. § 26 BDSG (D.I).
   b) Datenschutzgrundsätze aus Art. 5ff. DSGVO (D.II.).
3. Zentral sind Transparenzregeln und Betroffenenrechte (D.II.4. und III.).
4. Das gilt auch für alte Betriebsvereinbarungen, die daher überprüft werden müssen (F.).
5. In jeder Einzelbetriebsvereinbarung sind insbesondere der Zweck der Verarbeitung, die Dauer der Verarbeitung, Löschungsregeln und die Zugriffsrechte zu regeln (E.I.).
6. In Rahmenbetriebsvereinbarungen können Gegenstände geregelt werden, die unabhängig vom konkreten Verarbeitungszweck immer gleich auszugestalten sind, etwa die Betroffenenrechte (E.II.). Rahmenbetriebsvereinbarungen spielen eine große Rolle zur „Rettung" von alten Betriebsvereinbarungen (F.IV.).
7. Moderner, effizienter Datenschutz ist technischer Datenschutz. Das spielt für Betriebsvereinbarungen eine große Rolle. Wo sich der technische Datenschutz ans Mitbestimmungsrecht aus § 87 Abs. 6 BetrVG anknüpfen lässt, sind die entsprechenden Regelungen zwingend, ansonsten kann auf freiwillige Betriebsvereinbarungen gemäß § 88 BetrVG zurückgegriffen werden (E.IV.).
8. Ein Konzernprivileg enthält die DSGVO nicht, aber eine Tendenz Konzerndatenverarbeitung ggfs. doch zu privilegieren. Daher sind, soweit möglich, Konzernbetriebsvereinbarungen zu empfehlen (E.V.).
9. Der Betriebsrat ist auch nach der neuen Rechtslage weiterhin nicht selbst verantwortliche Stelle für die Datenverarbeitung, sondern insoweit Teil des Arbeitgebers, der die Datenverarbeitung verantwortet (G.I.).

10. Überwacht wird die Datenverarbeitung des Betriebsrats durch die staatlichen Aufsichtsbehörden. Die müssten personell aufgestockt werden. Kontrolldefizite an dieser Stelle verantwortet aber nicht der Betriebsrat, sondern der Gesetzgeber.

11. Daneben ist es empfehlenswert, dass Betriebsräte ab einer bestimmten Größe in einer freiwilligen Betriebsvereinbarung einen eigenen externen Datenschutzbeauftragten erhalten.

    Der kann, je nach Konstellation, auch gemäß § 80 Abs. BetrVG erforderlich sein.

12. Der Betriebsrat kann die Aufsichtsbehörden eigenständig einschalten. Für Beratung des Betriebsrats ergibt sich das aus Art. 57 Abs. 1 lit. c i.V.m. Abs. 3 DSGVO (H.II.1.). Für die Meldung von Datenschutzverstößen durch den Arbeitgeber ist das möglich, wenn der Betriebsrat vorab vergeblich den Arbeitgeber und den betrieblichen Datenschutzbeauftragten um Abhilfe ersucht hat (H.II.2.).

Literaturverzeichnis

AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Hrsg.), Das Standard-Datenschutzmodell – eine Methode zur Datenschutzberatung und -prüfung auf Basis einheitlicher Gewährleistungsziele, 2018.

Brandt, Jochen, Datenschutz im Betriebsrat – Doppelaufgabe, AiB 2016, 16–18.

BSI (Hrsg.), BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise, 2018, abrufbar unter: http://bsi.bund.de/gshb.

Datenschutzkonferenz (Hrsg.), DSGVO-Kurzpapier Nr. 5, Datenschutzfolgen-Abschätzung nach Art. 35 DSGVO, 24.07.2017, abrufbar unter: www.lfd.niedersachsen.de.

Däubler, Wolfgang, Gläserne Belegschaften – Das Handbuch zum Beschäftigtendatenschutz, 7. Aufl., Frankfurt am Main, 2017.

Däubler, Wolfgang/Kittner, Michael/Klebe, Thomas/Wedde, Peter, Betriebsverfassungsgesetz, 16. Aufl. 2018 („DKKW").

Däubler, Wolfgang/Wedde, Peter/Weichert, Thilo/Sommer, Imke, EU-Datenschutz-Grundverordnung und BDSG-neu, Kompaktkommentar, Frankfurt am Main 2018.

Dzida, Boris/Grau, Timon, Beschäftigtendatenschutz nach der Datenschutz-Grundverordnung und dem neuen BDSG, DB 2018, 189–194.

Ehmann, Eugen/Selmayr, Martin (Hrsg.), Datenschutzgrundverordnung, 2. Aufl., München 2018.

Ellguth, Peter/Kohaut, Susanne, Tarifbindung und betriebliche Interessenvertretung, Ergebnisse aus dem IAB-Betriebspanel 2016, WSI Mitteilungen 4/2017, 278–286.

Franck, Lorenz, Altverhältnisse unter DSGVO und neuem BDSG – Anwendung des neuen Datenschutzrechts auf bereits laufende Datenverarbeitungen? ZD 2017, 509–513.

Franzen, Martin, Datenschutz-Grundverordnung und Arbeitsrecht, EuZA 2017, 313–351.

Franzen, Martin/Gallner, Inken/Oetker, Hartmut (Hrsg.), Kommentar zum europäischen Arbeitsrecht, 2. Aufl., München 2018.

Gaul, Björn/Pitzer, Saskia, Das Gesetz zur Anpassung des Datenschutzrechts an die DSGVO – Was ändert sich im Beschäftigtendatenschutz? ArbRB 2017, 241–244.

Gola, Peter, Eigenständigkeit des Betriebsrats und Kontrolle durch den Datenschutzbeauftragten – ein ungelöster Konflikt, ZBVR online 2017, Nr. 7/8, 31–34.

Gola, Peter (Hrsg.), Datenschutz-Grundverordnung: DSGVO-VO (EU) 2016/679, Kommentar, 2. Aufl., München 2018.

Gola, Peter/Pötters, Stephan/Wronka, Georg, Handbuch Arbeitnehmerdatenschutz, 7. Aufl., 2016.

Grimm, Detlef, Die „Rahmenbetriebsvereinbarung-DSGVO" als Mittel zur Umsetzung der neuen Datenschutzvorgaben – Teil 1, ArbRB 2018, 78–82.

Hans Böckler Stiftung (Hrsg.), Archiv Betriebliche Vereinbarungen, 2015.

Heuschmid, Johannes, Datenschutz-Grundverordnung und Betriebsverfassung – Eine Positionsbestimmung unter besonderer Berücksichtigung des primären Unionsrechts, SR 2019, 1.

IG Metall (Hrsg.), Handlungshilfe für Betriebsräte und Vertrauensleute Nr. 19: Datenschutzgrundverordnung, 4/2018.

Imping, Andreas, Neue Zeitrechnung im (Beschäftigten-)Datenschutz, CR 2017, 378–388.

Kiesche, Eberhard/Wilke, Matthias, Datenschutz im Betriebsrat, AiB 2017, 40–44.

Kiesche, Eberhard/Wilke, Matthias/Berger, Thomas, Update Betriebsvereinbarungen, AiB 2018, 15–22.

Klösel, Daniel/Mahnhold, Thilo, Die Zukunft der datenschutzrechtlichen Betriebsvereinbarung - Mindestanforderungen und betriebliche Ermessensspielräume nach DSGVO und BDSG nF, NZA 2017, 1428–1433.

Korinth, Michael H., Datenschutz-Grundverordnung – Was ändert sich für den Betriebsrat? - Auswirkungen auf Datenübertragungen an den Betriebsrat, Betriebsvereinbarungen und die sonstige Betriebsratsarbeit, ArbRB 2018, 47–50.

Körner, Marita, Formen der Arbeitnehmermitwirkung – Das französische Comité d'entreprise, Baden-Baden 1999.

Körner, Marita, Wirksamer Beschäftigtendatenschutz im Lichte der Europäischen Datenschutz-Grundverordnung (DSGVO), HSI-Schriftenreihe Band 18, Frankfurt 2017.

Kort, Michael, Schranken des Anspruchs des Betriebsrats auf Information gem. § 80 BetrVG über Personaldaten der Arbeitnehmer, NZA 2010, 1267–1272.

Kort, Michael, Das Dreiecksverhältnis von Betriebsrat, betrieblichem Datenschutzbeauftragten und Aufsichtsbehörde beim Arbeitnehmer-Datenschutz, NZA 2015, 1345–1352.

Kort, Michael, Arbeitnehmerdatenschutz gemäß der EU-Datenschutz-Grundverordnung, DB 2016, 711–716.

Kort, Michael, Was ändert sich für Datenschutzbeauftragte, Aufsichtsbehörden und Betriebsrat mit der DSGVO? – Die zukünftige Rolle der Institutionen rund um den Beschäftigtendatenschutz, ZD 2017, 3–7.

Kort, Michael, Der Beschäftigtendatenschutz gem. § 26 BDSG-neu – Ist die Ausfüllung der Öffnungsklausel des Art. 88 DSGVO geglückt? ZD 2017, 319–323.

Kramer, Philipp, Keine Kontrolle des Betriebs-/Personalrats durch den Datenschutzbeauftragten, DSB 2016, 265.

Krause, Rüdiger, Verhandlungen des 71. Deutschen Juristentages, Band I: Gutachten/Teil B: Digitalisierung der Arbeitswelt – Herausforderungen und Regelungsbedarf, Essen 2016.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung, Kommentar, 2. Aufl., München 2018.

Kurzböck, Christoph/Weinbeck, Kathrin, DSGVO-Verstöße im Betriebsratsbüro – wer haftet? BB 2018, 1652–1655.

LfDI Baden-Württemberg (Hrsg.), Der Ratgeber Arbeitnehmerdatenschutz: Zwischen wirtschaftlicher Abhängigkeit und informationeller Selbstbestimmung, Stuttgart 2017.

Maas, Ingrid/Schmitz, Karl/Wedde, Peter, Datenschutz 2014 – Probleme und Lösungsmöglichkeiten, Frankfurt am Main 2014.

Maschmann, Frank, Datenschutzgrundverordnung: Quo vadis Beschäftigtendatenschutz? – Vorgaben der EU-Datenschutzgrundverordnung für das nationale Recht, DB 2016, 2480–2486.

Middel, Lukas, Beschäftigtendatenschutz im Lichte der DSGVO und unter Berücksichtigung des BDSG (neu), AuR 2018, 411.

Müller-Knapp, Hjort, Wulff Partnerschaft (Hrsg.), Rundbrief Nr. 39, Hamburg 2018, abrufbar unter: http://www.arbeitnehmer-anwaelte.de/.

Müller-Glöge, Rudi/Preis, Ulrich/Schmidt, Ingrid (Hrsg.), Erfurter Kommentar zum Arbeitsrecht, 18. Aufl., München 2018 („ErfK").

Paal, Boris P./Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DSGVO BDSG, Kommentar, 2. Aufl., München 2018.

Reinecke, Gerhard, Die Begriffe Arbeitnehmer und Beschäftigter, NJW 2018, 2081–2087.

Roßnagel, Alexander, Datenschutzgesetzgebung für öffentliche Interessen und den Beschäftigungskontext, DuD 2017, 290–294.

Rost, Maria Christina, Bußgeld im digitalen Zeitalter – was bringt die DSGVO? RDV 2017, 13–20.

Schrey, Joachim/Kielkowski, Jacek, Die datenschutzrechtliche Betriebsvereinbarung in DSGVO und BDSG 2018 – Viel Lärm um Nichts? BB 2018, 629–635.

Schulze, Marc-Oliver/Pfeffer, Julia, Datenschutzkonforme Rahmenbetriebsvereinbarung zur Informations- und Kommunikationstechnik (IKT), ArbRAktuell 2017, 358–361.

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

Sörup, Thorsten, Gestaltungsvorschläge zur Umsetzung der Informationspflichten der DSGVO im Beschäftigungskontext, ArbRAktuell 2016, 207–213.

Sörup, Thorsten/Marquardt, Sabrina, Auswirkungen der EU-Datenschutzgrundverordnung auf die Datenverarbeitung im Beschäftigungskontext, ArbR-Aktuell 2016, 103–106.

Sydow, Gernot (Hrsg.), Europäische Datenschutzgrundverordnung – Handkommentar, 2. Aufl., Baden-Baden, Wien, Zürich 2018.

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

Tiedemann, Jens, Auswirkungen von Art. 88 DSGVO auf den Beschäftigtendatenschutz – Gestaltungsspielräume für Gesetzgeber und Betriebsparteien, ArbRB 2016, 334–337.

Wieduwilt, Hendrik, Behörden verzweifeln am neuen Datenschutz, FAZ vom 25.6.2018.

Wiese, Günther/Kreutz, Peter/Oetker, Hartmut et al., Gemeinschaftskommentar zum Betriebsverfassungsgesetz, 11. Aufl. 2018 („GK-BetrVG").

Wisskirchen, Gerlind/Schiller, Jan Peter, Aktuelle Problemstellungen im Zusammenhang mit „Bring your own device", DB 2015, 1163–1168.

Wolff, Amadeus/Brink, Stefan (Hrsg.) Beck'scher Online-Kommentar Datenschutzrecht, 24. Aufl. 2018 („BeckOK Datenschutzrecht").

Wurzberger, Sebastian, Anforderungen an Betriebsvereinbarungen nach der DSGVO – Konsequenzen und Anpassungsbedarf für bestehende Regelungen, ZD 2017, 258–263.

Wybitul, Tim, Was ändert sich mit dem neuen EU-Datenschutzrecht für Arbeitgeber und Betriebsräte? – Anpassungsbedarf bei Beschäftigtendatenschutz und Betriebsvereinbarungen, ZD 2016, 203–208.

Wybitul, Tim, Der neue Beschäftigtendatenschutz nach § 26 BDSG und Art. 88 DSGVO, NZA 2017, 413–419.

Wybitul, Tim, Betriebsvereinbarungen im Spannungsverhältnis von arbeitgeberseitigem Informationsbedarf und Persönlichkeitsschutz des Arbeitnehmers – Handlungsempfehlungen und Checkliste zu wesentlichen Regelungen, NZA 2017, 1488–1494.

Wybitul, Tim/Sörup, Thorsten/Pötters, Stephan, Betriebsvereinbarungen und § 32 BDSG: Wie geht es nach der DSGVO weiter? – Handlungsempfehlungen für Unternehmen und Betriebsräte, ZD 2015, 559–564.

Wybitul, Tim/von Gierke, Lukas, Checklisten zur DSGVO – Teil 2: Pflichten und Stellung des Datenschutzbeauftragten im Unternehmen, BB 2017, 181–185.

Wybitul, Tim/Neu, Leonie/Strauch, Martin, Schadensersatzrisiken für Unternehmen bei Datenschutzverstößen – Verteidigung gegen Schadensersatzforderungen nach Art. 82 DSGVO, ZD 2018, 202.

In der Schriftenreihe des Hugo Sinzheimer Instituts für Arbeitsrecht sind zuletzt erschienen:

Band 27 Martin Franzen
Stärkung der Tarifautonomie durch Anreize zum Verbandsbeitritt
ISBN 978-3-7663-6855-3

Band 26 Frank Bayreuther
Sicherung der Leistungsbedingungen von (Solo-)Selbständigen, Crowdworkern und anderen Plattformbeschäftigten
ISBN 978-3-7663-6850-8

Band 25 Stefan Greiner
Das arbeitskampfrechtliche Verhältnismäßigkeitsprinzip
ISBN 978-3-7663-6829-4

Band 24 Daniel Ulber/Karoline Wiegandt
Die Bindung von Arbeitnehmervereinigungen an die europäischen Grundfreiheiten
ISBN 978-3-7663-6761-7

Band 23 Claudia Schubert
Betriebliche Mitbestimmung in Unternehmen und Konzernen mit Matrixorganisation
ISBN 978-3-7663-6713-6

Band 22 Bernd Waas / Wilma B. Liebman / Andrew Lyubarsky / Katsutoshi Kezuka
Crowdwork – A Comparative Law Perspective
ISBN 978-3-7663-6697-9

Band 21 Holger Brecht-Heitzmann / Judith Reuter
Perspektiven zur rechtlichen Stärkung des Ehrenamts in der sozialen Selbstverwaltung
ISBN 978-3-7663-6658-0

Band 20 Ulrich Preis / Alberto Povedano Peramato
Das neue Recht der Allgemeinverbindlicherklärung im Tarifautonomiestärkungsgesetz
ISBN 978-3-7663-6657-3

Band 19 Eva Kocher / Jürgen Kädtler / Ulrich Voskamp / Laura Krüger
Noch verfassungsgemäß?
Fernwirkungen bei Arbeitskämpfen in der Automobilindustrie und die Verfassungsmäßigkeit des § 160 Abs. 3 SGB III
ISBN 978-3-7663-6466-1

Weitere Informationen zur Schriftenreihe: www.hugo-sinzheimer-institut.de