



Marita Körner

Beschäftigtendatenschutz im Geltungsbereich der DSGVO

Rechtswissenschaftliche
Beiträge der
Hamburger Sozialökonomie

Heft 25

Marita Körner

Beschäftigtendatenschutz im Geltungsbereich der DSGVO

Rechtswissenschaftliche
Beiträge der
Hamburger Sozialökonomie

Heft 25

Prof. Dr. Marita Körner

Professorin für Deutsches und Internationales Arbeits- und Sozialrecht und Rechtsvergleichung am Fachbereich Sozialökonomie der Fakultät für Wirtschafts- und Sozialwissenschaften an der Universität Hamburg; Zweitmitglied der Fakultät für Rechtswissenschaft der Universität Hamburg.

Impressum

Kai-Oliver Knops, Marita Körner, Karsten Nowrot (Hrsg.)
Rechtswissenschaftliche Beiträge der Hamburger Sozialökonomie

Heft 25, August 2019

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet unter <http://dnb.dnb.de> abrufbar.

ISSN 2366-0260 (print)
ISSN 2365-4112 (online)

Reihengestaltung: Ina Kwon
Produktion: UHH Druckerei, Hamburg
Schutzgebühr Euro 5

Die Hefte der Schriftenreihe „Rechtswissenschaftliche Beiträge der Hamburger Sozialökonomie“ finden sich zum Download auf der Website des Fachgebiets Rechtswissenschaft am Fachbereich Sozialökonomie unter der Adresse:

<https://www.wiso.uni-hamburg.de/fachbereich-sozoek/professuren/koerner/fiwa/publikationsreihe.html>

Fachgebiet Rechtswissenschaft
Fachbereich Sozialökonomie
Fakultät für Wirtschafts- und Sozialwissenschaften
Universität Hamburg
Von-Melle-Park 9
20146 Hamburg

Tel.: 040 / 42838 - 3521
Fax: 040 / 42838 - 8129
E-Mail: Beate.Hartmann@wiso.uni-hamburg.de

Inhalt

A. Hintergrund: Reform des Datenschutzes durch die DSGVO	5
B. DSGVO und Beschäftigtendatenschutz: „Öffnungsklausel“ in Art. 88 DSGVO	6
C. Sonderrolle von Betriebsvereinbarungen für den Beschäftigtendatenschutz	8
I. Anforderungen aus Art. 88 DSGVO	8
1. Aus Art. 88 Abs. 1 DSGVO	9
2. Aus Art. 88 Abs. 2 DSGVO	9
II. Datenschutzgrundsätze nach der DSGVO	12
1. Berücksichtigung von Art. 6 DSGVO.....	12
2. Berücksichtigung von Art. 9 DSGVO.....	12
3. Berücksichtigung von Art. 5 DSGVO.....	12
4. Transparenzregeln.....	14
III. Betroffenenrechte.....	16
Literaturverzeichnis	19

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,¹ 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 von 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,² 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 daher 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 ans 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

* Die folgenden Ausführungen sind ein leicht überarbeiteter Auszug aus: *Marita Körner, Die Auswirkungen der Datenschutz-Grundverordnung (DSGVO) in der betrieblichen Praxis*, Frankfurt 2019 (HSI-Schriftenreihe Bd. 28).

1 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.

2 *Körner, Wirksamer Beschäftigtendatenschutz im Lichte der Europäischen Datenschutz-Grundverordnung (DSGVO)*, HSI-Schriftenreihe Band 18, Frankfurt 2017, S. 31 ff.

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 Rechts-Übung 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. zurückgreift³ – wenn § 26 BDSG auch umfassender ist –, bleibt auch die bisherige Rechtsprechung dazu weiter relevant.

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.⁴ Das allein deutet schon darauf hin, dass es sich bei den nationalen Regelungen, seien es gesetzliche oder kollektivvertragliche, um eigenständige Erlaubnistatbestände handelt.

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,⁵ 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.⁶ 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

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

4 Dazu unten C.I.2.

5 Vgl. Körner, a.a.O., S. 17 ff.

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

wird, unter welches Niveau eine nationale Regelung im Beschäftigtendatenschutz keinesfalls sinken darf, was materiell dem 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,⁷ 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“.⁸ 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,⁹ was nationale Abweichungen zugunsten eines höheren Schutzniveaus erschwerte. Die Situation stellt sich bei der DSGVO gerade wegen der Öffnung für nationale Regelung anders dar.¹⁰

Die Vorgaben der Verordnung sind also als Mindestbedingungen für den Beschäftigtendatenschutz zu verstehen.¹¹ 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.

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,

7 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.; Wýbitul, Der neue Beschäftigtendatenschutz nach § 26 BDSG und Art. 88 DSGVO, NZA 2017, 413.

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

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

10 A.a.O.

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

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, wäre 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 und alte daran kritisch zu überprüfen. 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. 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.

C. Sonderrolle von Betriebsvereinbarungen für den 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.¹² Von der DSGVO und einem einheitlichen europäischen Datenschutz bliebe dann angesichts der zahlreichen Öffnungen für nationale Regelungen nicht viel übrig. Die Datenschutzerfordernisse ergeben sich aus Art. 88 DSGVO.

Da in Deutschland Betriebsvereinbarungen eine große Rolle als Rechtfertigung für die Verarbeitung von Beschäftigtendaten spielen, müssen auch sie sich an der DSGVO orientieren.

¹² So aber offenbar *Heuschmid*, SR 2019, 1 ff.

Anders als in anderen EU-Staaten haben sich die Betriebspartner schon früh mit Fragen des Beschäftigtendatenschutzes befasst und mittlerweile einen großen Bestand an betriebsverfassungsrechtlichem Beschäftigtendatenschutz in Gestalt von datenschutzrechtlichen Betriebsvereinbarungen geschaffen, der bis zum Inkrafttreten der DSGVO viel genauer als die Generalklausel zum Beschäftigtendatenschutz in § 32 BDSG a.F. zentrale Fragen des Beschäftigtendatenschutzes behandelt hat. Daher war es wichtig, diese Regelungsebene auch unter der DSGVO zu erhalten, was schließlich im europäischen Verhandlungsprozess gelungen ist. Das war nicht selbstverständlich, da andere Mitgliedstaaten das Instrument der datenschutzrechtlichen Betriebsvereinbarung nicht kennen und daher an einer entsprechenden Öffnung kein Interesse hatten.

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 Datenverarbeitung 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 DSGVO¹³ 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 Rechts auf informationelle Selbstbestimmung der Beschäftigten darf in Betriebsvereinbarungen strenger geschützt werden als in der DSGVO selbst.¹⁴

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

¹³ So auch schon in: *Körner*, HSI-Schriftenreihe Nr. 18, S. 50 ff.

¹⁴ Dazu schon oben B.

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,¹⁵ 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 Regelung geöffneten Bereich des Beschäftigtendatenschutzes das Mindestdatenschutzniveau der DSGVO nicht unterschritten wird.¹⁶ Allgemeine Hinweise in Betriebsvereinbarungen auf die DSGVO reichen nicht; das wären keine „besonderen“ Maßnahmen. Vielmehr ist Leitlinie, dass Maßnahmen zur Wahrung der menschlichen Würde sowie berechtigter Interessen und Grundrechte der betroffenen Personen getroffen werden müssen. Dabei geht es vor allem um das Recht auf informationelle Selbstbestimmung¹⁷ und um das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme¹⁸ 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 auch 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.¹⁹ 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“.*²⁰

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 DSGVO 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.²¹ Diese Unterscheidung wird

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

16 Tiedemann, ArbRB 2016, 334, 336.

17 BVerfG vom 15.12.83 – 1 BvR 209/83, BVerfGE 65, 1.

18 BVerfG vom 27.2.2008 – 1 BvR 370/07, BVerfGE 120, 274.

19 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.

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

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

z.T. in der Literatur bestritten,²² 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).

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.

Schließlich ist gem. Art. 88 Abs. 2 DSGVO besondere Vorsicht geboten bei Überwachungssystemen am Arbeitsplatz. Da es in Betriebsvereinbarungen zum Beschäftigtendatenschutz in der Regel 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 abgewichen 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,²³ – 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.²⁴ So grundsätzlich können Kontrollverbote nicht ausgeschlossen werden, da die DSGVO eine strengere nationale Regelung ermöglicht²⁵ 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.

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

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

24 *Maschmann*, DB 2016, 2480.

25 *Körner*, a.a.O., S. 52 ff.

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.²⁶

Eine ausdrückliche Regelung dazu enthält die DSGVO nicht. In der rechtswissenschaftlichen Literatur wird das z.T. empfohlen²⁷ bzw. sogar für verpflichtend gehalten.²⁸ 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 im Sinne von Art. 6 DSGVO gelten soll.²⁹ Eine Pflicht dazu besteht aber nicht.³⁰

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 gem. 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 eingestuft 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

26 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.

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

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

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

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

die Nichtberücksichtigung überzeugen häufig nicht. So wird dort dann doch für erforderlich gehalten, jedenfalls die Zweckbindung in jede Betriebsvereinbarung aufzunehmen.³¹ 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, „ggfs.“ auch noch die Datenrichtigkeit.³²

Diese nicht sehr gradlinigen Vorschläge dürften zu Rechtsunsicherheit führen. Daher ist es besser und ergibt sich auch aus Art. 26 Abs. V 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.

Jedenfalls reicht es nicht, wenn die datenschutzrechtlichen Grundsätze nur beachtet werden.³³ Auch nach dieser Ansicht wird allerdings konzidiert, dass es für neu abzuschließende Kollektivvereinbarungen zu empfehlen ist, „die datenschutzrechtlichen Grundsätze in ausdrückliche Regelungen zu übersetzen“.³⁴

Der zentrale Grundsatz des Datenschutzrechts, die Zweckbindung jeder Vereinbarung (**Art. 5 Abs. 1 lit. b DSGVO**) ist zwar in vielen Betriebsvereinbarungen bereits enthalten, häufig aber nicht präzise genug. Hier besteht Kontroll- und ggfs. Nachbesserungsbedarf in jedem Einzelfall,³⁵ weil der Zweck der Dreh- und Angelpunkt für jede Datenverarbeitung und alle daraus folgenden Befugnisse und Einschränkungen für die Verwendung der Beschäftigten-daten ist. Soll etwa eine Personaldatenbank eingeführt werden, würde als Zweckbestimmung „Personalverwaltung“ nicht reichen, sondern 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 gem. Art. 30 DSGVO an.

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. Da Art und Umfang der Datenminimierung vom jeweiligen Zweck der Datenverarbeitung abhängt, müssen die entsprechenden Minimierungsmaßnahmen in die konkrete Betriebsvereinbarung aufgenommen werden und reichen nicht etwa allgemeine Hinweise in einer Rahmenbetriebsvereinbarung, dass der Grundsatz der Datenminimierung einzuhalten sei.

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

32 *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.

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

34 A.a.O.

35 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.

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.

Auch eine Speicherbegrenzung muss gem. **Art. 5 Abs. 1 lit. e DSGVO** ausdrücklich vorgesehen werden. Eine Regelung, dass Beschäftigtendaten 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, sollte das im Zusammenhang mit neuen Aufgaben hilfreich sein, ist es 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 reicht es nicht, diesen Punkt in einer Rahmenbetriebsvereinbarung zu regeln. Technische und organisatorische Vorkehrungen spielen auch hier eine große Rolle.

4. *Transparenzregeln*

Die inhaltlich-materiellen Transparenzvorgaben sind ein Kerntück der DSGVO.³⁶ 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 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

36 *Korinth*, ArbRB 2018, 47.

müssen sich Art, Inhalt und Umfang der legitimierten Verarbeitungsvorgänge klar aus der Betriebsvereinbarung ergeben.³⁷

Als derzeit gültiger Maßstab können dafür die Grundsätze der Keylogger-Entscheidung des BAG (noch zum alten Recht)³⁸ und die EGMR-Entscheidung in der Sache *Barbulescu*³⁹ 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 verdeckten 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. Genauer 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 gehalten.⁴⁰ 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 *Keylogger*-Entscheidung des BAG, nur offen zulässig.

Auf dieser Linie liegt auch die Entscheidung des EGMR im Fall *Lopez Ribalda*,⁴¹ 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.⁴² 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

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

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

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

40 EGMR, Urt. v. 12.1.2016 – 61496/08, DuD 2016, 395.

41 EGMR, Urt. v. 9.1.2018 – 1874/13 (*Lopez Ribalda u.a./Spanien*), NLMR 2018, 38.

42 EGMR, Urt. v. 22.2.2018 – 588/13 (*Libert/France*), ZD 2018, 263.

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.

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 gem. **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.⁴³ 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.⁴⁴

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.⁴⁵ 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 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.⁴⁶ 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

43 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.

44 So u.a. *Sörup*, ArbRAktuell 2016, 207.

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

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

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.⁴⁷

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.⁴⁸ Allerdings bleibt es auch dann empfehlenswert, die Pflichten aus Art. 12 ff. DSGVO in einer Betriebsvereinbarung zu dokumentieren und ggfs. zu konkretisieren.⁴⁹ 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.

47 A.a.O.

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

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

Literaturverzeichnis

- DÄUBLER, Wolfgang/WEDDE, Peter/WEICHERT, Thilo/SOMMER, Imke, Datenschutzgrundverordnung 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.
- FRANZEN, Martin, Datenschutz-Grundverordnung und Arbeitsrecht, EuZA 2017, 313-351.
- GAUL, Björn/PITZER, Saskia, Das Gesetz zur Anpassung des Datenschutzrechts an die DSGVO - Was ändert sich im Beschäftigtendatenschutz? ArbRB 2017, 241-244.
- GOLA, Peter (Hrsg.), Datenschutz-Grundverordnung: DSGVO - VO (EU) 2016/679, Kommentar, 2. Aufl., München 2018.
- HEUSCHMID, Johannes, Datenschutzgrundverordnung 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.
- 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, Wirksamer Beschäftigtendatenschutz im Lichte der Europäischen Datenschutz-Grundverordnung (DSGVO), HSI-Schriftenreihe Band 18, Frankfurt 2017.
- KÜHLING, Jürgen/BUCHNER, Benedikt (Hrsg.), Datenschutz-Grundverordnung, Kommentar, 2. Aufl., München 2018.
- MASCHMANN, Frank, Datenschutzgrundverordnung: Quo vadis Beschäftigtendatenschutz? – Vorgaben der EU-Datenschutzgrundverordnung für das nationale Recht, DB 2016, 2480-2486.
- PAAL, Boris P./PAULY, Daniel A. (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DSGVO BDSG, Kommentar, 2. Aufl., München 2018.
- ROSSNAGEL, Alexander, Datenschutzgesetzgebung für öffentliche Interessen und den Beschäftigungskontext, DuD 2017, 290–294.
- SCHREY, Joachim/KIELKOWSKI, Jacek, Die datenschutzrechtliche Betriebsvereinbarung in DSGVO und BDSG 2018 - Viel Lärm um Nichts? BB 2018, 629-635.
- 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, ArbRAktuell 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.
- WURZBERGER, Sebastian, Anforderungen an Betriebsvereinbarungen nach der DSGVO - Konsequenzen und Anpassungsbedarf für bestehende Regelungen, ZD 2017, 258-263.
- 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.

Rechtswissenschaftliche Beiträge der Hamburger Sozialökonomie

ISSN 2366-0260 (print) / ISSN 2365-4112 (online)

Bislang erschienene Hefte

Heft 1

Felix Boor, Die Yukos-Enteignung. Auswirkungen auf das Anerkennungs- und Vollstreckungssystem aufgehobener ausländischer Handelsschiedssprüche

Heft 2

Karsten Nowrot, Sozialökonomie als disziplinäre Wissenschaft. Alternative Gedanken zur sozialökonomischen Forschung, Lehre und (Eliten-) Bildung

Heft 3

Florian Hipp, Die kommerzielle Verwendung von frei zugänglichen Inhalten im Internet

Heft 4

Karsten Nowrot, Vom steten Streben nach einer immer wieder neuen Weltwirtschaftsordnung. Die deutsche Sozialdemokratie und die Entwicklung des Internationalen Wirtschaftsrechts

Heft 5

Karsten Nowrot, Jenseits eines abwehrrechtlichen Ausnahmecharakters. Zur multidimensionalen Rechtswirkung des Widerstandsrechts nach Art. 20 Abs. 4 GG

Heft 6

Karsten Nowrot, Grundstrukturen eines Beratungsverwaltungsrechts

Heft 7

Karsten Nowrot, Environmental Governance as a Subject of Dispute Settlement Mechanisms in Regional Trade Agreements

Heft 8

Margaret Thornton, The Flexible Cyborg: Work-Life Balance in Legal Practice

Heft 9

Antonia Fandrich, Sustainability and Investment Protection Law. A Study on the Meaning of the Term Investment within the ICSID Convention

Heft 10

Karsten Nowrot, Of “Plain” Analytical Approaches and “Savior” Perspectives: Measuring the Structural Dialogues between Bilateral Investment Treaties and Investment Chapters in Mega-Regionals

Heft 11

Maryna Rabinovych, The EU Response to the Ukrainian Crisis: Testing the Union’s Comprehensive Approach to Peacebuilding

Heft 12

Marita Körner, Die Datenschutzgrundverordnung der Europäischen Union: Struktur und Ordnungsprinzipien

Heft 13

Christin Krusenbaum, Das deutsche Krankenversicherungssystem auf dem Prüfstand – Ist die Bürgerversicherung die ultimative Alternative?

Heft 14

Marita Körner, Age Discrimination in the Context of Employment

Heft 15

Avinash Govindjee/ Judith Brockmann/ Manfred Walser, Atypical Employment in an International Perspective

Heft 16

Cara Paulina Gries, Gesetzliche Barrieren bei der Integration von geduldeten Flüchtlingen in den deutschen Arbeitsmarkt

Heft 17

Karsten Nowrot, Aiding and Abetting in Theorizing the Increasing Softification of the International Normative Order - A Darker Legacy of Jessup’s Transnational Law?

Heft 18

Matti Riedlinger, Das CSR-Richtlinie-Umsetzungsgesetz: Implementierung von Corporate Social Responsibility Berichtspflichten in nationales Recht

Heft 19

Karsten Nowrot, “Competing Regionalism” vs. “Cooperative Regionalism”: On the Possible Relations between Different Regional Economic Integration Agreements

Heft 20

Karsten Nowrot, The 2017 EU Conflict Minerals Regulation: An Effective European Instrument to Globally Promote Good Raw Materials Governance?

Heft 21

Karsten Nowrot, The Other Side of Rights in the Processes of Constitutionalizing International Investment Law: Addressing Investors' Obligations as a New Regulatory Experiment

Heft 22

Karsten Nowrot/Emily Sipiorski, Arbitrator Intimidation and the Rule of Law: Aspects of Constitutionalization in International Investment Law

Heft 23

Karsten Nowrot, European Republicanism in (Legitimation) Action: Public Participation in the Negotiation and Implementation of EU Free Trade Agreements

Heft 24

Karsten Nowrot, Non-Recognized Territorial Entities in the Post-Soviet Space from the Perspective of WTO Law: Outreach to Outcasts?

