



Marita Körner

Die Rolle des Betriebsrats im Beschäftigtendatenschutz

Rechtswissenschaftliche
Beiträge der
Hamburger Sozialökonomie

Heft 27

Marita Körner

Die Rolle des Betriebsrats im Beschäftigtendatenschutz

Rechtswissenschaftliche
Beiträge der
Hamburger Sozialökonomie

Heft 27

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 27, September 2019

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikations 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](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. Der Betriebsrat als Hüter des Beschäftigtendatenschutzes	5
I. Betriebsvereinbarung als zentrales Datenschutz-Regelungsinstrument.....	5
II. Kollision zwischen Datenschutz und Mitbestimmungsrechten?	6
III. Einbeziehung des Betriebsrats in die Datenschutzfolgenabschätzung?.....	8
B. Zu regelnde Datenschutzinhalte in Betriebsvereinbarungen	10
I. Notwendige Datenschutzinhalte in Einzelbetriebsvereinbarungen	10
II. Datenschutzregelungen in Rahmenbetriebsvereinbarungen.....	11
III. Übersicht über Datenverarbeitungs-Regelungsgegenstände.....	13
IV. Technische Maßnahmen	14
V. Konzerndatenverarbeitung	16
C. Umgang mit alten Betriebsvereinbarungen	17
I. Grundsätzliche Überlegungen.....	17
II. Einzelprüfung	18
III. FAQ.....	19
IV. Rahmenbetriebsvereinbarungen	19
V. Steckbriefe	20
Literaturverzeichnis	23

A. Der Betriebsrat als Hüter des Beschäftigtendatenschutzes*

Die Rolle des Betriebsrats im Beschäftigtendatenschutz ist im EU-Vergleich eine deutsche Besonderheit, deren Fortschreibung in der europäischen Regelung zunächst nicht selbstverständlich war. Erst im Laufe des jahrelangen Verhandlungsprozesses ist es gelungen, die Rolle des Betriebsrats auch im Geltungsbereich der DSGVO zu erhalten.

Dabei war auch im deutschen Kontext ursprünglich die Funktion des Betriebsrats bei der Sicherung des Beschäftigtendatenschutzes nicht eindeutig.

I. Betriebsvereinbarung als zentrales Datenschutz-Regelungsinstrument

Dass die Betriebsvereinbarung ein eigenständiges Regelungsinstrument i.S.v. § 4 I BDSG a.F. („andere Rechtsvorschrift“) für Beschäftigtendatenschutz sein kann,¹ 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.² Das BAG hatte allerdings in den 1980er Jahren auch eine Abweichung zu Lasten des Datenschutzniveaus der Beschäftigten erlaubt,³ 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 eingefordert⁴ 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 Betriebsvereinbarungen handelt, die als Datenschutzregelungsinstrument bislang nur in Deutschland eine Rolle spielen, wohingegen sich das von Tarifverträgen für den Bereich Beschäftigtendatenschutz nicht sagen lässt.⁵

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

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

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

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

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

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

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.⁶ 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.

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 ermöglicht Mitbestimmung bei der Aufstellung von Personalauswahl- und Beurteilungsgrundsätzen. Darüber hinaus können gemäß § 88 BetrVG freiwillige (Rahmen-) Betriebsvereinbarungen zur Verarbeitung von Beschäftigtendaten abgeschlossen werden.⁷

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 materiellrechtlich 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 Abs. 1 BDSG n.F. stellt dabei wie § 32 Abs. 3 BDSG a.F. klar, dass die Datenerhebung des Betriebsrats im Rahmen seiner

⁶ So auch *Klösel/Mahnhold*, NZA 2017, 1428, 1429 m.w.N. zu den Gegenstimmen.

⁷ Zu Rahmenbetriebsvereinbarungen s.u. C.IV.

betriebsverfassungsrechtlichen Aufgaben gerechtfertigt ist,⁸ – zumal Abs. 6 klarstellt, dass es nicht zu einer Einschränkung von Beteiligungsrechten kommen darf –, aber dabei die datenschutzrechtlichen Anforderungen der DSGVO einhalten muss. Bei genauer Betrachtung läuft das im 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, die allerdings gem. § 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.⁹ Ob auch der EuGH das so sehen würde, ist nicht eindeutig, insbesondere wenn der Betriebsrat nicht als eigene verarbeitende Stelle angesehen wird. Für den rechtlich korrekten Inhalt von Datenschutz-Betriebsvereinbarungen 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.¹⁰ Darüber hinaus hat der Arbeitgeber die Rechte aus § 23 Abs. 1 BetrVG.

8 So auch Rundbrief Arbeitnehmeranwälte, 39/2018, S. 17 (unter www.arbeitnehmer-anwaelte.de).

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

10 Vgl. dazu auch zur Überforderung der nationalen Datenschutzbehörden nach Inkrafttreten der DSGVO in FAZ 25.6.2018: „Behörden verzweifeln am neuen Datenschutz“.

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.

Jedenfalls ist der Vertreterbegriff in Art. 35 Abs. 9 DSGVO weiter als in der Definitionsnorm Art. 4 Abs. 17 DSGVO,¹¹ 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.¹²

„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.¹³ 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.¹⁴

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.¹⁵ Bei unbestimmt vielen Betroffenen, wie bei OnlinePortalen, 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.

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

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

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

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

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

Da deren Einführung auch unter § 87 Abs. 1 Nr. 6 BetrVG fällt, ist der Betriebsrat aus mitbestimmungsrechtlichen Gründen zu beteiligen und wird er eine Datenschutzfolgenabschätzung sogar verlangen können,¹⁶ denn insoweit verfolgen das Mitbestimmungsrecht 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.¹⁷

Der Widerspruch zwischen § 87 Abs. 1 Nr. 6 BVerfG 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 Selbstschutz 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.¹⁸

Im Übrigen werden die Aufsichtsbehörden in Zukunft dadurch mehr Rechtssicherheit schaffen können, dass sie gem. 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 der Aufsichtsbehörde genannt ist.¹⁹ Die Aufsichtsbehörden haben bereits begonnen, an einer als „Blacklist“ bezeichneten Liste zu arbeiten.²⁰

16 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 Datenschutz-Betriebsvereinbarung dem Betriebsrat einen Entwurf der Datenschutzfolgenabschätzung vorzulegen.

17 *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.

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

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

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

B. 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.²¹ 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 allgemeinen Grundsätze der DSGVO müssen in allen Betriebsvereinbarungen zum Beschäftigtendatenschutz berücksichtigt werden. Nur die müssen 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, Lösungsregeln 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 die 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 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

21 Vgl. dazu schon *Körner*, Wirksamer Beschäftigtendatenschutz im Lichte der Europäischen Datenschutz-Grundverordnung (DSGVO), Frankfurt 2017.

- 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.²² 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).
 - Löschfristen sind anzugeben; ggfs. Hinweis auf ein Löschkonzept mit Hilfe technischer Voreinstellungen.
 - Ggfs. Schnittstellen zu andere Systemen. Je nach konkreter Ausgestaltung kann dieser Punkt auch in einer Rahmenbetriebsvereinbarung geregelt werden.

II. Datenschutzregelungen in Rahmenbetriebsvereinbarungen²³

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 Datenschutzbeauftragten 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. 13 f. 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.

²² Details in IGM, Handlungshilfe für Betriebsräte und Vertrauensleute Nr. 19: Datenschutz-Grundverordnung 4/2018, S. 19 ff.

²³ Da Rahmenbetriebsvereinbarungen vor allem für die „Rettung“ von alten Betriebsvereinbarungen eine große Rolle spielen, werden sie ausführlicher dort behandelt, vgl. unten C.IV.

6. Angaben zu den technischen Datenschutzmaßnahmen, Art. 25 DSGVO, d.h. Mindestanforderungen an jede IT-Anwendung (u.a. Anonymisierung, Pseudonymisierung, Verschlüsselung, Löschroutinen).²⁴
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 Steckbriefen²⁵).
9. Regelung zur Datenübermittlung an Dritte sowie ggfs. zum internationalen Datentransfer.
10. Ggfs. Regelungen zur Datenschutzfolgenabschätzung.²⁶
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.²⁷
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.
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,²⁸ 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.²⁹ 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

24 Zum technischen Datenschutz auch noch im Folgenden unter IV.

25 Vgl. dazu unten C.V.

26 Zu Mitwirkungsmöglichkeiten des Betriebsrats an der Datenschutzfolgenabschätzung schon oben A.III.

27 Schulze/Pfeffer, ArbRAktuell 2017, 358 ff., Nr. 8.

28 Zu diesen noch unten C.

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

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.³⁰ In Gestalt von Steckbriefen gibt es diese Muster in der betrieblichen Praxis vereinzelt schon.³¹

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 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

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

31 S.u. C.V.

rechtfertigen könnten.³² 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, RIFD-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 technische 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 Beschäftigtendaten 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 Regelung 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 §

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

87 Abs. 1 Nr. 6 BetrVG anknüpfen lässt, sind die Regelungen zwingend, ansonsten kann auf freiwillige Betriebsvereinbarungen gem. § 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 Beschäftigendaten, die zu unterschiedlichen Zwecken verarbeitet werden, wie Personalverwaltung, Telefon- und Smartphone-Nutzung, Zugangssysteme, interne soziale Netzwerke oder Ortungssysteme, ist vorzunehmen.³³ Um wirksame Standards für technische Voreinstellungen für die Verarbeitung von Beschäftigendaten 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)³⁴ und das Standard-Datenschutzmodell der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder³⁵ Unterstützung.³⁶

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 Arbeitgebereinstimmens entfallen zu lassen und nur noch auf die Erforderlichkeit für die Betriebsratsaufgaben abzustellen.³⁷ 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.³⁸

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 allerdings bei hochkomplexer Datenverarbeitung überzogene Anforderungen.³⁹ Solange der deutsche Gesetzgeber zu dieser Frage nicht handelt,

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

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

35 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.

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

37 *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.

38 Vgl. DKKW § 80 Rn 155.

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

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 Beschäftigten-
daten, 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 konzern-
verbundenen Unternehmen benötigen also eine eigene Rechtfertigung, die der DSGVO ent-
sprechen muss. Art. 4 Abs. 19 DSGVO definiert den Konzern nur. Dagegen hält Erwägungs-
grund 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 Rechts-
wirkung. 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,⁴⁰ ermöglicht Art. 47 DSGVO die Datenübermittlung im Konzern auf der Basis
von Binding Corporate Rules. Die sind 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 Beschäftigten-
daten im Konzern regeln können,⁴¹ 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 entsprechen müssen. Da jedenfalls Abweichungen vom Standard der DSGVO nach
unten unzulässig sind,⁴² könnte ein generelles Konzernprivileg durch nationales Recht und
daher auch durch Betriebsvereinbarungen nicht eingeführt werden.⁴³ Allerdings zeigt Erwä-
gungsgrund 48, dass auch ein generelles Verbot einer Übermittlung von Beschäftigtendaten
i.d.R. nicht wirksam sein wird, jedenfalls die im Erwägungsgrund 48 vorgesehene Interessen-
abwägung 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.

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

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

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

43 *Maschmann*, a.a.O.

C. 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.⁴⁴ 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 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.⁴⁵

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.⁴⁶ Z.T. wird zwar von deren Fortgeltung ausgegangen, kann aber nur dann weiter als Rechtfertigung für die Verarbeitung von Beschäftigtendaten herangezogen werden, wenn sie der DSGVO entspricht.⁴⁷

In beiden Fällen stellt sich die Frage, inwieweit alte Betriebsvereinbarungen an Art. 88 Abs. 2 DSGVO und die allgemeinen Regeln in Art. 5 ff. 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. 5 ff. DSGVO nicht verletzen. Diese Frage kann mit letzter Verbindlichkeit nur der Europäische Gerichtshof beantworten.⁴⁸ 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,⁴⁹ d.h. es müssen in der Betriebsvereinbarung nur die Aspekte aus Art. 88 Abs. 2 DSGVO aufgegriffen werden, um die es in der

44 HBS – Archiv Betriebliche Vereinbarungen 2015.

45 BAG, Beschl. v. 9.7.2013 – 1 ABR 19/12, NZA 2014, 99.

46 Franck, ZD 2017, 509, 511.

47 Maschmann, DB 2016, 2480, 2485.

48 Kiesche/Wilke/Berger, AiB 2018, 15, 16.

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

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 Umkleieräume von der Überwachung ausgeschlossen werden. Dabei handelt es sich dann um eine „Maßnahme zur Wahrung der menschlichen Würde“,⁵⁰ 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 jedenfalls Anpassungsbedarf bei den viel dezidiert als nach altem Datenschutzrecht in der DSGVO geforderten Transparenzanforderungen bestehen. Dass die Transparenz der Verarbeitung von Beschäftigtendaten derzeit im Fokus der datenschutzrechtlichen Diskussion steht,⁵¹ zeigt auch die jüngste Datenschutz-Rechtsprechung des EGMR.

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 gem. § 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“.⁵²

Dafür kommen mehrere Wege in Betracht. Bei denen ist zu beachten, dass das Gesetz in Art. 88 Abs. 2 DSGVO nur „angemessene“ Regelungen verlangt, sodass es auf die Situation ankommt, mit welchem Umfang und in welcher Detailtiefe die Voraussetzungen der DSGVO in den Betriebsvereinbarungen erscheinen müssen.⁵³

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 nehmen sind.⁵⁴ Dann nämlich könnten alte Betriebsvereinbarungen im Grunde nie der DSGVO entsprechen.

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

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

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

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

54 So *Grimm*, ArbRB 2018, 78.

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.⁵⁵

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 ordnungskonform 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.⁵⁶

IV. Rahmenbetriebsvereinbarungen

Rechtssicherer ist aber eine grundlegende Rahmenbetriebsvereinbarung. Dadurch könnten bestehende Betriebsvereinbarungen durch datenschutzrechtliche Klarstellungen und Ergänzungen „gerettet“ werden.⁵⁷ Rahmenbetriebsvereinbarungen sind, was die allgemeinen Datenschutz-Grundsätze angeht, aber auch für neue Betriebsvereinbarungen sinnvoll⁵⁸ 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.⁵⁹ 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 gehört jedenfalls der Verarbeitungszweck und alle an ihn gebundenen Faktoren, wie die zulässige Speicherdauer oder

55 *Wibytul/Sörup/Pöppers*, ZD 2015, 559, 561.

56 Rundbrief Arbeitnehmeranwälte, 39/2018, S. 6.

57 So u.a. *Wibytul*, NZA 2017, 1488, 1490.

58 So schon oben B.II.

59 A.a.O.

die zugriffsberechtigten Personen. Dagegen dürfen Datenschutzregeln, die unabhängig von jeweiligen Verarbeitungszweck, immer gleich sind, wie etwa die Betroffenenrecht, 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. dargestellten 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 B.II. Dargestellten.

Rahmenbetriebsvereinbarungen können, wo es sinnvoll erscheint, z.B. wenn sie sehr umfangreich sind, um eine FAQ-Liste⁶⁰ ergänzt werden, in der die Beschäftigten leichter Zugriff auf die wichtigsten Datenschutzregeln erhalten.

An sich sind Rahmenbetriebsvereinbarungen für den Beschäftigtendatenschutz nichts Neues. Schon seit Jahrzehnten werden in den Betrieben auf freiwilliger Basis EDV-Rahmenbetriebsvereinbarungen abgeschlossen,⁶¹ 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.⁶²

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,⁶³ 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

60 Dazu schon oben III.

61 Schapper, *ArbuR* 1988, 97.

62 Däubler, *Gläserne Belegschaften*, 2017, 7. Aufl., Rn. 817.

63 www.datev.de/datenschutz-steckbrief

mit Steckbriefen weisen daher für alte Betriebsvereinbarungen 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.⁶⁴

64 S.o. B.II.

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.
- 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/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.
- FRANCK, Lorenz, Altverhältnisse unter DSGVO und neuem BDSG - Anwendung des neuen Datenschutzrechts auf bereits laufende Datenverarbeitungen? ZD 2017, 509-513.
- 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.
- IG METALL (Hrsg.), Handlungshilfe für Betriebsräte und Vertrauensleute Nr. 19: Datenschutzgrundverordnung, 4/2018.
- 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.
- KÖRNER, Marita, Wirksamer Beschäftigtendatenschutz im Lichte der Europäischen Datenschutz-Grundverordnung (DSGVO), HSI-Schriftenreihe Band 18, Frankfurt 2017.
- KORT, Michael, Arbeitnehmerdatenschutz gemäß der EU-Datenschutz-Grundverordnung, DB 2016, 711-716.
- KRAUSE, Rüdiger, Verhandlungen des 71. Deutschen Juristentages, Band I: Gutachten/TeilB: Digitalisierung der Arbeitswelt – Herausforderungen und Regelungsbedarf, Essen 2016.
- KÜHLING, Jürgen/BUCHNER, Benedikt (Hrsg.), Datenschutz-Grundverordnung, Kommentar, 2. Aufl., München 2018.
- 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.
- PAAL, Boris P./PAULY, Daniel A. (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DSGVO BDSG, Kommentar, 2. Aufl., München 2018.
- 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.
- 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.

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?

Heft 25

Marita Körner, Beschäftigtendatenschutz im Geltungsbereich der DSGVO

Heft 26

Vladlena Lisenco/Karsten Nowrot, The 2018 Pridnestrovian Law on State Support for Investment Activities: Some Thoughts on an Investment Statute in a Frozen Conflict Situation

