Studien zum deutschen und europäischen Arbeitsrecht 95

Benjamin Blum

People Analytics

Eine datenschutzrechtliche Betrachtung moderner Einsatzszenarien für automatisierte, datenbasierte Entscheidungen

Nomos

Studien zum
deutschen und europäischen Arbeitsrecht

Herausgegeben von

Band 95

Benjamin Blum

People Analytics

Eine datenschutzrechtliche Betrachtung moderner Einsatzszenarien für automatisierte, datenbasierte Entscheidungen

Nomos

The book processing charge was funded by the Baden-Württemberg Ministry of Science, Research and Arts in the funding programme Open Access Publishing and the University of Mannheim.

Diese Publikation entstand im Rahmen der Landesgraduiertenförderung Baden-Württemberg.

This publication was prepared under a grant through the Landesgraduiertenförderung Baden-Württemberg.

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

Zugl.: Mannheim, Univ., Diss., 2020

u.d.T.: People Analytics: Eine datenschutzrechtliche Betrachtung moderner Einsatzszenarien für automatisierte, datenbasierte Entscheidungen

1. Auflage 2021

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-8487-8214-7
ISBN (ePDF): 978-3-7489-2636-8

DOI: https://doi.org/10.5771/9783748926368

Onlineversion
Nomos eLibrary

Meinem Opa

Vorwort

Die vorliegende Arbeit wurde im Dezember 2020 von der Fakultät für Rechtswissenschaft und Volkswirtschaftslehre an der Universität Mannheim als Dissertation angenommen. Literatur und Rechtsprechung wurden für die Veröffentlichung noch einmal aktualisiert und befinden sich auf dem Stand von April 2021.

Zuvorderst möchte ich mich bei meinem geschätzten Doktorvater, Prof. Dr. Friedemann Kainer, für die ausgezeichnete Betreuung, den immer spannenden und lehrreichen Diskurs zu diesem Thema sowie für die unglaublich schnelle Erstellung des Erstgutachtens bedanken. Während meiner Zeit als wissenschaftlicher Mitarbeiter an seinem Lehrstuhl hat er mich bei allen Fragen des Lebens unterstützt und mir zahlreiche Gelegenheiten geboten, mich weiterzuentwickeln. Herrn Prof. Dr. Jens Bülte danke ich für die rasante Erstellung des Zweitgutachtens sowie die lehrreiche Zeit als wissenschaftliche Hilfskraft an seinem Lehrstuhl, in welcher ich erste Einblicke in den Wissenschaftsapparat gewinnen durfte. Auch während meiner Promotionszeit stand er für einen fachlichen und persönlichen Austausch im Westflügel immer zur Verfügung. Herrn Prof. Dr. Eibe Riedel danke ich für die Übernahme des Vorsitzes beim Rigorosum, die Erstellung eines Gutachtens für die Landesgraduiertenförderung Baden-Württemberg sowie die zahlreichen lehrreichen und unterhaltsamen Kaffee-Pausen zwischendurch.

Der Landesgraduiertenförderung Baden-Württemberg möchte ich ebenso meinen Dank aussprechen für die Förderung meines Promotionsvorhabens aussprechen wie dem Nomos-Verlag, dessen Ansprechpartner mir für Fragen immer zur Verfügung standen und vor allem eine Vollförderung für eine Open Access-Publikation organisiert haben.

Herausragender Dank gilt vor allem meiner Familie, die mich schon mein ganzes Leben bei meinem Bildungs- und Lebensweg mit allen Kräften unterstützt. Besonders möchte ich mich bei meinem Vater, Gerhard Blum, bedanken, der mir in allen Lebenslagen mit voller Kraft und bedingungslos beisteht und vor allem mir das Studium und diese Arbeit erst ermöglicht hat. Ein besonderer Dank gilt auch meiner Frau, Jana Blum, die, seit ich sie kenne, Unglaubliches leistet und vor allem mir – trotz unseres gemeinsamen Nachwuchses in der „Hochphase meiner Dissertation", ihres eigenen Master-Studiums sowie ihrer Berufstätigkeit – immer

die notwendige Zeit verschafft hat, um die Dissertation in der geplanten Zeit fertigzustellen. Großer Dank gebührt auch meinem Großvater, Otto Blum, der mir schon in jungem Alter den Gedanken einer Promotion in den Kopf gepflanzt hat und mich meine ganze Kindheit und Jugend über ermutigt hat, hohe Ziele anzustreben. Ohne ihn hätte ich diese Arbeit mit Sicherheit nicht veröffentlicht, sodass ich ihm auch diese Arbeit widme. Schließlich möchte ich auch meinen Sohn, Malo Blum, nicht unerwähnt lassen, der unbewusst und unbeabsichtigt ab Juli 2019 dafür sorgte, dass ich mich bei meiner Arbeit auf das Wesentliche konzentriere, in dem er einen beträchtlichen Anteil der 24 Stunden eines Tages für sich in Anspruch nahm.

Ein ganz besonderer Dank gilt auch der gesamten „Westflügel-Gang", welche mich in meinen Vorhaben immer bestärkt und auch für die nötigen Auflockerungen und Ablenkungen im Alltag gesorgt hat und für einen exzellenten fachlichen Austausch, aber auch für private Angelegenheiten immer ein offenes Ohr hatte. Besonders hervorheben möchte ich hierbei Lucina Herzog, LL.M. (Cambridge), die durch ihre kritische Durchsicht und ihre zahlreichen Anmerkungen mit Verbesserungsvorschlägen zu einer wesentlichen Verbesserung dieser Arbeit beigetragen hat.

Zum Gelingen dieser Arbeit trugen selbstverständlich auch noch weitere Menschen bei, die ich aber leider nicht alle namentlich an dieser Stelle erwähnen kann, dennoch aber an dieser Stelle mich bei ihnen herzlich bedanken möchte.

Großniedesheim, im Juni 2021 *Benjamin Blum*

Inhaltsübersicht

Inhaltsverzeichnis

Abkürzungsverzeichnis

a.A.	andere Auffassung
a.E.	am Ende
a.F.	alte Fassung
ABl.	Amtsblatt
Abs.	Absatz
AES	Advanced Encryption Standard
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AGG	Allgemeines Gleichbehandlungsgesetz
AI	Artificial Intelligence (siehe KI)
Alt.	Alternative
Anh.	Anhang
AP	Arbeitsrechtliche Praxis
APA	Advanced People Analytics
ArbG	Arbeitsgericht
ArbGG	Arbeitsgerichtsgesetz
ArbR	Arbeitsrecht
ArbRAktuell	Arbeitsrecht Aktuell
ArbRB	Arbeits-Rechtsberater
ArbSchG	Arbeitsschutzgesetz
ArbStättV	Arbeitsstättenverordnung
Art.	Artikel
Aufl.	Auflage
BAG	Bundesarbeitsgericht
BAGE	Entscheidungen des Bundesarbeitsgerichts
BB	Betriebsberater
BDSG	Bundesdatenschutzgesetz
BeckOK	Beck'scher Online-Kommentar
BeckRS	Beck-Rechtssache
BEEG	Bundeselterngeld- und Elternzeitgesetz
Beschl.	Beschluss
BetrVG	Betriebsverfassungsgesetz

BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BMAS	Bundesministerium für Arbeit und Soziales
BPersVG	Bundespersonalvertretungsgesetz
BR-Drs.	Bundesratsdrucksache
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BYOD	Bring Your Own Device
bzw.	beziehungsweise
CCZ	Corporate Compliance Zeitschrift
CM/Rec	Recommendation of the Committee of Ministers
CO	Kohlenstoffmonoxid
CR	Computer & Recht
CuA	Computer und Arbeit
CV	Curriculum Vitae (Lebenslauf)
d.h.	das heißt
DANA	Datenschutznachrichten
DatenSR	Datenschutzrecht
DB	Der Betrieb
DLIES	Discrete Logarithm Integrated Encryption Scheme
DPIA	Data Protection Impact Assessment (= Datenschutzfolgenabschätzung)
DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
DSGVO/ DS-GVO	Datenschutzgrundverordnung
DSK	Datenschutzkonferenz
DS-RL	Datenschutzrichtlinie (RL 95/46/EG)
DSWR	Datenverarbeitung, Steuer, Wirtschaft, Recht
DuD	Datenschutz und Datensicherheit
DVBl	Deutsches Verwaltungsblatt
e.V.	eingetragener Verein

EBPM	Evidenzbasiertes Personalmanagement
ECC	Elliptic Curve Cryptography
ECIES	Elliptic Curve Integrated Encryption Scheme
ECLI	European Case Law Identifier
EDPB	European Data Protection Board (→ *siehe EDSA*)
EDSA	Europäischer Datenschutzausschuss
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
EKMR	Europäische Kommission für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
EP	Europaparlament
ErfK	Erfurter Kommentar zum Arbeitsrecht
ErwG	Erwägungsgrund
et. al.	et alii
etc.	et cetera
EU	Europäische Union
EuArbRK	Kommentar zum europäischen Arbeitsrecht
EuGH	Europäischer Gerichtshof
EU-GRC	Charta der Grundrechte der Europäischen Union
EUV	Vertrag über die Europäische Union
EuZA	Europäische Zeitschrift für Arbeitsrecht
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EzA	Entscheidungen zum Arbeitsrecht
f./ff.	folgende/r
FAQ	Frequently Asked Questions
FAT(32)	File Allocation Table (32)
Fn.	Fußnote
FS	Festschrift
GDPR	General Data Protection Regulation
GewO	Gewerbeordnung
GG	Grundgesetz
ggf.	gegebenenfalls
GK-BetrVG	Gemeinschaftskommentar zum Betriebsverfassungsgesetz
GLONASS	Globalnaja nawigazionnaja sputnikowaja sistema (russisch für: Globales Satellitennavigationssystem)

GmbH	Gesellschaft mit beschränkter Haftung
GPS	Global Positioning System
GS	Großer Senat
GWR	Gesellschafts- und Wirtschaftsrecht
h.M.	herrschende Meinung
HdbIT-DSR	Handbuch des IT- und Datenschutzrechtes
HGB	Handelsgesetzbuch
HK	Handkommentar
HR	Human Ressources
HRM	Human Ressources Management
i.E.	im Ergebnis
i.R.d.	im Rahmen der/des
i.S.d.	im Sinne der/des
i.V.m.	in Verbindung mit
ID	Identifikator
IKT	Informations- und Kommunikationstechnologie
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
IP	Internet Protocol
IT	Informationstechnologie
ITRB	IT-Rechtsberater
JZ	Juristenzeitung
Kfz	Kraftfahrzeug
KI	Künstliche Intelligenz
KMU	Klein- und mittelständische Unternehmen
KR/K&R	Kommunikation und Recht
KSchG	Kündigungsschutzgesetz
LAG	Landesarbeitsgericht
LAN	Local Area Network
LBS	Location Based Services
lit.	litera (Buchstabe)
Ls.	Leitsatz
m. Anm.	mit Anmerkung
m.a.W.	mit anderen Worten
m.w.N.	mit weiteren Nachweisen

MHdB-ArbR	Münchener Handbuch zum Arbeitsrecht
Mio.	Million/Millionen
MMR	Multimedia und Recht
MuSchG	Mutterschutzgesetz
n.F.	neue Fassung
NJOZ	Neue Juristische Online-Zeitschrift
NJW	Neue Juristische Wochenschrift
NJW-RR	Neue Juristische Wochenschrift – Rechtsprechungsreport
Nr./Nrn.	Nummer/Nummern
NTFS	New Technology File System
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NVwZ-RR	Neue Zeitschrift für Verwaltungsrecht – Rechtsprechungsreport
NZA	Neue Zeitschrift für Arbeitsrecht
NZA-RR	Neue Zeitschrift für Arbeitsrecht – Rechtsprechungsreport
o.g.	oben genannt/e/er/es
öAT	Zeitschrift für das öffentliche Arbeits- und Tarifrecht
OCR	Optical Character Recognition (Texterkennung in Bildern mittels Software)
OLAP	Online Analytical Processing
OLG	Oberlandesgericht
Os.	Orientierungssatz
PA	People Analytics
PC	Personal Computer
PDF	Portable Document Format
PinG	Privacy in Germany
PMS	Personalmanagementsystem
ppm	parts per mol
RdA	Recht der Arbeit
RDV	Recht der Datenverarbeitung
resp.	respektive
RFID	Radio-Frequency Identification
RL	Richtlinie
Rn.	Randnummer
Rs.	Rechtsache
RSA	Rivest-Shamir-Adleman
RW	Rechtswissenschaft

S.	Satz / Seite
s.o.	siehe oben
SGB	Sozialgesetzbuch
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
sog.	sogenannt/e/s
SPA	Simple People Analytics
SprAuG	Sprecherausschussgesetz
SQL	Structured Query Language
SSID	Service Set Identifier
st. Rspr.	ständige Rechtsprechung
StGB	Strafgesetzbuch
str.	streitig
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TOM	technische-organisatorische Maßnahme
u.a.	unter anderem
u.ä.	und ähnliche(s)
u.U.	unter Umständen
u.v.m.	und viele/vieles mehr
UAbs.	Unterabsatz
Urt.	Urteil
USA	United States of America
v.	vom/von
Var.	Variante
VerSanG(-E)	Verbandsanktionengesetz(-Entwurf)
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
vgl.	vergleiche
VO	Verordnung
VOIP	Voice over IP
VPN	Virtual Private Network
VuR	Verbraucher und Recht
Wi-Fi	Wireless Fidelity
WLAN	Wireless LAN

WP	Working Paper
WPS	Wi-Fi Positioning System
z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutzrecht
ZESAR	Zeitschrift für europäisches Sozial- und Arbeitsrecht
ZfA	Zeitschrift für Arbeitsrecht
zfm	Zeitschrift für Forderungsmanagement
zfo	Zeitschrift Führung + Organisation
zit. n.	zitiert nach
ZRP	Zeitschrift für Rechtspolitik
ZSR	Zeitschrift für Schweizerisches Recht

A. Einleitung

§ 1 Überblick

Die Menschheit ist auf dem Weg zur digitalen Evolution. Die Technisierung und Digitalisierung des Alltags schreiten unaufhörlich voran – und dies mit einer rasanten Geschwindigkeit. In den letzten Jahrzehnten wurde der Fortschritt durch die erhöhte Rechenkapazität und den nahezu unbegrenzten Speicherplatz nochmals exponentiell beschleunigt. Big Data, Machine Learning und Künstliche Intelligenz[1] sind Begriffe, die inzwischen jedermann bekannt und nahezu täglich Gegenstand der medialen Berichterstattung im technischen Bereich sind.[2] Mit der Zunahme von Daten und deren Verarbeitung hat auch der Schutz dieser Daten, vor allem der personenbezogenen Daten, eine ganz andere Bedeutung erlangt.[3] Die Gesellschaft muss vor den Risiken des digitalen Umfelds geschützt werden, sodass der Einzelne nicht zu einem bloßen Datenobjekt degradiert[4] und die Privatsphäre ein Relikt aus alten Zeiten wird.

Auch vor der Arbeitswelt macht der digitale Fortschritt keinen Halt. Vielmehr ist diese die „zentrale Schnittstelle der Veränderung"[5]. Jeder Unternehmer[6] strebt dem Ziel der Gewinnmaximierung nach. Dieses Ziel kann auf verschiedenste Wege erreicht werden. Einer davon ist die Kostensenkung durch Rationalisierung von Arbeitsprozessen, also der Minimierung des erforderlichen Arbeits- und Kostenaufwandes durch effizientere Ausgestaltung von Arbeitsprozessen. In diesem Zusammenhang werden sog. *Business-Intelligence*-Systeme (BI-Systeme) relevant.[7] Der Begriff der *Business Intelligence* selbst ist schon alt und wurde wohl das erste Mal in

1 Kurz: KI, englisch: Artificial Intelligence (AI).
2 Siehe beispielsweise das größte technische Newsportal Deutschlands: www.heise.de.
3 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 37 Rn. 5.
4 So bereits das Bundesverfassungsgericht im Jahr 1983, vgl. BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1 – Volkszählungsurteil.
5 *BMAS*, Grünbuch Arbeiten 4.0, S. 6.
6 Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die gewählte männliche Form schließt eine adäquate weibliche oder diverse Form gleichberechtigt ein.
7 *Grothe/Gentsch*, Business intelligence, S. 69.

der „*Cyclopaedia of Commercial and Business Anectotes*“ aus dem Jahre 1868 verwendet: Hier wird beschrieben, wie ein Bankier Informationen nutzt, um Profit daraus zu schlagen, indem er diese Informationen als Erster besitzt.[8] Im Kontext der Informationstechnik dürfte *Luhn* erstmals 1958[9] den Begriff verwendet haben[10] und zwar in dem Zusammenhang, wie Informationen automatisch auf die Zielperson abgestimmt und entsprechend im Unternehmen verteilt werden können, um die Entscheidungsfindung zu unterstützen und zu optimieren. So wird im Kern der Begriff auch heute noch verstanden.[11] BI-Systeme sind Systeme, die computerbasiert unternehmerische Entscheidungen unterstützen – mit Hilfe von Algorithmen. Kombiniert mit neueren Technologien, die diese Business Intelligence nutzen (z.B. *People Analytics*), können inzwischen automatisiert Entscheidungen gefällt werden.[12]

Solch automatisierte Entscheidungen sind selbstverständlich auch im HR-Management denkbar und werden vor allem außerhalb Europas bereits weitgehend angewandt.[13] So können beispielsweise ungeeignete Bewerber auf eine Stelle durch einen Computer aussortiert oder die gesamte Bewerberliste nach Eignung sortiert werden. Ein Beispiel wäre, dass diese mit einem Punktewert, einem sog. „Score“ versehen werden, damit der Verantwortliche[14] sofort einen Überblick über die Geeignetheit eines Kandidaten hat. In den Vereinigten Staaten und teilweise sogar in Großbritannien wenden bereits 70 % der Unternehmen solche Systeme an.[15] Manche Unternehmen gehen sogar so weit, dass sie die Bewerber überhaupt nicht mehr persönlich interviewen, sondern den Computer die Entscheidung

8 *Kirkland*, Cyclopaedia of Commercial and Business Anecdotes, S. 210.
9 *Luhn*, IBM Journal 1958, 314.
10 *Dorschel*, Praxishandbuch Big Data, S. 256.
11 *Gola*, Datenschutz am Arbeitsplatz, S. 12 Rn. 27 f.
12 WHWS/*Broy/Heinson*, B. II. Die automatisierte Einzelfallentscheidung im Beschäftigungsverhältnis, Rn. 1: „*Immer häufiger werden IT-Systeme auch über Beschäftigte entscheiden, ohne dass ein Mensch beteiligt ist.*“
13 Vgl. *Peck*, The Atlantic 2013 (Dezember 2013); *O'Neil*, Weapons of math destruction, S. 108: 60-70 % der Unternehmen wenden solche Technologien an, im Vergleich zu 30-40 % im Jahr 2014.
14 Es sind stets Personen männlichen und weiblichen Geschlechts gleichermaßen gemeint; zur besseren Leserlichkeit und ohne Diskriminierungsabsicht wird im Folgenden nur die männliche Form verwendet.
15 *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, <www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/BSt_DSGVOundADM_dt.pdf>, S. 7; so auch *O'Neil*, Weapons of math destruction, S. 108.

treffen lassen. Es findet also keinerlei menschliche Interaktion mehr statt.[16] Dieses Szenario ist jedoch nicht lediglich im Bewerbungsverfahren, sondern auch während eines intakten Arbeitsverhältnisses denkbar, wenn es darum geht, welche Arbeitnehmer auf Schulungen geschickt, befördert oder gar entlassen werden sollen. Für die Entscheidung des Computers können in den Entscheidungsalgorithmus unzählige Daten einfließen, die von der fachlichen Qualifikation des Arbeitnehmers bis hin zu Persönlichkeits- und Gesundheitsaspekten reichen können. Das gesamte HR-Management wird also immer datenlastiger bzw. datengetriebener (auch *evidenzbasiertes* Management genannt; die zugrundeliegenden Ansätze werden unter dem Stichwort *People Analytics* zusammengefasst).

Aufgrund immer leistungsfähigerer Computer und der Möglichkeit nahezu unbegrenzt Daten zu speichern, sind allumfassende „Auswertungen von Menschen" binnen Bruchteilen von Sekunden möglich. Bereits früh hat das Bundesverfassungsgericht daher festgestellt, dass es kein „belangloses Datum" (mehr) gibt.[17] Der Grundstein für das heutige Datenschutzrecht wurde gelegt. Seit dem 25.05.2018 gibt es nunmehr in Europa eine neue Regelung des Datenschutzes, die sog. Datenschutz-Grundverordnung[18]. Sie soll den heutigen Anforderungen, die durch die rasche technologische Entwicklung entstanden sind, gerecht werden.[19]

In Art. 22 DSGVO findet sich eine Regelung über automatisierte Entscheidungen im Einzelfall einschließlich Profiling. Es ist umstritten, ob es sich hierbei um ein Verbot mit Erlaubnisvorbehalt[20] oder lediglich um ein Betroffenenrecht handelt, welches dieser geltend machen muss, wenn er nicht Betroffener einer automatisierten Entscheidung sein will[21]. Ausnahmen sind nur im Rahmen der Ausnahmetatbestände von Art. 22 Abs. 2 DSGVO möglich. Das Profiling wird in Art. 4 Nr. 4 DSGVO defi-

16 Vgl. *Peck*, The Atlantic 2013 (Dezember 2013).

17 BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1 (44) – Volkszählungsurteil Rn. 158.

18 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. EU L 119/1.

19 Vgl. Erwägungsgrund 6 der DS-GVO.

20 *Eichler*, RDV 2017, 10 (11); *Taeger*, RDV 2017, 3; wohl auch *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 78 Rn. 61; *Sörup/Marquardt*, ArbRAktuell 2016, 103 (106); Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 29b; Sydow/*Helfrich*, Art. 22 DSGVO Rn. 39 f.

21 Dafür EuArbRK/*Franzen*, Art. 22 DSGVO Rn. 3 m.w.N.; zweifelnd an einem Verbot Plath/*Kamlah*, Art. 22 DSGVO Rn. 4.

niert als *jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogene Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.* Zumindest nach dem Wortlaut des Erwägungsgrunds 71 der Verordnung könnte man davon ausgehen, dass das Profiling auch eine automatisierte Entscheidung darstellt und daher unter das Verbot fällt. So würde das im Erwägungsgrund explizit aufgeführte Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen als modernes Tool im Personalmanagement jedenfalls erheblichen datenschutzrechtlichen Bedenken unterliegen.

Doch auch auf bereits eingesetzte Systeme, die wegen der etwas anderen Formulierung des § 6a BDSG a.F. aufgrund mangelnder automatisierter Entscheidung im Einzelfall zulässig waren, könnte ein weitergehendes Verbot durch Art. 22 DSGVO Auswirkungen dergestalt haben, dass diese nunmehr umgestaltet bzw. abgeschafft werden müssen. Aktuelle Personalbedarfsplanungssysteme basieren beispielsweise darauf, dass zukünftiger quantitativer, zeitlicher und örtlicher Personalbedarf automatisiert durch Algorithmen bestimmt wird.[22] Hierbei werden sog. *Data Mining*-Systeme eingesetzt, welche bislang unbekannte Zusammenhänge in Personaldaten entdecken sollen, wobei wohl häufig auf anonymisierte Daten zurückgegriffen werden kann.[23] *Data Mining*-Systeme sind Anwendungen, die bislang unbekannte und potenziell nützliche Muster in Daten erkennen können.[24] Eine Vielzahl der Daten sind im Unternehmen in aller Regel bereits vorhanden und in den Datenbanken der Personalmanagementsysteme[25] gespeichert. Diese müssen nur noch zusammengeführt bzw. verknüpft und mit den eingangs genannten BI-Systemen ausgewertet werden.

Nach einer repräsentativen Studie von LinkedIn und Bitkom Research sammeln bereits 78 % der befragten Unternehmen Daten der Beschäftig-

22 *Strohmeyer*, Informationssysteme im Personalmanagement, S. 95.
23 *Strohmeyer*, Informationssysteme im Personalmanagement, S. 165.
24 *Strohmeyer*, Informationssysteme im Personalmanagement, S. 157.
25 Ein Personalmanagementsystem ist ein System zur umfassenden Verwaltung von Personaldaten. Je nach Ausgestaltung des Systems kann ein solches System die Personalbedarfsplanung, Personaleinsatzplanung, Personalentwicklungsplanung, Personalkostenplanung sowie die Personalabrechnung und -verwaltung (Personalakte) in einem Softwarepaket bündeln und den erforderlichen Aufwand der HR-Manager deutlich reduzieren.

ten und analysieren diese IT-basiert. 36 % der Unternehmen planen die Nutzung von *Big Data* zur Optimierung der HR-Prozesse, während 9 % diese Technologie sogar schon einsetzen. Allerdings haben auch 52 % der Unternehmen noch generelle Datenschutz- und Sicherheitsbedenken und verzichten daher auf einen weitergehenden Einsatz.[26]

Bereits aus diesen Zahlen ist ersichtlich, dass die rechtliche Lage zum (Beschäftigten-)Datenschutz noch weitestgehend ungeklärt ist, weshalb Unternehmen – vor allem in Anbetracht der hohen Sanktionen nach dem neuen Datenschutzrecht, die nach Art. 83 Abs. 5 DSGVO auf bis zu 20 Mio. Euro oder 4 % des weltweiten Jahresgesamtumsatzes festgesetzt werden können – schlichtweg darauf verzichten. Sollten mit der Anwendbarkeit der DSGVO nunmehr jegliche Analysen und Prognosen im HR-Management verboten sein, so wäre dies das Aus für das moderne Personalmanagement. Dies bedeutete enorme Wettbewerbsnachteile gegenüber Wettbewerbern außerhalb der Europäischen Union, die ihr Humankapital effektiver einsetzen können.

Da Entscheidungen immer häufiger datenbasiert gefällt werden, soll im Rahmen dieser Dissertation untersucht werden, auf Basis welcher Daten Entscheidungen im HRM nach neuem Datenschutzrecht wie gefällt werden dürfen, insbesondere inwieweit eine Automatisierung bzw. Computerunterstützung im Hinblick auf Personalentscheidungen zulässig ist.

§ 2 *Interessenskonflikt im Arbeitsverhältnis*

Bevor jedoch mit der rechtlichen Analyse dieser Technologien begonnen werden kann, sollen für das bessere Verständnis der Materie zunächst die Interessen der jeweiligen Parteien an der Nutzung bzw. dem Schutz der Daten dargestellt werden, um in Abwägungsfällen diese besser einordnen und bewerten zu können. Im Arbeitsverhältnis besteht grundsätzlich ein Interessenskonflikt: Der Arbeitgeber hat vor Beginn des Arbeitsverhältnisses kaum bis gar keine Informationen über den Arbeitnehmer und umgekehrt. Lediglich die von der jeweiligen Partei zur Verfügung gestellten Informationen können im Vorfeld ausgewertet werden, wobei auch hier moderne Plattformen und Tools helfen, weitere Informationen zu beschaffen. So nutzen Arbeitgeber inzwischen soziale Netzwerke, um mehr über die Bewerber herauszufinden, während sich Arbeitnehmer auf Arbeitge-

26 Vgl. *Bitkom Research GmbH/LinkedIn Deutschland, Österreich, Schweiz*, "Big Data" verändert das Personalwesen nachhaltig.

berbewertungsportalen wie *kununu*[27] informieren können. Hinzu kommt, dass beiden Seiten daran gelegen ist, nur positive Informationen über sich selbst Preis zu geben, während negative Aspekte möglichst unter den Tisch gekehrt werden sollen. Hierauf soll im Folgenden jedoch nochmals näher eingegangen werden.

I. Asymmetrische Informationsverteilung im Arbeitsverhältnis

Auf dem Arbeitsmarkt sowie im Arbeitsverhältnis besteht grundsätzlich ein Informationsgefälle zwischen Arbeitgeber und (potenziellem) Arbeitnehmer, welches zu einer sog. *Adverse Selection* bei Vertragsschluss bzw. zum Auftreten von *Moral Hazard* nach Vertragsschluss führen kann. Beides sind Begriffe aus der Verhaltensökonomik, einem Teilgebiet der Volkswirtschaftslehre.[28]

1. Prinzipal-Agenten-Theorie

Die Prinzipal-Agenten-Theorie versucht die Probleme, die durch das Informationsgefälle entstehen, zu beschreiben. Der Prinzipal ist dabei eine Person bzw. Organisation (hier: der Arbeitgeber) für die der Agent (hier: der Arbeitnehmer) eine Handlung durchführt. Der Agent hat Informationen, über die der Prinzipal nicht verfügt. Dieser versucht an diese Informationen zu kommen.[29] Diese ungleiche Informationsverteilung führt dazu, dass das optimale Gleichgewicht zwischen Arbeitsangebot und -nachfrage nicht erreicht wird und nur sog. „Second-best-Lösungen" erzielt werden.[30] Beispielsweise wird im Rahmen des Bewerbungsverfahrens ein Bewerber ausgewählt, der nicht die optimale Besetzung für die Stelle ist bzw. erhält der Arbeitnehmer während des Beschäftigungsverhältnisses zu viel Lohn für die verrichtete Arbeitsleistung. Hierbei weiß der Arbeitnehmer besser

27 *kununu* gehört zum beruflichen sozialen Netzwerk XING und ermöglicht es Mitarbeitern und Bewerbern ihre Arbeitgeber anonym zu bewerten, Angaben zum Betriebsklima, Gehalt, zu den Vorgesetzen etc. zu machen. Somit haben potenzielle Kandidaten für eine neue Stelle die Möglichkeit, von dritter Stelle etwas mehr über das Unternehmen im Vorfeld zu erfahren.

28 Vgl. *Mankiw/Taylor*, Grundzüge der Volkswirtschaftslehre, S. 371 ff.

29 *Mankiw/Taylor*, Grundzüge der Volkswirtschaftslehre, S. 371.

30 Vgl. *Hochhold/Rudolph*, Principal-Agent-Theorie, in: Schwaiger/Meyer, Theorien und Methoden der Betriebswirtschaft, S. 135.

als sein Arbeitgeber, wie sehr er sich bei seiner Arbeit anstrengt, welche Fähigkeiten er hat etc.[31] Der Arbeitgeber versucht, an diese Information zu gelangen, um den optimalen Arbeitnehmer auszuwählen bzw. den leistungsäquivalenten Lohn zu bezahlen. Dafür werden immer häufiger Tools eingesetzt, die das Internet (und somit auch soziale Netzwerke) nach Informationen über den Bewerber durchsuchen, um somit ein möglichst umfassendes Bild („Profil") vom Bewerber zu erhalten.

2. Adverse Selection

Ein Begriff aus der Prinzipal-Agenten-Theorie ist die sog. *Adverse Selection*. Diese tritt auf, wenn ein Agent vor Vertragsschluss mehr Information über seine eigene Situation hat als der Prinzipal und dies schlussendlich dazu führt, dass der Prinzipal keinen Vertrag mit dem Agenten abschließen möchte, da der Agent möglicherweise einen höheren Preis als angemessen verlangt.[32] Ohne die Möglichkeit, sich Informationen über den Agenten zu beschaffen, führt dies dazu, dass Arbeitgeber lediglich Lohnangebote abgeben in Höhe der durchschnittlich erwarteten Leistung der Arbeitnehmer; gute Arbeitnehmer sind zu diesem Preis nicht bereit zu arbeiten, weshalb sich nur noch Agenten mit unterdurchschnittlicher Leistung auf dem Markt befinden und der Markt im Worst-Case-Szenario zusammenbricht.[33] Um diese negative Auslese zu verhindern, gibt es verschiedene Möglichkeiten Informationsasymmetrie zu beseitigen. Für die potenziellen Arbeitnehmer besteht ein Anreiz durch *Signaling*, also dem Übermitteln von privaten Informationen mit dem Ziel, dem Arbeitgeber ihre Fähigkeiten zu vermitteln. Umgekehrt führt der Arbeitgeber ein *Screening* durch. Er versucht also möglichst viele Informationen über den Bewerber einzuholen bspw. durch Fragebögen, Tests, Vereinbarung einer Probezeit etc.[34]

In der modernen Arbeitswelt erstellen Arbeitnehmer daher Profile auf beruflichen sozialen Netzwerken, die dann entweder durch Head Hunter oder durch Personalverantwortliche bei den Unternehmen schnell gefunden werden können. So gibt es beispielsweise beim Netzwerk *LinkedIn*

31 *Mankiw/Taylor*, Grundzüge der Volkswirtschaftslehre, S. 372.
32 *Mankiw/Taylor*, Grundzüge der Volkswirtschaftslehre, S. 374.
33 *Hochhold/Rudolph*, Principal-Agent-Theorie, in: Schwaiger/Meyer, Theorien und Methoden der Betriebswirtschaft, S. 137.
34 Vgl. *Hochhold/Rudolph*, Principal-Agent-Theorie, in: Schwaiger/Meyer, Theorien und Methoden der Betriebswirtschaft, S. 138.

die Möglichkeit, Empfehlungen von bisherigen Arbeitskollegen und Vorgesetzten einzuholen und auf seine Seite zu setzen, um durch *Signaling* dem Arbeitgeber positive Informationen über sich selbst, die durch Dritte generiert wurden, zu vermitteln. Dies erfolgt mit dem Ziel, die *Adverse Selection* zu vermeiden und somit die gewünschten Stellen und Gehälter angeboten zu bekommen. Im Rahmen des *Screenings* werden diese Informationen durch die Arbeitgeber genutzt.[35]

3. Moral Hazard

Das Beschäftigungsverhältnis ist ein „klassisches Beispiel für Moral Hazard"[36]. *Moral Hazard* bedeutet „moralische Versuchung" und umschreibt das Problem, dass eine Person, deren Verhalten unzulänglich beobachtbar ist, dazu neigt, sich unehrlich oder auf andere Weise unerwünscht zu verhalten. Gerade bei Arbeitnehmern besteht hier die Versuchung, sich um die arbeitsvertraglichen Pflichten zu drücken.[37] Dieser Moral Hazard kann einerseits dadurch beseitigt werden, dass Arbeitgeber Anreize schaffen, mehr und/oder effizienter zu arbeiten wie beispielsweise durch eine Zahlung eines hohen Lohnes oder durch die Einführung einer variablen bzw. erfolgsabhängigen Vergütung. Andererseits kann der Arbeitgeber durch stärkere Überwachung (sog. *Monitoring*[38]) bei gleichem Lohnniveau dagegenwirken oder die verschiedenen Ansätze kombinieren.

Gerade das *Monitoring* durch Arbeitgeber wird mit der zunehmenden Digitalisierung der Arbeit einfacher: Elektronische Geräte erfassen automatisiert (Nutzungs-)Daten, die von Arbeitgebern ausgewertet werden, um festzustellen, welche Leistung der jeweilige Arbeitnehmer erbringt. Durch den Vergleich mit anderen Arbeitnehmern kann festgestellt werden, ob hier ein „Underperforming" vorliegt und somit auch der *Moral Hazard*, beispielsweise ausgelöst durch *Adverse Selection*, Niederschlag findet. Entgegenwirken können Arbeitgeber dem Problem im laufenden Beschäfti-

35 Die Nutzung von Daten in beruflich orientierten sozialen Netzwerken durch Arbeitgeber ist zulässig, da Arbeitnehmer diese Informationen ja gerade dort veröffentlichen, um von Arbeitgebern gefunden zu werden, vgl. hierzu auch *Göpfert/Dußmann*, NZA-Beilage 2016, 41 (43 f.).

36 *Mankiw/Taylor*, Grundzüge der Volkswirtschaftslehre, S. 373.

37 *Mankiw/Taylor*, Grundzüge der Volkswirtschaftslehre, S. 373.

38 *Hochhold/Rudolph*, Principal-Agent-Theorie, in: Schwaiger/Meyer, Theorien und Methoden der Betriebswirtschaft, S. 139; vgl. auch WHWS/*Geiger*, Teil A. VI. Bedrohung des Persönlichkeitsrechts des Arbeitnehmers, Rn. 16.

gungsverhältnis dadurch, dass sie an das *Monitoring* rechtliche oder tatsächliche Folgen knüpfen. Hier können erfolgsbezogene Boni, variable Vergütung bis hin zu Versetzungen und Kündigungen bei Unterschreitung gewisser Schwellenwerte als Beispiele genannt werden.

II. Die unterschiedlichen Interessen der Parteien

Es wurde bereits herausgearbeitet, dass die Parteien des Arbeitsvertrags das Interesse haben, gewisse Informationen zurückzuhalten und andere wiederum Preis zu geben. Worin das Informationsinteresse des Arbeitgebers und das Geheimhaltungsinteresse des Arbeitnehmers genau liegt und welchen Ursprung diese Interessen haben, soll im Folgenden nochmals detailliert dargestellt werden.

1. Das Informationsinteresse des Arbeitgebers

Das Informationsinteresse des Arbeitgebers ist vielseitig. Einerseits sind Arbeitgeber gezwungen, persönliche Daten zu erheben, um diese an die staatliche Verwaltung weiterzugeben (z.B. für die Erhebung der Lohnsteuer, Sozialversicherung etc.). Bereits 1985 wurde von *Peters* festgestellt, dass sich aus 113 Gesetzen und Verordnungen die Verpflichtung des Arbeitgebers ergibt, insgesamt 75 verschiedenen staatlichen Datenempfängern Arbeitnehmerdaten zukommen zu lassen.[39] Dieser Informationsverpflichtung möchten die Arbeitgeber möglichst kostengünstig nachkommen, indem sie IT-Systeme einsetzen.[40]

Andererseits hat der Arbeitgeber auch ein Interesse, seine Arbeitnehmer möglichst effizient, d.h. nach ihren Fähigkeiten, Kenntnissen sowie ihren (persönlichen) Stärken und Schwächen entsprechend, auf dem optimalen Arbeitsplatz einzusetzen und somit *Moral Hazard* zu vermeiden.[41] Aus Sicht des Arbeitgebers ist der Arbeitnehmer ein Produktionsfaktor, der optimal „verwendet" werden muss. Die Folge ist eine Schematisierung der Anforderungen an den einzelnen Arbeitnehmer, die mithilfe automa-

39 *Peters*, DSWR 1985, 186 (188).
40 *Walz*, Mitbestimmung 1986, 292 (294).
41 Zur Personaloptimierung als Teil des Rechts auf unternehmerische Freiheit, vgl. auch *Götz*, Big Data im Personalmanagement, S. 17.

tisierter Verarbeitung möglichst effizient erfolgen soll.[42] Durch die elektronische Datenverarbeitung sinken die Transaktionskosten des Arbeitgebers im Hinblick auf die Datengewinnung und -verarbeitung enorm, sodass die Begrenzung des Informationsinteresses durch Kosten praktisch weggefallen ist. Bestes Beispiel hierfür ist die Videoüberwachung von Beschäftigten: Der Arbeitgeber kann sehr einfach ohne Personalkosten mit einmaligem Aufwand seine Beschäftigten lückenlos aufzeichnen,[43] mit zunehmender Speicherkapazität und sinkenden Kosten quasi über deren gesamtes „Betriebsleben".

Das Informationspotential durch die Verwendung von IT-basierten Systemen lässt sich gut für Planungszwecke nutzen, damit die Arbeitsleistung, bestmöglich auf den Arbeitsprozess bezogen, bewertet und gesteuert sowie die Arbeitsleistungen verschiedener Arbeitnehmer miteinander verglichen werden können. Hierdurch objektiviert und rationalisiert sich die Personalentscheidung.[44]

2. Das Geheimhaltungsinteresse des Arbeitnehmers

Arbeitnehmer profitieren nicht lediglich von der automatisierten Verarbeitung, da die vom Arbeitgeber gesammelten Informationen sowohl für als auch gegen den Arbeitnehmer verwendet werden können (z.B. kann ein Belastungsprofil des Arbeitnehmers für die Zuweisung eines passenden Arbeitsplatzes genutzt werden, genauso aber auch für einen Selektionsmechanismus beim Stellenabbau[45]).

Der größte Profit des Arbeitnehmers von einem Personalinformationssystem liegt darin, dass die individuelle Situation besser berücksichtigt,[46] sowie mögliche noch unbekannte Störfaktoren (z.B. nicht eine funktionierende oder anders gelebte Hierarchie im Unternehmen[47]) durch Big Data-Auswertungen identifiziert und aus dem Weg geräumt werden können.

Arbeitnehmer haben also ein Interesse, gewisse Informationen über sich Preis zu geben, um die eigene Arbeitssituation zu verbessern. Nicht außer Acht gelassen werden darf allerdings, dass Beschäftigte ein ebenso großes

42 *Simitis*, in: FS Coing 70, S. 495 (500).
43 *Franzen*, ZfA 2012, 172 (174 f.).
44 *Simitis*, in: FS Coing 70, S. 495 (505 f.).
45 *Simitis*, in: FS Coing 70, S. 495 (507).
46 *Simitis*, in: FS Coing 70, S. 495 (506).
47 Siehe unten, **E. § 4.**

Interesse haben, möglichst wenige persönliche Informationen preiszugeben, um ihre Privatsphäre zu schützen.[48] Das Interesse der Arbeitnehmer liegt vornehmlich darin, *selbst* die Entscheidungsgewalt darüber zu haben, welche Informationen der Arbeitgeber erhält bzw. an ihn weitergegeben werden und für welche Zwecke er diese Informationen einsetzen darf.[49] Zudem besteht ein hohes Interesse daran, nicht lückenlos überwacht und dokumentiert zu werden,[50] um nicht jede einzelne Handlung im Arbeitsalltag ggf. rechtfertigen zu müssen.

3. Technikspezifische Risiken

Dieser Interessenskonflikt wird durch den Einsatz moderner IT-Technologie, bei welcher immer mehr Daten durch die Arbeitgeber gesammelt werden, verstärkt: Technologien wie Personalinformationssysteme führen zu einem deutlichen Informationsgefälle zwischen (internen) Arbeitnehmern und externen Bewerbern.[51] Der Arbeitgeber verfügt über deutlich mehr Informationen über die bereits Beschäftigten. Dies resultiert dann darin, dass dieser eher dazu neigt, interne Bewerber zu berücksichtigen als externe. Hierdurch lässt sich sowohl das Risiko der *Adverse Selection* als auch das des *Moral Hazard* verringern. Unternehmen werden daher zu einer Art „closed shops"[52], bei denen es insbesondere für externe Bewerber besonders schwierig ist, eine entsprechende Anstellung zu finden. Da Stellen jedoch vielfach nicht nur intern besetzt werden können bzw. auch „frischer Wind" ins Unternehmen gebracht werden soll, investieren Arbeitgeber in Technologien, die es ihnen ermöglichen, auch von externen Bewerbern möglichst viele Informationen zu bekommen (beispielsweise durch Recherche in sozialen Netzwerken, aber auch durch Eignungs- und Persönlichkeitstests im Rahmen der Einstellung bzw. Assessment Centern).

Weit bedenklicher und gravierender ist es jedoch, dass es durch den technischen Fortschritt möglich wurde, Arbeitnehmer quasi lückenlos zu überwachen, sei es per Videoüberwachung im Betrieb, Überwachung des betrieblichen PCs, GPS-Ortung von Fahrzeugen oder Mobiltelefonen,

48 *Franzen*, ZfA 2012, 172 (175).
49 *Schmitz*, Interessenausgleich im Beschäftigtendatenschutz, S. 32.
50 *Thüsing*, RDV 2009, 1.
51 *Simitis*, in: FS Coing 70, S. 495 (508).
52 *Däubler*, Gläserne Belegschaften, § 2 Rn. 33.

RFID-Ordnung innerhalb Gebäuden, bis hin zur Überwachung der Vitalfunktionen durch Wearables.[53] Die technischen Möglichkeiten von Arbeitgebern ihre Arbeitnehmer zu überwachen, steigen mit zunehmendem Technikfortschritt exponentiell und sind heute – zumindest aus technischer Hinsicht – nahezu grenzenlos.

Auf bestimmte Geräte wie beispielsweise Mobiltelefone, PCs oder Fahrzeuge sind die Arbeitnehmer angewiesen,[54] sodass sie keine Möglichkeit haben, einer etwaigen Überwachung zu entgehen. Da die meisten Arbeitstransaktionen mit Hilfe von entsprechenden Informations- bzw. Kommunikationssystemen digital abgebildet werden, besteht eine noch nie dagewesene Transparenz von Leistung- und Verhalten, denn jede Nutzung eines technischen Geräts hinterlässt personenbezogene Spuren (z.B. bei PCs beispielsweise Cookies, IP-Adressen etc.; bei Mobilgeräten zusätzlich noch die IMEI-Nummer[55]), die zu Verhaltens- und Leistungskontrollen verwendet werden können.[56] Dies führt dazu, dass die Arbeitgeber durch die Verknüpfung der Einzeldaten[57] genaue Persönlichkeitsprofile über ihre Arbeitnehmer erstellen können und dies oftmals – teilweise datenschutzwidrig – auch tun.[58]

Die Sammlung verschiedener Daten zum Zwecke der detaillierten Auswertung und dem Auffinden noch unbekannter Muster wird unter den Überbegriff *Big Data* gefasst.[59] Die seit dem 21. Jahrhundert vorhandene nahezu unbegrenzte Speicher- und Rechenkapazität ermöglicht es Arbeitgebern alle Daten zu erfassen und innerhalb kürzester Zeit auszuwerten – dies dank immer stärkerer Rechenkapazität zu erschwinglichen Preisen. Typische Analysemethoden in diesem Zusammenhang sind beispielsweise Online Analytical Processing (OLAP) sowie Data Mining.

Beim Data-Mining werden systematisch statistische Methoden auf große Datenbestände angewandt, um unbekannte Querverbindungen und

53 In *Gola*, Datenschutz am Arbeitsplatz werden verschiedene Überwachungssituationen aufgezählt und untersucht.
54 *Tinnefeld/Viethen*, NZA 2000, 977 (978).
55 Sog. Internet Mobile Equipment Identity; dies ist eine 15-stellige Seriennummer anhand welcher jedes Mobilgerät, welches einen SIM-Schacht hat, identifiziert werden kann. Die IMEI kann durch Eingabe von *#06# in das Wählfeld abgefragt werden.
56 Zu Datenspuren im Internet, vgl. *Köhntopp/Köhntopp*, CR 2000, 248.
57 Vgl. *Däubler*, Gläserne Belegschaften, § 2 Rn. 36.
58 *Tinnefeld/Viethen*, NZA 2000, 977 (979).
59 Zur Verwendung des Begriffs bei Beschäftigtendaten, vgl. *BMAS*, Weißbuch Arbeiten 4.0, S. 142.

Trends zu erkennen.[60] Bei OLAP hingegen wird dem System „eine Frage gestellt" bzw. eine Hypothese in den Raum gestellt, welche durch Analyse der Daten bestätigt oder widerlegt werden soll.[61]

Ein weiteres Risiko ist die einfache Übermittlung bereits gesammelter und elektronisch erfasster Daten; einmal gespeichert können die Daten unbegrenzt oft vervielfältigt und an verschiedenste Empfänger in Bruchteilen von Sekunden versandt werden.[62] Dies gilt nicht nur innerhalb eines Betriebs, sondern über das Internet auch über Betriebs- und Unternehmensgrenzen hinaus bis hin ins nicht-europäische Ausland bei multinationalen Konzernen. Nicht übersehen werden darf hierbei das Risiko von Datenpannen, bei denen unbefugte Dritte Zugriff auf die gespeicherten Informationen über die Arbeitnehmer erhalten.[63]

So bleibt festzustellen, dass die Möglichkeit der Informationsgewinnung aus Daten zwar enorme Vorteile vor allem für die Arbeitgeber, aber auch für die Arbeitnehmer bringen kann, ebenso groß jedoch auch die Risiken sind. Typisches Beispiel hierfür ist die Einführung einer Totalüberwachung als Datenmissbrauch.

III. Datenschutz als Instrument zum Interessensausgleich

Hier setzt das (Beschäftigten-)Datenschutzrecht an, welches die Zulässigkeit der Erhebung und Verarbeitung von personenbezogenen Daten regelt, und vor allem eine maßlose Datensammlung beschränkt[64] sowie Missbräuche mit Strafen belegt. Im Endeffekt stellt das Datenschutzrecht eine Kodifizierung der erforderlichen Grundrechtsabwägung zwischen den Rechten des Verarbeiters (zumeist der Arbeitgeber) sowie des Betroffenen (Arbeitnehmer) im Wege der praktischen Konkordanz dar. So bestimmt Erwägungsgrund 2 der DSGVO, dass „*die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten […] gewährleisten [sollten], dass ihre Grundrechte und Grundfrei-*

60 *Heinson/Schmidt*, CR 2010, 540 (542).
61 *Heinson/Schmidt*, CR 2010, 540 (542).
62 *Roßnagel et al.*, Datenschutz bei Wearable Computing, S. 29.
63 Vgl. jüngst eine der wohl größten Datenpannen weltweit bei welcher 24,5 Mio. hochsensible medizinische Datensätze weltweit ungeschützt zugänglich waren; hierzu *Greenbone Networks GmbH*, Sicherheitsbericht, <www.greenbone.net/wp-content/uploads/CyberResilienceReport_DE.pdf>.
64 *Heinson/Schmidt*, CR 2010, 540 (541 f.).

heiten und insbesondere ihr Recht auf Schutz personenbezogener Daten […] gewahrt bleiben."

Auf nationaler und unionaler Ebene ist das informationelle Selbstbestimmungsrecht des Beschäftigten aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG (bzw. auf unionaler Ebene das Recht auf Privatheit Art. 7 f. EU-GRC) mit dem Eigentumsrecht (Art. 14 Abs. 1 und 2 GG / Art. 17 EU-GRC), der unternehmerischen Freiheit (Art. 12 Abs. 1 GG / Art. 16 EU-GRC) sowie der Vertragsfreiheit des Arbeitgebers (Art. 2 Abs. 1 GG) in einen schonenden Ausgleich (sog. „praktische Konkordanz") zu bringen.[65] Das immer zu berücksichtigende Kriterium der Erforderlichkeit (§ 26 Abs. 1 BDSG) ist letztlich eine Ausprägung der Grundrechtsabwägung um die Verhältnismäßigkeit zu sichern. Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten muss geeignet und gleichzeitig das mildeste Mittel darstellen, um die unternehmerischen Interessen und Zwecke bei der Durchführung des Beschäftigtenverhältnisses zu verwirklichen. Wo immer möglich, gilt es, so die Datensammlung auf ein Minimum zu begrenzen.[66] Dies ergibt sich ebenfalls aus Art. 5 Abs. 1 lit. c DSGVO, wonach personenbezogene Daten auf das für Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen (Grundsatz der Datenminimierung).

Gerade im Beschäftigtendatenschutz hat die jahrelange Rechtsprechung des BAG nunmehr ein sehr diffiziles Regelungsregime zur Generalklausel des § 32 BDSG a.F. geschaffen, welches zu einem gerechten Ausgleich der widerstreitenden Interessen führen soll. Diese Rechtsprechungsgrundsätze sollen nach dem Willen des Gesetzgebers auch mit Inkrafttreten der DSGVO weiterhin Anwendung finden.[67] Allerdings bringen neue Technologien – wie beispielsweise *Big Data* – mitunter große (technikspezifische) Risiken, die bislang in der Rechtsprechung kaum behandelt wurden, bereits in naher Zukunft sicherlich zum Alltag der täglichen Judikatur gehören werden.

IV. Zwischenergebnis

Wie die Ausführungen zeigen, herrschen – gerade im Beschäftigungsverhältnis – immer Interessensgegensätze zwischen der verarbeitenden Stelle

65 *Brink/Schwab*, RDV 2017, 170 (172).
66 *Brink/Schwab*, RDV 2017, 170 (172 f.).
67 Vgl. BT-Drs. 18/11325, S. 97.

(Arbeitgeber) und dem Betroffenen (Arbeitnehmer), die durch das (Beschäftigten-)Datenschutzrecht in einen gerechten Ausgleich gebracht werden müssen. Nicht jede Datenerhebung und -verarbeitung führt zwangsweise zu einem Nachteil für den Arbeitnehmer. Die erhobenen Daten können durchaus zum Vorteil des Arbeitnehmers eingesetzt werden. Teilweise ist der Arbeitgeber „als verlängerter Arm des Staates" sogar dazu verpflichtet, Daten zu erheben und an die entsprechenden staatlichen Stellen wie beispielsweise die Finanzverwaltung weiterzuleiten. Das Beschäftigtendatenschutzrecht darf daher nicht als reines Abwehrrecht des Arbeitnehmers gegen die Datenerhebung und -verarbeitung durch den Arbeitgeber gesehen werden, sondern soll vielmehr Missbrauchsfälle verhindern und eine möglichst weitgehende Grundrechtsverwirklichung der einzelnen Parteien ermöglichen.[68] Bei jedem einzelnen Verarbeitungsvorgang müssen daher die Interessen aller Beteiligten und die Gefahren für die Grundrechte genau durchleuchtet werden, bevor pauschal ein Urteil gefällt wird. Bereits aus der Eigenschaft der tangierten Grundrechte als Individualschutzrechte folgt, dass immer Einzelfallgerechtigkeit herzustellen ist.

68 So bestimmt bereits Art. 1 Abs. 3 DSGVO, dass der freie Verkehr personenbezogener Daten aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Union weder eingeschränkt noch verboten werden darf.

B. Die Entwicklung des Personalmanagements

§ 1 Ursprünge des Personalmanagements

Das Personal war nicht immer eine Ressource von hoher Bedeutung für ein Unternehmen. Bis Anfang der 1960er Jahre wurden die Mitarbeiter nicht in die Unternehmensstrategie einbezogen, sodass sich das ursprüngliche Personalwesen auf die Bereitstellung gesunder und günstiger Arbeitskräfte beschränkte und lediglich die kaufmännische Verwaltung übernahm. Den Begriff des „Personalmanagements" gibt es seit ungefähr Mitte der 1960er Jahre.[69] Seit diesem Zeitpunkt wurde das Personal in der Strategieplanung immer wichtiger. Es bestand das Ziel, das Personal an die komplexeren organisatorischen Anforderungen anzupassen (sog. Institutionalisierung). Personalarbeit wurde zentralisiert und Personalverantwortliche dafür ausgebildet. Bildung, Freizeit und Arbeitsplätze als qualitative Sozialpolitik wurden zunehmend wichtigere Faktoren in der Personalarbeit.[70] Der Arbeitnehmer wurde nicht mehr nur als Arbeitskraft gesehen, sondern auch seine weiteren sozialen Bedürfnisse rückten mehr in den Fokus.

§ 2 Wandel des Personalmanagements über die Zeit

Im Rahmen der Humanisierung der Arbeit kamen von der amerikanischen Human-Relations-Bewegung Anfang der 1970er Jahre starke Impulse, die Organisationen menschenfreundlicher zu gestalten und den einzelnen Arbeitnehmer mit seinen Gefühlen, Bedürfnissen und Werten zu betrachten. Die Perspektive änderte sich von einer Anpassung des Menschen an die Organisation um 180 Grad zu einer Anpassung der Organisation an den Menschen. Schlagworte wie Mitarbeiterorientierung oder kooperative Führung kamen auf. Mitarbeiterzufriedenheit wurde zum obersten Ziel.[71]

Erst ab den 1980er Jahren dominierte die Ökonomisierung die Strategie. Die Organisation als auch das Personal mussten aufgrund des zuneh-

---

69 *Wunderer/Dick/Jäger*, Personalmanagement - quo vadis?, S. 50.
70 Zum Ganzen: *Wunderer/Dick/Jäger*, Personalmanagement - quo vadis?, S. 50 f.
71 *Wunderer/Dick/Jäger*, Personalmanagement - quo vadis?, S. 51 f. m.w.N..

menden Marktdrucks wirtschaftlicher gestaltet werden. Ausgelöst durch häufige Stellenwechsel und einem Mangel an qualifizierten Arbeitskräften, war es Unternehmen nicht mehr möglich, ihre strategischen Ziele zu erreichen, weshalb die Personalstrategie in die Unternehmensstrategie integriert und mit dieser verknüpft werden musste. Die Unternehmen wurden aufgrund von Globalisierung und Digitalisierung vor neue Herausforderungen gestellt und das Management mehr auf eine unternehmerische Orientierung ausgerichtet: Der einzelne Arbeitnehmer wandelte sich „ein Stück weit" vom Mitarbeiter zum Mitunternehmer.[72]

Erste Softwaresysteme für das Personalmanagement kamen sodann in den 1990er Jahren auf (z.B. PeopleSoft, NCR/Teradata und Oracle),[73] beschränkten sich jedoch darauf, die wichtigsten Personaldaten zu erfassen, um den Überblick über die Beschäftigten zu behalten. Allerdings blieb der Absatz dieser Systeme gering, da die Unternehmen oftmals keine größeren Investitionen in solche Systeme tätigten und bereits sehr komplexe HR-Systeme im Einsatz hatten.[74] Erst um die Jahrtausendwende begannen die Softwarehersteller „HR-Analyse"-Systeme zu schaffen, die eine umfassende Sammlung von Daten vorhersahen. Diese sollte dem Management über simple Auswertungen einen Überblick über die wichtigsten Zahlen der Belegschaft zur Verfügung stellen (z.B. Gesamtbeschäftigtenanzahl, Dauer des Bewerbungsverfahrens, Fluktuationsquote etc.) und vor allem die bislang oftmals chaotisch und ungenau geführten Personalakten in eine gepflegte und aktuelle Datenbank überführen.[75]

Mit dem Aufkommen von sozialen Netzwerken wie Facebook, Google (Plus), LinkedIn etc. kamen neue Analysesysteme wie beispielsweise Hadoop, R u.ä. auf, die es ermöglichten, große (unstrukturierte) Datenmengen in kürzester Zeit zu verarbeiten. *Big Data* wurde das neue zentrale Thema bei Datenanalysen.[76] Erstmals wurde es möglich, verschiedenste Datenquellen miteinander zu verknüpfen, sodass nicht nur noch Daten

72 *Wunderer/Dick/Jäger*, Personalmanagement - quo vadis?, S. 52 f. m.w.N..
73 *Holthaus/Park/Stock-Homburg*, DuD 2015, 676 (677).
74 *Bersin*, The Geeks Arrive in HR: People Analytics Is Here, 2015, abrufbar unter: https://www.forbes.com/sites/joshbersin/2015/02/01/geeks-arrive-in-hr-people-analytics-is-here/ (letzter Abruf am: 17.10.2017).
75 *Bersin*, The Geeks Arrive in HR: People Analytics Is Here, 2015, abrufbar unter: https://www.forbes.com/sites/joshbersin/2015/02/01/geeks-arrive-in-hr-people-analytics-is-here/ (letzter Abruf am: 17.10.2017).
76 *Bersin*, The Geeks Arrive in HR: People Analytics Is Here, 2015, abrufbar unter: https://www.forbes.com/sites/joshbersin/2015/02/01/geeks-arrive-in-hr-people-analytics-is-here/ (letzter Abruf am: 17.10.2017).

aus dem Personalmanagement Grundlage für Entscheidungen sein mussten, sondern auch aus anderen Business Units miteinbezogen werden konnten bis hin zur Auswertung bereits vorhandener Online-Netzwerke.[77]

Deutlich umfassendere Analysen wurden somit durchführbar und der Begriff der *People Analytics* geboren. Mit diesen neuen Technologien ist es Unternehmen möglich, auf Basis umfassender Daten Zusammenhänge zu erkennen, die bislang – dadurch bedingt, dass die Mitarbeiter in verschiedenen Business Units mit unterschiedlichen Vorgesetzten arbeiten und daher der Informationsfluss zum HR oftmals nicht einwandfrei funktioniert – nicht einmal erahnt werden konnten.

In Deutschland steckt *People Analytics* jedoch noch in den Kinderschuhen.[78] Erste *People Analytics*-Projekte laufen gerade erst an, Expertengruppen werden gebildet und Einsatzmöglichkeiten im Unternehmen geprüft. Kennzahlen- und HR-Reporting-Systeme sind zwar schon häufig im Einsatz, allerdings lassen sich hierdurch derzeit weder betriebswirtschaftliche Folgen direkt ableiten noch Ursachen für Veränderungen aufdecken. Es mangelt an weitergehenden Analysen.[79]

Die Rechtsunsicherheit im Bereich des Datenschutzes – vor allem im Hinblick auf Vorgaben der DSGVO – bremst die Entwicklung in diesem Bereich derzeit sehr stark. People Analytics-Suites existieren bereits einige. Als anschauliche Beispiele können hier u.a. Microsoft Office Delve[80], das IBM Personal Social Engangement Dashboard[81], SAP SuccessFactors[82] oder das vor allem in den USA bekannte Tool Workforce Ready HR

77 *Holthaus/Park/Stock-Homburg*, DuD 2015, 676 (677).

78 So auch *Atabaki/Biemann*, Potenziale der Datenanalyse für HR (People Analytics), in: Petry/Jäger, Digital HR, S. 134: "Die vorherrschende Personalpraxis in Deutschland ist derzeit noch von einer systematischen strategischen Analyse von Mitarbeiterdaten entfernt.".

79 *Atabaki/Biemann*, Potenziale der Datenanalyse für HR (People Analytics), in: Petry/Jäger, Digital HR, S. 134.

80 https://support.office.com/de-de/article/was-ist-office-delve-1315665a-c6af-4409-a28d-49f8916878ca (letzter Abruf am: 22.05.2018).

81 http://www-935.ibm.com/services/services-offerings/pdf/Intro-Social-Engagement-Dashboard(1).pdf (letzter Abruf am: 22.05.2018).

82 https://www.sap.com/germany/products/human-resources-hcm/workforce-planning-hr-analytics.html (letzter Abruf am: 19.09.2019).

des Herstellers Kronos[83] genannt werden. Viele davon werden noch nicht eingesetzt, weil datenschutzrechtliche Bedenken bestehen.[84]

§ 3 Neue Chancen und Herausforderungen durch die Digitalisierung

In Deutschland sehen derzeit die Personalverantwortlichen das größte Veränderungspotential durch die Digitalisierung im HRM bei Social Media, gefolgt von mobilen Anwendungen und Data-Analytics sowie Cloud-Anwendungen. „Zukunftsweisende Treiber" wie *People Analytics* finden bislang noch keine Berücksichtigung in den Top 5-Treibern.[85]

International und branchenübergreifend wird das Thema Data Analytics an erster Stelle der wichtigsten Digitaltechnologien gesehen.[86] Data Analytics ist eine notwendige, aber nicht hinreichende Bedingung für den Einsatz von *People Analytics*.

I. Soziale Medien

Soziale Medien werden hingegen vor allem dazu genutzt, um die Unternehmensbekanntheit zu steigern, die Arbeitgebermarke aufzubauen und Bewerbungen zu generieren bzw. potenzielle Mitarbeiter aktiv anzusprechen (sog. *Active Sourcing*). Sie dienen ebenfalls dazu, die interne Kommunikation und Zusammenarbeit zu verbessern und die Mitarbeitermotivation zu erhöhen.[87] Hierbei ist zwischen unternehmensinternen sozialen

---

83 https://www.kronos.com/products/workforce-ready-suite/workforce-ready-hr (letzter Abruf am: 19.09.2019).

84 Vgl. beispielsweise das Gutachten des hessischen Datenschutzbeauftragten zur Unzulässigkeit des Einsatzes von Office 365 an Schulen, *Der Hessische Beauftragte für Datenschutz und Informationsfreiheit*, Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft Office 365 in hessischen Schulen, 09.07.2019, abrufbar unter: https://datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-f%C3%BCr-datenschutz-und (letzter Abruf am: 03.06.2020); vgl. ferner *Raif/Swidersky*, GWR 2017, 351 (351, 354).

85 *Kienbaum Institut @ ISM*, Digitalisierung@HR - Strukturen, Prozesse & Kompetenzen der Zukunft, <www.yumpu.com/de/document/read/56587003/digitalisierunghr-strukturen-prozesse-kompetenzen-der-zukunft>; *Jochmann/Belch*, Personalführung 2016, 58 (62).

86 *Jäger/Petry*, Digital HR - Ein Überblick, in: Petry/Jäger, Digital HR, S. 33 f.

87 *Jäger/Petry*, Digital HR - Ein Überblick, in: Petry/Jäger, Digital HR, S. 36.

Netzwerken (wie beispielsweise „workplace by facebook“[88], aber auch Kollaborationstools wie Slack[89] oder Microsoft Teams[90]) sowie unternehmensexternen Netzwerken (XING[91], LinkedIn[92], Facebook[93] etc.) zu unterscheiden. Während die berufsbezogenen Netzwerke XING und LinkedIn von Arbeitgebern unproblematisch zur Bewerbersuche genutzt werden dürfen, da die Nutzer ihre Daten ja gerade deshalb einstellen, um von Unternehmen gefunden zu werden, ist bei den freizeitbasierten sozialen Netzwerken wie Facebook u.ä. ein *Active Sourcing* kritisch zu betrachten.[94]

II. Mobile Media

Unterstützt werden Data Analytics durch die Nutzung von Mobile Media, welche es ermöglichen, immer mit dem Human Ressource Management verbunden zu sein bzw. die Informationen direkt an den Endbenutzer weiterzuleiten (z.B. durch Apps, mobile Websites, Location Based Services, Chat-Bots etc.).[95] Hierbei fällt eine Menge an Transaktions- und Telemetriedaten an, die für den Benutzer unsichtbar sind, aber für Auswertungen genutzt werden können. Viele der genannten Softwarelösungen (wie SuccessFactors von SAP oder Workforce Ready HR von Kronos) bieten den Arbeitnehmern und Bewerbern die Möglichkeit, die gesamte Kommunikation mit dem HR vollständig vom Smartphone abzuwickeln, Krankmeldungen digital einzureichen, Urlaub in der App zu beantragen oder

88 https://web.facebook.com/workplace?source=topbar&ref=AVv7xfYYE0MsHvK7S67OzyLqIPBNBY09t_nEPfsWnzGRWBsQSg46aS1QaPEk4pJMpe_7szay_THNubKxPuw3fRnsipZBLGqhRLvVK0yb3bG2Ii3SX8_pv2Ar-7h0XPJ-2QT_FW_l_aTGqdYr6NGOHzaOoDrJHwhxZzRJM5azO5gxVJJDDtSIc3gqW6kCeM0z3BZX_3wyvzxqtXVdPvFyYbMaaWXA5QemUkgs3mh_8otieg (letzter Abruf am: 19.09.2019).

89 Der Werbeslogan von Slack lautet: „Slack bietet deinem Team einen zentralen Ort für Koordination und Kommunikation, damit ihr alle euer Bestes geben könnt.“, vgl. https://www.slack.com (letzter Abruf am: 19.09.2019).

90 „Teams bündelt alles Wichtige an einem Ort. So können Sie praktisch überall produktiv sein und ganz einfach im Team chatten, Dateien gemeinsam bearbeiten und in Ihren bevorzugten Anwendungen arbeiten.“, https://products.office.com/de-de/microsoft-teams/free (letzter Abruf am: 19.09.2019).

91 www.xing.com.

92 www.linkedin.com.

93 www.facebook.com.

94 Instruktiv hierzu *Forst*, NZA 2010, 427; *Kort*, DuD 2012, 722 (beide noch zum alten Datenschutzrecht).

95 *Jäger/Petry*, Digital HR - Ein Überblick, in: Petry/Jäger, Digital HR, S. 38 f.

schnell eine Schicht mit einem geeigneten Arbeitskollegen zu tauschen. Dies verspricht große Vorteile für die Arbeitnehmer, aber auch für die Arbeitgeber in puncto Effizienz und Komfort. Hierbei muss jedoch darauf geachtet werden, dass sich solche Apps nicht als „Trojaner für die Privatsphäre" entpuppen, indem die anfallenden Verkehrsdaten dazu genutzt werden, die Arbeitnehmer auf Schritt und Tritt zu überwachen und deren Aktivitäten zu tracken.

III. Cloud-Dienste

Damit diese mobilen Apps funktionieren, aber auch andere Daten weltweit in Sekundenschnelle abgerufen werden können, ist es zweckmäßig bzw. für viele Anwendungen sogar erforderlich, dass die Daten in der Cloud bereitgestellt werden. Somit können die mobilen Anwendungen nicht nur im unternehmensinternen Netzwerk, sondern auch von unterwegs oder zuhause aufgerufen und etwaige Prozesse schnell und effizient durchgeführt werden. Die Bereitstellung von Daten in der Cloud bedeutet nichts anderes als die Anbindung der Datenserver an das Internet und somit die Freigabe des Zugriffs auch außerhalb unternehmens- bzw. konzerninterner Netzwerke. Durch immer schneller werdende Internetverbindungen in Kombination mit dieser Technologie können Standort- (wie günstigere Betriebs- und Wartungskosten[96]) oder auch Skalierungsvorteile (z.B. Betrieb mehrerer virtueller Server-Instanzen auf einem leistungsstärkeren physischen Server) genutzt werden. Ebenso lässt sich eine Redundanz der Systeme schaffen, um die Ausfallsicherheit zu erhöhen. Durch die Möglichkeit der dynamischen Zuteilung von Hardware-Ressourcen ist es so aber auch möglich, mit Hilfe intelligenter Zeitplanung bei der Ausführung der Aufgaben, umfassende Auswertung innerhalb kürzerer Zeit durchzuführen, ohne dass sich einzelne Unternehmen hierfür leistungsstarke Server kaufen müssen. Hierdurch werden vorhandene Rechenkapazitäten besser ausgenutzt und damit die Effizienz der Systeme gesteigert.

96 Viele Unternehmen betreiben ihre Server im Ausland, um Strom- und Personalkosten zu sparen. Durch schnelle Internetverbindungen erleiden die Endnutzer hierdurch keine Nachteile. Problematisch ist dies, wenn Server außerhalb der EU in Ländern mit einem niedrigeren Datenschutzstandard als Deutschland betrieben werden (siehe insofern die Schutzvorschriften in der DSGVO, Art. 44 ff.).

IV. „Internet of Things“ (IoT)

Gerade bei der Nutzung von IoT[97]-Geräten wie Wearables[98] fallen eine Vielzahl von Sensordaten in Echtzeit an. Diese könnten im Bereich des Human Ressource-Managements für Maßnahmen des Gesundheitsmanagements oder aber auch für eine umfassende Leistungs- und Verhaltenskontrolle der Mitarbeiter genutzt werden.[99] So wurde in Studien festgestellt, dass der Einsatz von Fitness Wearables die Produktivität bis zu 8,5 % und die Jobzufriedenheit bis zu 3,5 % steigern kann. Noch besser sieht es beim Einsatz von Google Glass[100] in der Logistikbranche aus: Hier wurden Produktivitätssteigerungen von 25 % gemessen.[101]

Für die effektive Nutzung dieser Daten benötigt es hohe Speicherkapazitäten (Stichwort: *Cloud* bzw. *Big Data*) und leistungsstarke Hardware, um die Menge der Daten in einer solchen Geschwindigkeit auswerten zu können, sodass auf eventuelle Problemdaten rechtzeitig reagiert werden kann. Würde man beispielsweise die Pulsdaten von Lageristen aufzeichnen, so könnte man anhand erhöhter Pulswerte feststellen, dass ein Arbeitnehmer derzeit etwas (zu) Schweres hebt. Im Sinne des präventiven Gesundheitsmanagements könnte ein Arbeitgeber veranlasst sein, solche Situationen zu vermeiden und einen anderen Mitarbeiter auf seiner Smart Watch benachrichtigen, dass dieser dem Kollegen zur Hilfe eilen soll. Hierzu bedürfte es eines Trackings in Echtzeit auf einem zentralisierten Server,

---

97 Begriff für den Anschluss alltäglicher Geräte wie beispielsweise Uhren, Kleidung, Maschinen und Geräte aber auch PKWs und Messgeräte an das Internet, um in Echtzeit Zugriff auf die Daten zu erhalten und Auswertungen durchzuführen.

98 Wearables werden am Körper getragen bzw. sind in körpernahe Gegenstände integriert und unterstützen den Menschen in verschiedenster Weise, ohne dass es hierfür eine Daten- oder Befehlseingabe benötigt, vgl. *Mülder*, Überblick zu Potentialen neuer Technologien für HR, in: Petry/Jäger, Digital HR, S. 114 Hierzu zählen beispielsweise Smart Watches, Fitness-Tracker, Smart Glasses usw.

99 *Jäger/Petry*, Digital HR - Ein Überblick, in: Petry/Jäger, Digital HR, S. 40.

100 Google Glass ist ein Wearable in Form einer Brille, die es dem Träger ermöglicht, Informationen im Sichtfeld angezeigt zu bekommen, Fotos und Videos aufzunehmen und zu telefonieren. Die aktuelle Brille ist dabei mit einem Vier-Kern-Prozessor ausgestattet, besitzt eine 8 MP-Kamera und wird mit Bluetooth mit dem Handy oder mittels Wifi direkt mit dem Internet verbunden. Siehe https://www.google.com/glass/start/ (letzter Abruf 05.03.2020).

101 *Blinn*, Wearables und Arbeitnehmerdatenschutz - Vom freiwilligen Selbstoptimierer zum Kontrollinstrument des Arbeitgebers?, in: Taeger, Smart world - smart law?, S. 521 f. m.w.N. zu den einzelnen Studien.

um festzustellen, welcher Arbeitnehmer gerade „frei" ist und deshalb ihm zur Hand gehen könnte. Würden die Daten nur abends oder stündlich synchronisiert und ausgewertet, könnte man zwar langfristig darauf reagieren, wenn einzelne Arbeitnehmer überbelastet sind, aber nicht in der konkreten Situation.

Gerade solche Einsatzszenarien (ob Echtzeiterfassung oder auch nur tägliche) sind im Hinblick auf den Datenschutz und das Persönlichkeitsrecht der Arbeitnehmer höchst problematisch. Arbeitnehmer könnten sich einem dauernden Überwachungsdruck ausgesetzt sehen, obwohl im konkret genannten Beispiel das Gesundheitstracking zum Vorteil der Arbeitnehmer genutzt würde.

Dass eine solche Überwachung der (Vital-)funktionen keine Science-Fiction ist, bestätigen Berichte aus der Presse: So berichteten Redakteure der britischen Tageszeitung „The Telegraph", dass unter ihren Schreibtischen Sensoren zur Anwesenheitserkennung angebracht wurden. Der Energiekonzern BP verteilte 25.000 Fitnesstracker unter seinen Mitarbeitern, die kontinuierlich Vitaldaten wie Herzfrequenz, Schrittfrequenz und Schlafverhalten registrierten und dem Arbeitgeber zur Auswertung zur Verfügung stellen. Auch hier wurden die Programme nach Angaben der Arbeitgeber zur Gesundheitsförderung eingesetzt.[102] Solch umfassende und höchstpersönliche[103] Daten könnten jedoch genauso gut zur missbräuchlichen Verhaltenskontrolle genutzt werden.

Die Nutzung und Analyse solcher Daten für Entscheidungen fallen unter den eingangs genannten Begriff der Data Analytics bzw. beim Einsatz für HR-Zwecke unter den Begriff der People Analytics.[104]

---

102 Zu den Beispielen, siehe *Mülder*, Überblick zu Potentialen neuer Technologien für HR, in: Petry/Jäger, Digital HR, S. 115.

103 Diese Daten werden durch Art. 9 Abs. 1 DSGVO besonders geschützt; siehe hierzu auch Art. 4 Nr. 14 DSGVO.

104 Teilweise auch *HR Analytics* oder *HR Intelligence* genannt, vgl. *Jäger/Petry*, Digital HR - Ein Überblick, in: Petry/Jäger, Digital HR, S. 43; der Begriff *Workforce Analytics* ist ebenfalls ein Synonym, vgl. *Reindl/Krügl*, People Analytics: Big Data im Personalwesen, 2016, abrufbar unter: https://t3n.de/magazin/people-analytics-big-data-personalwesen-239328/ (letzter Abruf am: 26.09.2019).

C. People Analytics

§ 1 Überblick, Einführung

Das Thema „Analytics" spielt für das Personalmanagement seit Mitte des 20. Jahrhunderts eine Rolle.[105] *People Analytics* ist dabei eine sehr moderne Variante des Human Resources Managements und wird erst seit wenigen Jahren angewandt. Vor allem in Deutschland steckt People Analytics, wie bereits erwähnt, noch in den Kinderschuhen.[106]

Im Unterschied zum Talentmanagement, bei welchem die „Talente" für das Unternehmen identifiziert, gereiht und nach ihrem Potential bewertet werden,[107] ist People Analytics deutlich umfassender und benötigt eine sehr viel größere Datenmenge. People Analytics basiert daher weitgehend auf Big Data-Auswertungen.[108] Diese neue Form der Analyse soll dem Personalmanagement ermöglichen, auf Grundlage von Daten das Verhalten und die Eigenschaften von Mitarbeitern zu erfassen und zu analysieren,

---

105 Siehe hierzu bereits **B. § 2**; ferner *Holthaus/Park/Stock-Homburg*, DuD 2015, 676 (677).

106 So auch *Atabaki/Biemann*, Potenziale der Datenanalyse für HR (People Analytics), in: Petry/Jäger, Digital HR, S. 134; siehe hierzu auch *Kleb*, Haufe Steuer Office Gold 2017, HI7351934. So nutzten im Jahr 2015 lediglich 9 % der Unternehmen Big Data im Personalwesen, hiervon waren mehr als ein Viertel Großunternehmen mit mehr als 500 Mitarbeitern, vgl. Bitkom Research GmbH, Big Data im Personalmanagement, <business.linkedin.com/content/dam/business/talent-solutions/regional/de-de/c/pdfs/BigDataimPersonalmanagement_LinkedIn_Bitkom.pdf>; einer Studie des Karriereportals *Monster* zufolge nutzen lediglich im Jahr 2017 5,8 % der Unternehmen automatisierte Personalauswahlsysteme, vgl. *Weitzel et al.*, Digitalisierung der Personalgewinnung, <www.uni-bamberg.de/fileadmin/uni/fakultaeten/wiai_lehrstuehle/isdl/Studien_2018_2_Digitalisierung_der_Personalgewinnung_Digital-Version_20180207_ff_a.pdf>.

107 Vgl. *Bersin*, Why People Management is Replacing Talent Management, 2015, abrufbar unter: http://joshbersin.com/2015/01/why-people-management-is-replacing-talent-management/ (letzter Abruf am: 17.10.2017); zur Zulässigkeit des Talentmanagements unter Einsatz moderner Technologien siehe bereits *Kainer/Weber*, BB 2017, 2740.

108 *Athanas*, Big Data im HR: Sieben praktische Gedanken über ein Trendthema, abrufbar unter: https://blog.metahr.de/2015/02/05/big-data-im-hr-sieben-praktische-gedanken-ueber-ein-trendthema/ (letzter Abruf am: 27.09.2017); *Freeman*, People Analytics for Dummies, S. 1.

um damit das volle Potential dieser auszuschöpfen und frühzeitig auf Probleme zu reagieren (sog. **Advanced Analytics**[109]).[110] Anders als beim Talentmanagement wird der Fokus nicht alleine auf die Talente der Beschäftigten gesetzt, sondern auch auf das Umfeld wie beispielsweise die Unternehmenskultur. Ebenso werden mögliche Aktivierungsfaktoren miteinbezogen, um die Motivation und Zufriedenheit zu steigern und somit die Fluktuation möglichst gering zu halten.[111] People Analytics befindet sich also an der Schnittstelle zwischen Statistik, Verhaltensforschung, technischen Systemen und Personalstrategie.[112]

Nach der Definition von *Hamann* sind People Analytics „Datenanalysen im Personalbereich, die sich nicht mehr auf die klassischen Quellen und Ziele beschränken, sondern Informationen aus vielfältigen internen und externen Bereichen verknüpfen und so dem HR-Management neue Einblicke und Handlungsoptionen eröffnen."[113] *Raif* und *Swidersky* definieren – wenn auch deutlich zu kurz gegriffen – People Analytics als den Abgleich wesentlicher Eigenschaften bisheriger Arbeitnehmer mit neuen Bewerbern.[114]

Im Ergebnis spricht man von People Analytics, wenn versucht wird, mit Hilfe von Daten (anstatt Bauchgefühl) die richtigen Entscheidungen zu treffen, wobei eine möglichst große Datenmasse als Grundlage herangezogen werden soll, um exaktere Auswertungen und somit bessere Entscheidungen treffen zu können.[115] Es handelt sich daher um evidenz-

---

109 *Jäger/Petry*, Digital HR - Ein Überblick, in: Petry/Jäger, Digital HR, S. 44: Advanced Analytics sind gekennzeichnet durch multidimensionale Analysemethoden (OLAP) sowie multivariate Statistiken, die Zusammenhänge erkennen lassen. Automatisierte Mustererkennung ist ebenfalls Teil davon. *Jäger* und *Petry* sprechen in diesem Zusammenhang nicht von Big Data, sondern von *Smart Data*.

110 *Athanas*, Big Data im HR: Sieben praktische Gedanken über ein Trendthema, abrufbar unter: https://blog.metahr.de/2015/02/05/big-data-im-hr-sieben-praktische-gedanken-ueber-ein-trendthema/ (letzter Abruf am: 27.09.2017); auch *Götz* spricht bei „People Analytics" von einer fortgeschrittenen Datenverarbeitung, vgl. *Götz*, Big Data im Personalmanagement, S. 22.

111 *Bersin*, Why People Management is Replacing Talent Management, 2015, abrufbar unter: http://joshbersin.com/2015/01/why-people-management-is-replacing-talent-management/ (letzter Abruf am: 17.10.2017).

112 *Freeman*, People Analytics for Dummies, S. 12.

113 *Hamann*, Kapitel 6: Datenschutzrecht, in: Arnold/Günther, Arbeitsrecht 4.0, Rn. 50; vgl. auch *Dzida*, NZA 2017, 541 f.

114 *Raif/Swidersky*, GWR 2017, 351.

115 So wohl auch *Jäger/Petry*, Digital HR - Ein Überblick, in: Petry/Jäger, Digital HR, S. 44, die das als das zentrale Ziel von *People Analytics* beschreiben; ähnlich *Dzida/Groh*, ArbRB 2018, 179 (180).

basiertes Personalmanagement (EBPM) in der modernsten Form. People Analytics eröffnen völlig neue Möglichkeiten für ein evidenzbasiertes Management.[116]

People Analytics kann beispielsweise zur Beantwortung folgender Fragen eingesetzt werden: Welche Schlüsselmitarbeiter befinden sich gerade „auf dem Absprung"?[117] Wie kann ich diese an den Arbeitsplatz binden?[118] Wer ist das „Perfect Match" für die zu besetzende Stelle?[119] Welche persönlichen oder betrieblichen Situationen führen zu einer arbeitgeber- oder arbeitnehmerseitigen Kündigung?[120] Welchen Arbeitnehmer kündige ich am besten? Wie muss die Stellenausschreibung aussehen, um interessante Arbeitnehmer anzulocken?[121] Aus welchen Mitarbeitern ist es im Unternehmen möglich, ein optimales Team zusammenzustellen?[122]

Es handelt sich um eine interdisziplinäre Aufgabe, wobei aus den verschiedenen Forschungsbereichen Daten verknüpft werden sollen. Ausgang der Analyse sind die bereits im Unternehmen existierenden Daten. Diese werden mit externen Daten (z.B. aus der Verhaltensforschung) verknüpft und es wird versucht, Muster in den Daten zu erkennen. Hierfür benötigt es die IT, da diese Auswertungen mit rein menschlicher Gedankenkraft aufgrund der Masse an Daten und den unbekannten Zusammenhängen nicht mehr möglich sind. Die hierdurch gewonnen Erkenntnisse werden in weiterer Folge auf die Arbeitskräfte im Unternehmen angewandt. Ziel ist es, bestimmtes Verhalten prognostizieren und so Handlungsempfehlungen aussprechen zu können. Die umgesetzten Ergebnisse fließen wiederum in weitere Analysen mit ein und ermöglichen so eine stetige Verbesserung der Prognosen durch Anreicherung weiterer (Erfahrungs-)daten.

---

116 Vgl. *Kleb*, Haufe Steuer Office Gold 2017, HI7351934 unter Ziff. 2. Evidenzbasiertes Personalmangement kann aber auch ohne People Analytics stattfinden, wenn beispielsweise durch Untersuchungen lediglich vorhandene Instrumente in Ihrer Wirksamkeit untersucht und validiert werden. Zum EBPM instruktiv *Sliwka/Biemann*, Human Resources Manager 2011, 76 ff.

117 *Dzida*, NZA 2017, 541 (542).

118 *Gola*, Datenschutz am Arbeitsplatz, Rn. 34.

119 *Bissels/Mayer-Michaelis/Schiller*, DB 2016, 3042.

120 *Bissels/Mayer-Michaelis/Schiller*, DB 2016, 3042.

121 *Gola*, Datenschutz am Arbeitsplatz, Rn. 33.

122 *Hamann*, Kapitel 6: Datenschutzrecht, in: Arnold/Günther, Arbeitsrecht 4.0, Rn. 50.

Die folgenden Daten könnten beispielsweise für Workforce oder People Analytics genutzt werden:

Tabelle: Datenpunkte für People Analytics (angelehnt an Kleb 2017)

Stammdaten	**IT-Nutzungs- und Sensordaten**	**HR-Instrumente**	**Externe Daten**
Geschlecht	Mail-Adressaten	Mitarbeiter-befragungen	Balanced Scorecards
Alter	In Mails geäußerte Gefühle	360° Feedback	Unternehmensperformance
Muttersprache / Sprachen	Social-Media-Aktivitäten	Ideenmanagement	Börsenkurs
Gehalt/Lohn	Besuchte Internetseiten	Leistungsbeurteilung	Arbeitgeberbewertungen
Organisationseinheit	Google Anfragen	Zielvereinbarung / Zielerreichung	Social Media Äußerungen
Vertragstyp	Wikipedia Anfragen	Austrittgründe	…
Firmenzugehörigkeit	Beiträge im Wissensmanagement	Weiterbildungen	
Ebene/Titel	Verwendete Dokumente	Bewerbungen	
Führungsspanne	Geodaten	Assessments	
Umfang der Führungsaufgabe	Häufige Kommunikationspartner	Rekrutierungskanäle	
Weiterbildungen	Vitalparameter (erfasst durch Wearables) wie Puls, Blutdruck	Work-Life-Balance	
Krankheitstage	Screen-Time am Mobiltelefon	…	
Entfernung Wohnort/Arbeitsplatz	Screen-Time in jeweiligen Anwendungen auf dem PC		
…	Physikalische Nähe zu anderen Arbeitnehmern (NFC-Tagging/Bluetooth)		
	…		

Eine solch umfangreiche Erfassung, Verarbeitung und Verknüpfung von Daten kann sowohl in datenschutzrechtlicher als auch anti-diskriminierungsrechtlicher und persönlichkeitsrechtlicher Perspektive kritisch werden, wenn nicht exakte Grenzen und Verarbeitungszwecke festgelegt werden. Insbesondere bei den IT-/Sensordaten wird es vielfach geboten sein,

aggregierte (und somit anonymisierte) Daten zu verwenden, um die Bedenken zu beseitigen.[123] Hierauf wird jedoch an späterer Stelle bei den untersuchten Nutzungsszenarien genauer eingegangen.[124]

§ 2 Verfahren und eingesetzte Techniken bei People Analytics

I. Überblick

Moderne People Analytics-Systeme verwenden Big Data-Methoden, die die vier Kriterien *Volume*, *Variety*, *Velocity*, *Veracity/Value*[125] erfüllen, indem sie große (Volume), vielfach unstrukturierte (Variety) Datenmengen in Echtzeit (Velocity) auswerten, um hieraus Prognosedaten zu generieren sowie Korrelationen in den bisherigen Datensätzen zu erkennen (Veracity/Value). Erst die Fülle an Daten ermöglicht eine solch differenzierte und diffizile Analyse von Personalfaktoren, weshalb der Einsatz von Big Data notwendige Voraussetzung für moderne und effiziente People Analytics ist.[126]

Insbesondere der umfassende Anfall von digitalen Daten in Form von E-Mails, Browserverläufen, sozialen Netzwerken, digitalen Kollaborationen (Crowd-Working / digitale Teamarbeit), Sensordaten u.v.m. ermöglicht es, unbekannte Korrelationen zwischen verschiedenen Faktoren zu finden, die bislang im Verborgenen blieben. Zusammenhänge, die unbekannt sind, werden vom Menschen nicht proaktiv protokolliert, weshalb die automatische Erfassung solcher Daten durch Computer bzw. Logdateien einen wesentlichen Beitrag an der Ermöglichung solcher Analysen leistet. Erst wenn Zusammenhänge im Ansatz erkannt werden, wird ein menschlicher Analyst hierauf ein besonderes Augenmerk legen und diesen näher nachgehen.

An dieser Stelle kann perspektivisch auch *Künstliche Intelligenz* ins Spiel kommen.[127] Derzeit sind es sog. *Data Scientists* - ein sehr junges Betätigungsfeld[128] -, die Zusammenhänge mittels Auswertungstechnologien wie

123 Ähnlich *Kleb*, Haufe Steuer Office Gold 2017, HI7351934.
124 So z.B. Dashboards für Abteilungsleiter, vgl. **E. § 3 III**.
125 Siehe **C. § 2 II. 1. b**).
126 In Bezug auf Business Analytics ebenso *Hoening/Esch/Wald*, Haufe Steuer Office Gold, HI10713394.
127 Zur Definition von Künstlicher Intelligenz siehe **C. § 2 II. 2. a**).
128 An der Universität Mannheim gibt es beispielsweise erst seit dem Jahr 2017 einen Masterstudiengang in Data Science, siehe *Universität Mannheim*, Presse-

Hadoop[129] und R[130] in Daten suchen und hieraus ihre Schlüsse ziehen (Analyse und Interpretation großer Datenmengen[131]). Mittels KI können die Systeme darauf trainiert werden - auch unternehmensübergreifend - bestimmte Muster in Daten zu suchen und dementsprechend eigene Schlüsse zu ziehen, indem sie vorhandene Datenstrukturen nach üblichen Mustern durchsuchen und auf die im Unternehmen vorhandenen Daten anwenden und daraus Vorhersagen treffen.[132]

II. Begriffsbestimmungen

1. Big Data

Unter Big Data wird trivial die Verarbeitung von großen Datenmengen in großer Geschwindigkeit und semi- bzw. unstrukturierter Vielfalt verstanden.[133] Unter diese sehr unspezifische Definition fällt somit auch das Verarbeiten von Arbeitnehmerdaten durch Arbeitgeber im Wege des Pro-

information 46/2016: Ausbildung zum Datenspezialisten: Neuer Masterstudiengang in Data Science startet im Frühjahr 2017.

129 Hadoop ist ein auf der Programmiersprache Java basierendes, quelloffenes Framework, mit dem sich große Datenmengen auf verteilten Systemen in hoher Geschwindigkeit verarbeiten lässt. Im Business Intelligence-Umfeld lassen sich mit dem Framework Reports und Analysen aus unterschiedlichsten Datenquellen mit unterschiedlichen Strukturen selbst im Petabyte-Bereich schnell und wirtschaftlich generieren, vgl. *Luber/Litzel*, Was ist Hadoop?, 01.09.2016, abrufbar unter: https://www.bigdata-insider.de/was-ist-hadoop-a-587448/ (letzter Abruf am: 10.10.2019).

130 R ist eine freie Programmiersprache, die insbesondere für Data Mining und Predictive Analytics eingesetzt wird. Sie ist eine der führenden Lösungen im Bereich der statistischen Datenanalyse, da sich Daten mit dieser Programmiersprache sehr flexibel auswerten und visualisieren lassen. Mittels R können Analysen bei Hadoop-Clustern durchgeführt werden, vgl. *Luber/Litzel*, Was ist R?, 27.04.2018, abrufbar unter: https://www.bigdata-insider.de/was-ist-r-a-707966/ (letzter Abruf am: 10.10.2019).

131 So die Beschreibung des Studiengangs, *Universität Mannheim*, Presseinformation 46/2016: Ausbildung zum Datenspezialisten: Neuer Masterstudiengang in Data Science startet im Frühjahr 2017.

132 Dies ist der größte Mehrwert von Big-Data-Technologien, siehe *Hoening/Esch/Wald*, Haufe Steuer Office Gold, HI10713394 sowie nachfolgend die Ausführungen zum Begriff „Big Data".

133 *Dorschel*, Praxishandbuch Big Data, S. 2.

filing[134] bzw. mithilfe von Auswertungsalgorithmen, weshalb dieser Begriff und seine Ausprägungen zunächst genauer dargestellt werden sollen.

a) Allgemeine Definition

In der Fachliteratur lassen sich unzählige Definitionen des Begriffs *Big Data* finden:

> *„Big Data steht für große Datenmengen, die über das Internet oder anderweitig gesammelt, verfügbar gemacht und ausgewertet werden.“*[135]

> *„Big Data-Verfahren zeichnen sich dadurch aus, dass große Datenbestände erhoben, gespeichert und vorgehalten werden. Diese Datenbestände werden sodann mit Hilfe von Algorithmen ausgewertet, um Erkenntnisse zu gewinnen.“*[136]

> *„Von Big Data spricht man, wenn der Datenumfang, der aus elektronischer Kommunikation generiert wird, so groß oder komplex ist oder sich so schnell ändert, dass diese Daten mit den üblichen Methoden der Datenverarbeitung nicht mehr ausgewertet werden können. Mittlerweile werden mit dem Begriff Big Data auch Technologien beschrieben, die man zum Sammeln und Auswerten dieser Datenmengen nutzt“*[137]

> *„Big Data steht für die Möglichkeit, in riesigen Datenmengen (volume), die in unterschiedlichen Formaten vorliegen (variety), schnell (velocity) Muster zu erkennen und die Daten dadurch gewinnbringend (value) nutzen zu können.“*[138]

> *„Unter Big Data wird das Erheben, Speichern, Zugreifen und Analysieren von großen und teilweise heterogenen, strukturierten und unstrukturierten Datenmengen verstanden.“*[139]

> *„Big Data analytics refers to the process of collecting; analyzing those unstructured, semi structured data to find out the correlation between them,*

134 Siehe die Legaldefinition in Art. 4 Nr. 4 DSGVO.
135 *Weichert*, ZD 2013, 251.
136 *Härting*, ITRB 2016, 209.
137 *Kaiser/Kraus*, zfo 2014, 379.
138 *Richter*, DuD 2016, 581.
139 *Waidner*, SIT-TR-2015-06, S. 8.

patterns and useful information those are helpful for decision making and needed for future growth of any organization or system."[140]

Spezialisten kritisieren, dass die Frage „Was ist Big Data?" „höchst unterschiedlich, in der Regel unzureichend und damit unzutreffend"[141] beantwortet wird, da sich hinter diesem „Buzzword" ein sehr facettenreiches Thema verbirgt, welches nicht mit einer allgemeinen Definition beantwortet werden kann.

In den gängigsten Definitionen werden dem Begriff *Big Data* jedoch vier spezifische Eigenschaften zugewiesen: Volume, Variety, Velocity, und Veracity bzw. Value („Die vier Vs"),[142] weshalb auf diese Eigenschaften im Folgenden näher eingegangen werden soll. Es wird hingegen nicht versucht, eine weitere allgemeingültige Definition zu finden, da die Technologien, die unter *Big Data* zu fassen sind, sich ständig weiterentwickeln und neue Möglichkeiten bieten, sodass eine Definition zum Zeitpunkt der Veröffentlichung dieser Arbeit bereits wieder veraltet sein könnte. Zudem kann eine exakte Definition dahinstehen, da der Begriff bislang keine rechtliche Relevanz erhalten hat. Wichtig ist, dass erst durch die Kombination der vier Vs sich das gesamte Potential von Big Data zeigt.[143]

b) Die „vier Vs": Volume, Variety, Velocity, Veracity/Value

aa) Volume

Unter *Volume* wird die zu verarbeitende Datenmenge verstanden, die bei Big Data – wie der Begriff bereits suggeriert – sehr groß ist. Aufgrund immer leistungsfähigerer und günstigerer Computerchips erhöht sich diese Datenmenge tagtäglich (Stichwort: „Internet of Things"[144]). Jedes Gerät erzeugt Daten, welche durch die Vernetzung an einem zentralen Ort, meist in der Cloud, gespeichert werden. Diese (zentrale) Ansammlung von Daten ermöglicht es schließlich, diese Daten einfach und aufgrund der immer zunehmenden Rechenleistung auch in Sekundenschnelle zu verarbeiten.

---

140 *Barman/Ahmed*, Big Data in Human Resource Management - Developing Research Context.
141 *Dorschel*, Praxishandbuch Big Data, S. 1.
142 Vgl. *Dorschel*, Praxishandbuch Big Data, S. 6 f. m.w.N.
143 *Kleb*, Haufe Steuer Office Gold 2017, HI7351934.
144 Hierzu bereits **B. § 3 IV**.

Nur am Rande sei erwähnt, dass die weltweit generierte Datenmenge *exponentiell* wächst. Eine vom Speicherhersteller *Seagate* finanzierte Studie der International Data Corporation (IDC) vom März 2017 sagt vorher, dass der weltweite Datenbestand im Jahr 2025 bei ungefähr 163 Zettabyte (ZB) liegen wird.[145] Im Vergleich: 2016 lag der Datenbestand „noch" bei 16,1 ZB.[146] Einer älteren Studie zufolge wurden in den Jahren 2000 bis 2003 auf der Erde mehr Informationen erzeugt als in den vergangen 300.000 Jahren.[147] Ein Zettabyte entspricht einer Milliarde Terrabyte. Da diese Größenordnung für Menschen kaum noch begreifbar ist, soll dies mit einem plastischen Beispiel veranschaulicht werden: Ein Terrabyte hat ungefähr die Datenmenge von einer Million Bücher;[148] der Datenbestand im Jahr 2016 entsprach bereits 1,61 x 10^{16} Büchern (= 16 Billiarden Büchern), im Jahr 2025 werden es bereits 163 Billiarden Bücher sein. Bei einer prognostizierten Weltbevölkerung von ca. acht Milliarden Menschen im Jahr 2025[149] entspräche dies einem Datenbestand von 20,37 Millionen Bücher pro Person.

Ohne intelligente Algorithmen und leistungsstarke Rechner sind solch große Datenmengen unmöglich zu verarbeiten. Der Trend, immer mehr Daten zu sammeln (um dann ggf. später festzustellen, ob diese tatsächlich benötigt werden), macht auch vor Unternehmen, insbesondere HR nicht halt. Es wurde bereits in Studien festgestellt, dass immer mehr Unternehmen ihre Daten in die Cloud laden.[150]

---

145 *Reinsel/Gantz/Rydning*, Data Age 2025: The Evolution of Data to Life-Critical, <www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf>, S. 3.

146 *Reinsel/Gantz/Rydning*, Data Age 2025: The Evolution of Data to Life-Critical, <www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf>, S. 3.

147 *Lyman/Varian*, The Journal of Electronic Publishing 2000, DOI: 10.3998/3336451.0006.204.

148 *Lyman/Varian*, The Journal of Electronic Publishing 2000, DOI: 10.3998/3336451.0006.204.

149 Vgl. Studie der UNO aus dem Jahr 2019, https://population.un.org/wpp/Graphs/Probabilistic/POP/TOT/900 (letzter Abruf am: 19.09.2019).

150 *Bersin*, BigData in HR Why it's here and What it Means, 2012, abrufbar unter: http://blog.bersin.com/bigdata-in-hr-why-its-here-and-what-it-means/ (letzter Abruf am: 17.10.2017).

bb) Variety

Unter *Variety* wird die Heterogenität der Datenquellen und -formate verstanden.[151] Aufgrund immer vielfältiger werdenden Anwendungsbereichen für IT-Anwendungen und daraus resultierenden verschiedenartigen Systemen, die Daten sammeln, kommt es – oftmals aufgrund mangelnder oder nicht eingehaltener Datenstandards – zu unterschiedlichsten Datenbanken, Dateiformaten und zugleich Quellen für diese Daten. Zentrale Aufgabe von Big Data ist es, Erkenntnisse aus diesen verschiedenartigen Daten zu gewinnen, um beispielsweise Muster, Zusammenhänge oder Abhängigkeiten zu erkennen.[152] So sollen Personalmanagementsysteme bei Bewerbungen Daten aus sozialen Netzwerken mit in einem Textprogramm geschriebenen Lebensläufen abgleichen, diese Daten mit Auswertungen aus dem Assessment Center verknüpfen, um schließlich den Kandidaten mit anderen Bewerbern und den bereits vorhandenen Arbeitnehmern abzugleichen. Während die Ergebnisse aus Einstellungstests möglicherweise noch in eine vorgegebene Maske eingetragen werden, sind die Daten aus sozialen Netzwerken meist unstrukturiert und Lebensläufe individuell (und vielfach nicht maschinenlesbar[153]) gestaltet.

cc) Velocity

Velocity bedeutet übersetzt Geschwindigkeit, wird jedoch im Zusammenhang mit Big Data nicht einheitlich verstanden. Überwiegend wird darunter die hohe Datenentstehungsrate sowie die Notwendigkeit deren schneller Verarbeitung und Ergebnisgenerierung verstanden. Von Bedeutung ist dies insbesondere für Echtzeit-Anwendungen, um beispielsweise Kreditkarten-Betrug zu unterbinden oder interaktive Online-Erlebnisse zu ermöglichen.[154] Im Bereich der hier untersuchten Technologien ist die Echt-

151 *Dorschel*, Praxishandbuch Big Data, S. 8.
152 *Dorschel*, Praxishandbuch Big Data, S. 8.
153 Es wird daher bisweilen empfohlen, anstatt kreativ gestaltete Lebensläufe, einfache, gut maschinenlesbare mit Schriftarten wie Arial oder Courier zu verwenden, da diese vielfach die Entscheidungsträger ohnehin nicht mehr zu Augen bekommen, vgl. *O'Neil*, Weapons of math destruction, S. 114. Viele Unternehmen verzichten daher völlig auf einen eigens gestalteten Lebenslauf und fordern die Bewerber auf, die Lebenslaufdaten in ein vorkonfiguriertes Online-Formular auf der Bewerbungswebsite einzutragen.
154 *Waidner*, SIT-TR-2015-06, S. 21.

zeitauswertung weniger relevant, da der Entscheidungsprozess (insbesondere aufgrund von Mitspracherechten des Betriebsrats[155]) ohnehin nicht binnen Sekunden abgeschlossen werden kann. Wichtig ist aber dennoch – insbesondere beim Anfall größerer Mengen an Personaldaten –, dass die Auswertung von Daten nicht Stunden und Tage benötigt, damit auf kurzfristige Ereignisse (z.B. Ausfall eines Arbeiters, wofür ein anderer, geeigneter Kollege einspringen muss) schnell reagiert werden kann.

dd) Veracity/Value

Das „vierte V" wird unterschiedlich definiert. Manche Definitionen sehen *Veracity* als Eigenschaft von Big Data an, also die Vertrauenswürdigkeit der Daten oder der daraus gezogenen Schlüsse.[156] In diesem Zusammenhang ist zu beachten, dass bei Big-Data-Auswertungen oftmals Daten verwendet werden, deren objektiver Erkenntniswert nicht sicher messbar ist (z.B. Daten aus sozialen Netzwerken).[157] Die verwendeten Algorithmen müssen diesen Aspekt jedoch bei der Ergebnisfindung berücksichtigen, damit die gezogenen Rückschlüsse richtig sind und damit einen Mehrwert darstellen.

In anderen Definitionen hingegen wird der Begriff *Value* verwendet, also die Möglichkeit, die gesammelten Daten gewinnbringend einzusetzen.[158] Da nur bei verlässlichen Datenquellen bzw. einer belastbaren Auswertung ein tatsächlicher Erkenntnisgewinn erzielt werden kann, greifen die Begriffe *Veracity* und *Value* ineinander bzw. ist der *Value* abhängig von der *Veracity*.

Während bei einem Algorithmus, der dem Benutzer individualisierte Nachrichten oder Werbung anzeigen soll, Fehler bei der Auswertung oder falsche Rückschlüsse recht unproblematisch sind („*Wieso erhalte ich jetzt Werbung für Pferdesättel, ich reite doch gar nicht?*"), sind unrichtige oder unvollständige Daten im Personalmanagement höchst problematisch. Stellt ein Algorithmus beispielsweise fest, dass ein Arbeitnehmer keine Arbeitsleistung erzielt, ohne z.B. die Information zu besitzen, dass es sich um ein nach § 38 Abs. 1 BetrVG freigestelltes Betriebsratsmitglied handelt (und

155 Dazu unter **D.** § **2**.
156 *Waidner*, SIT-TR-2015-06, S. 21.
157 *Dorschel*, Praxishandbuch Big Data, S. 8.
158 *Richter*, DuD 2016, 581.

somit ohnehin Sonderkündigungsschutz[159] genießt), so könnte das Ergebnis einer Auswertung lauten: „Unbedingt kündigen / loswerden". Die Auswertung des Arbeitsergebnisses selbst ist zwar richtig. Aufgrund der unvollständigen Daten ist der gezogene Schluss allerdings falsch, da dieser Arbeitnehmer aufgrund der Freistellung rechtmäßig keine Arbeitsleistung erbringt und zudem Sonderkündigungsschutz genießt. Untermauert wird die Wichtigkeit vollständiger und korrekter Daten durch das datenschutzrechtliche Gebot der Datenrichtigkeit in Art. 5 Abs. 1 lit. d DSGVO.[160] Die *Veracity* der Daten ist daher von allerhöchster Bedeutung im Bereich People Analytics.

c) Profilbildung durch Big Data und Scoring

Die Möglichkeiten, die Big Data bietet, sind unzählig. Eine der wichtigsten Anwendungsformen ist wohl die Profilbildung. Im Jahr 2012 hat beispielsweise Google seine Dienste Gmail, YouTube, Google+ etc. zusammengelegt, um alle über einen User vorhandenen Daten zu einem Profil kombinieren zu können und so ein „individuelleres Nutzungserlebnis" zu bieten.[161] Ein Google-Konto ist für die (sinnvolle) Nutzung von Android-Handys notwendig, da der Play Store, der Anwendungsmarkt für Android-Apps, die Verknüpfung mit einem Google-Konto erfordert.[162] Durch die Verknüpfung mit dem Mobiltelefon hat Google somit unzählige Möglichkeiten, Daten über die User zu sammeln. So erstellt Google standardmäßig auch ein Bewegungsprofil von jedem einzelnen Benutzer in der sog. „Google Maps Timeline"[163].

Bei einem Marktanteil von rund 79 %[164] in Deutschland (weltweit sind es sogar 88,1 %[165]) kann Google somit ein sehr exaktes Abbild der

159 § 15 Abs. 1 KSchG.
160 Vgl. zur Richtigkeit bei Persönlichkeitsprofilen *Betz*, ZD 2019, 148 (149).
161 Vgl. *Waidner*, SIT-TR-2015-06, S. 26.
162 *Waidner*, SIT-TR-2015-06, S. 26.
163 Siehe https://www.google.com/maps/timeline?pb (letzter Abruf am: 02.05.2018).
164 *Kantar*, Marktanteile von Android und iOS am Absatz von Smartphones in Deutschland von Januar 2012 bis Juni 2019, 2019, Statista, abrufbar unter: https://de.statista.com/statistik/daten/studie/256790/umfrage/marktanteile-von-android-und-ios-am-smartphone-absatz-in-deutschland/ (letzter Abruf am: 19.09.2019).
165 *Gartner*, Marktanteil von Android am Absatz von Smartphones weltweit vom 1. Quartal 2009 bis zum 1. Quartal 2019, 2018, Statista, abrufbar unter: https://d

(deutschen) Bevölkerung erstellen. So ist es nicht verwunderlich, dass Google mit seiner App Maps am exaktesten die Verkehrslage darstellen kann[166] und hierdurch die Konkurrenz nach und nach vom Markt verdrängt.[167] Die 45 Mio. Android-Smartphones[168] erzeugen jeweils Datenpunkte, die für verlässliche Verkehrsprognosen genutzt werden können (Ort, Geschwindigkeit, Standzeit), während andere Hersteller allenfalls auf einen Bruchteil der Geräte (sofern diese überhaupt etwaige Daten übermitteln) oder nur auf Verkehrsmeldungen zurückgreifen können.

Doch nicht nur Tech-Giganten[169] nutzen die Möglichkeiten von *Big Data* für ihre Zwecke. Auch Arbeitgeber holen sich im Vorfeld von Personalentscheidungen Daten über verschiedenste Wege ein und führen damit beispielsweise ein Scoring durch. Anhand dieser Scores können sie vorsortieren und selektieren.[170] Auch während des laufenden Beschäftigungsverhältnisses kann diese Technologie verwendet werden, um z.B. Zigarettenpausen, Toilettenbesuche, Privattelefonie, Smartphonenutzung etc. zu analysieren und anhand der hieraus gewonnen Erkenntnisse bessere Personalentscheidungen treffen zu können.[171]

Die unter § 2 genannten Systeme von Microsoft, SAP, Kronos und IBM nutzen ebenfalls allesamt Benutzerprofile (und Dashboards), um die Daten für den Endanwender der jeweiligen Anwendung (z.B. die Mobile oder

---

e.statista.com/statistik/daten/studie/246456/umfrage/marktanteil-von-googles-android-am-weltweiten-smartphone-absatz-nach-quartalen/ (letzter Abruf am: 19.09.2019).

166 Dass jedoch auch diese Vorhersagen nie völlig fehlerfrei sein können, zeigt ein Projekt eines Künstlers, der mit Hilfe von 99 Android-Smartphones einen „Fake-Stau" in Maps erzeugt hat („*Bollerwagen-Hack*"), vgl. https://www.suedde utsche.de/digital/google-maps-hacks-stauanzeige-1.4784081 (letzter Abruf am 18.05.2020).

167 Hierzu https://www.chip.de/news/Google-Maps-als-Navi-Ein-Vorteil-laesst-der-Konkurrenz-fast-keine-Chance_99347317.html (letzter Abruf 19.09.2019).

168 Es gibt 57 Mio. Smartphone-Nutzer in Deutschland (*Bitkom*, Anzahl der Smartphone-Nutzer in Deutschland in den Jahren 2009 bis 2018 (in Millionen), 2018, Statista, abrufbar unter: https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/ (letzter Abruf am: 19.09.2019), der Marktanteil von Android beträgt 79 %. Dies entspricht somit 45 Millionen Android-Nutzern.

169 Hierbei wird gerne von der „Gang of Four" oder kurz GAFA gesprochen: Google, Amazon, Facebook und Apple. Zu diesem Begriff gibt es einen eigenen Wikipedia-Artikel, siehe https://en.wikipedia.org/wiki/Big_Four_tech_companies (letzter Abruf am: 19.09.2019).

170 *Waidner*, SIT-TR-2015-06, S. 31.

171 *Waidner*, SIT-TR-2015-06, S. 31.

Web-Apps der jeweiligen Plattformen) darstellen zu können. Auch hier ist das Profil erforderlich, um die Daten für den jeweiligen Nutzer anzupassen bzw. Analysen auf Benutzerbasis durchführen zu können.

Diese Technologien werden vor allem außerhalb der Europäischen Union eingesetzt. In Deutschland bzw. der EU und somit im Geltungsbereich der DSGVO sind solche Profilbildungen allerdings strengen Vorgaben unterworfen.[172] Nichtsdestotrotz gehen Experten davon aus, dass in Deutschland ähnliche Möglichkeiten wie in anderen Ländern für People Analytics und EBPM bestehen.[173]

Die Unsicherheit ist jedoch noch groß: Eine gemeinsame Studie der Bitkom Research GmbH und LinkedIn aus dem Jahr 2015 ergab, dass ein Großteil der Unternehmen Big Data-Lösungen aufgrund datenschutzrechtlicher Bestimmungen oder Sicherheitsbedenken noch nicht einsetzen sowie unternehmensintern noch ein zu geringer Wissensstand der Fachkräfte über Analysemöglichkeiten besteht.[174] Unternehmen aus den USA, die *Big Data* bereits einsetzen, haben dahingegen erreicht, durch den Einsatz von Analysen die Fluktuationsquote von Mitarbeitern um 50 % zu senken.[175]

2. Künstliche Intelligenz

Der Begriff *Künstliche Intelligenz* (kurz: *KI* oder vom englischen Begriff *Artificial Intelligence* abgeleitet: *AI*) taucht im Zusammenhang mit *Big Data* immer wieder auf, weshalb auch dieser Begriff für die weitere Verwendung in dieser Arbeit definiert wird sowie die verschiedenen „Intelligenzstufen" kurz erläutert werden. Mit dem Einsatz künstlicher Intelligenz im Rahmen von Entscheidungsprozessen erhoffen sich Arbeitgeber eine bislang unerreichte Entscheidungsqualität, die weit über menschliche Maß-

172 Ausführlich hierzu nachfolgend **E. § 1 II.**

173 *Haufe Online Redaktion*, People Analytics: Wie lässt sich Big Data für HR nutzen?, 10.10.2019, abrufbar unter: https://www.haufe.de/personal/hrmanagement/People-Analytics-Wie-laesst-sich-Big-Data-fuer-HR-nutzen_80_501534.html (letzter Abruf am: 11.10.2019).

174 *Bitkom Research GmbH/LinkedIn Deutschland, Österreich, Schweiz*, "Big Data" verändert das Personalwesen nachhaltig.

175 *Kittner*, Big Datenschutz bei Big Data, 07.02.2018, abrufbar unter: https://www.haufe.de/personal/arbeitsrecht/datenschutz-zulaessigkeit-von-big-data-analysen_76_441566.html; *Niklas/Thurn*, BB 2017, 1589: Als Beispiele werden Microsoft und Xerox genannt.

stäbe hinausgehen könnte. Die Folge wäre, dass immer mehr Entscheidungen an Maschinen abgegeben werden.[176]

a) Allgemeine Definition

Der Begriff der künstlichen Intelligenz ist nicht neu, sondern wurde bereits im Jahr 1955 erstmals verwendet. Definiert wurde der Begriff im Rahmen eines Vorschlags für die erste Studie zum Thema Artificial Intelligence durch *John McCarthy*, *Marvin Minsky*, *Nathaniel Rochester* und *Claude Shannon*. Die Autoren beschrieben den Begriff folgendermaßen:

> *„An attempt will be made to find how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans, in improve themselves […] For the present purpose the artificial intelligence problem is taken to be that of making a machine behave in ways that would be called intelligent if a human were so behaving.*"[177]

Eine andere, sehr gut zutreffende Beschreibung kommt von *Elanine Rich* aus dem Jahr 1983:

> "*Artificial Intelligence is the study of how to make computers do things at which, at the moment, people are better.*"[178]

Eine einheitlich akzeptierte Definition von künstlicher Intelligenz gibt es jedoch bis heute nicht.[179] Dies ist dem Umstand geschuldet, dass die Begriffe „Intelligenz" und „intelligentes menschliches Verhalten" nicht gut definiert sind.[180] Entscheidend vorangebracht hat die Definition von künstlicher Intelligenz der britische Mathematiker *Alan Turing*– ebenfalls bereits im Jahr 1950 mit dem inzwischen weit bekannten *Turing-Test.* Demnach ist eine Maschine als intelligent zu bezeichnen, wenn ein

176 WHWS/*Broy/Heinson*, B. II. Die automatisierte Einzelfallentscheidung im Beschäftigungsverhältnis, Rn. 2.
177 *McCarthy et al.*, A Proposal for the Dartmouthg Summer Research Project on Artificial Intelligence, <aaai.org/ojs/index.php/aimagazine/article/view/1904/1802>.
178 *Schael*, DuD 2018, 547 (548).
179 *Holtel/Hufenstuhl/Klug*, Künstliche Intelligenz verstehen als Automation des Entscheidens, <www.bitkom.org/sites/default/files/file/import/Bitkom-Leitfaden-KI-verstehen-als-Automation-des-Entscheidens-2-Mai-2017.pdf>, S. 9.
180 *Wichert*, Künstliche Intelligenz, in: Hanser, Lexikon der Neurowissenschaft.

Mensch, der mit einem Computer kommuniziert, diesen nicht mehr als Computer identifizieren kann.[181]

Die Definition *Turings* leidet allerdings darunter, dass sie nur das spezifische Problem der Kommunikation behandelt und für andere Aspekte, die die Interaktion nicht betreffen, nicht anwendbar ist.

Zudem wird in der allgemeinen Bevölkerung das Verständnis des Begriffs „Künstliche Intelligenz" vorwiegend durch Hollywood geprägt und hat wenig mit der derzeitigen technischen Diskussion um KI zu tun, sondern mehr mit Science-Fiction.

Der Begriff der künstlichen Intelligenz zeichnet sich jedoch vor allem dadurch aus, dass KI-Systeme verstehen, schlussfolgern, lernen und interagieren können,[182] d.h. nicht nur starren, vorprogrammierten Abfolgen zur Lösung bestimmter Probleme folgen.

Obwohl Künstliche Intelligenz die Experten bereits seit Jahrzenten beschäftigt, kam der Durchbruch erst in den letzten Jahren, seitdem die entsprechende Rechen- und Speicherkapazität vorhanden ist. Durch diese zunehmenden Kapazitäten ist es nunmehr möglich mit Hilfe von neuronalen Netzen selbstlernende Systeme zu schaffen.[183] Diese zeichnen sich dadurch aus, dass sie keinen starren Abläufen folgen, sondern sich selbst optimieren können. Problematisch ist – insbesondere aus datenschutzrechtlicher Sicht –, dass die Entscheidungen daher für Menschen nur noch bedingt bis gar nicht mehr nachvollziehbar sind, da der Entscheidungsmechanismus der Maschine eine Art „Blackbox" ist.[184] Dies liegt unter anderem daran, dass solche neuronalen Netze mitunter schon 100 Millionen oder mehr Knoten haben, die letztendlich Entscheidungsparameter darstellen.[185]

---

181 Vgl. *Turing*, Mind 1950, 433 ff.

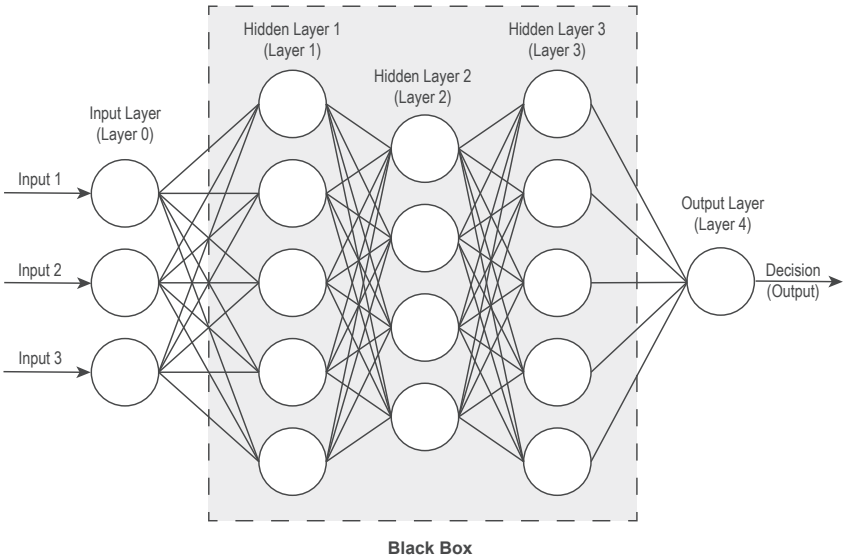
182 *Jäger/Petry*, Digital HR - Ein Überblick, in: Petry/Jäger, Digital HR, S. 46; *Bitkom e.V.*, Entscheidungsfindung mit Künstlicher Intelligenz, S. 16 f.: Abgeleitet vom Englischen Sense, Comprehend, Act and Learn.

183 *Jäger/Petry*, Digital HR - Ein Überblick, in: Petry/Jäger, Digital HR, S. 47.

184 *Gausling*, PinG 2019, 61 (68 f.); *Stiemerling*, 2.1 Technische Grundlagen, in: Kaulartz/Ammann/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, Rn. 61: auf der technischen Ebene nachvollziehbar, für den Anwender und Benutzer allerdings nicht.

185 *Körner*, 2.4 Nachvollziehbarkeit von KI-basierten Entscheidungen, in: Kaulartz/Ammann/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, Rn. 7.

Abbildung 1: Neuronales Netzwerk (Black Box) mit drei Entscheidungsebenen



b) Automation des Entscheidens

Bereits die Definition zeigt, dass schließlich der Grad der Automation des Entscheidens relevant dafür ist, wie „intelligent" eine Maschine ist. *Bitkom* hat im Jahr 2017 einen Leitfaden veröffentlicht, in welchem ein 5-Stufen-Modell zur Automation des Entscheidens entwickelt und vorgestellt wurde,[186] welches für die Zwecke dieser Arbeit nachfolgend kurz dargestellt werden soll.

aa) Das 5-Stufen-Modell zur Automation des Entscheidens

Auf **Stufe 0** entscheidet der Akteur (Mensch) allein und hat keine Maschine, die ihn hierbei aktiv unterstützt; diese Stufe ist der Ausgangspunkt für jede Automation des Entscheidens. **Stufe 1** ist assistiertes Entscheiden;

186 *Holtel/Hufenstuhl/Klug*, Künstliche Intelligenz verstehen als Automation des Entscheidens, <www.bitkom.org/sites/default/files/file/import/Bitkom-Leitfaden-KI-verstehen-als-Automation-des-Entscheidens-2-Mai-2017.pdf>, S. 21.

diese Entwicklung begann bereits in den 1980er Jahren mit einfachen Werkzeugen der Tabellenkalkulation, die es ermöglichten, in kürzester Zeit Antworten auf komplexe Fragen zu geben und die Effizienz somit um das 80-fache zu erhöhen. Auf **Stufe 2** liegt bereits teilweises Entscheiden vor; das System übernimmt die Berechnung und in manchen Anwendungsfällen kann es bereits selbstständig Entscheidungen treffen, wenn der Akteur zuvor seine Präferenzen geäußert hat. „Intelligenz" im Sinne der obigen Definition liegt hier noch keine vor, da die Entscheidungen entlang einer vorprogrammierten Abfolge von Befehlen verlaufen. **Stufe 3** ist geprüftes Entscheiden, d.h. die Maschine entwickelt aus der Situation heraus eigene Vorschläge; Auswahl und Priorisierung von Vorschlägen basieren auf einem Algorithmus, der nach *eigenem Gutdünken* auf alle verfügbaren Datenquellen zugreift. Letztendlich entscheidet jedoch der Akteur, welche Vorschläge er annimmt, ablehnt oder verwertet. Ab hier beginnt „Intelligenz" im Sinne der vorgeschlagenen Definition, denn hier ist der Vorschlagsalgorithmus selbstoptimierend, d.h. passt sich an die Bedürfnisse des Benutzers an, lernt aus seinen Entscheidungen, um noch bessere Vorschläge anbieten zu können. Bei **Stufe 4** überlässt der Mensch die Entscheidung der Maschine für vorab definierte Situationen vollständig. Als Beispiel wird die automatische Steuerung des Kühlsystems von Googles Rechenzentrumgenannt. Hier erkennt das System seine Leistungsgrenzen selbst und entwickelt bessere Strategien, um Energie effizienter nutzen zu können. Bei besonders ungewöhnlichen Situationen (z.B. Naturkatastrophen) wird das System allerdings keine adäquaten Entscheidungen mehr treffen können und ein Mensch muss die Kontrolle übernehmen.

Bei den Stufen 1-4 spricht man von einer schwachen KI oder *Artificial Narrow Intelligence* (kurz: ANI).[187]

Stufe 5 hingegen setzt vollständig autonome Entscheidungen voraus. Hier wird dem System dauerhaft und zuverlässig die Kontrolle über Entscheidungen für eine große und komplexe Anwendungsdomäne überlassen; selbst bei Problemfällen und ungewöhnlichen Situationen kann die Maschine autark sinnvolle Entscheidungen treffen. Ein solches System würde als starke KI oder *Artificial General Intelligence* (kurz: AGI) bezeichnet. Derzeit gibt es keine starke KI.[188] Prognosen gehen davon aus, dass eine solche erst gegen Mitte des Jahrhunderts erreicht wird.[189] Voraussetzung hierfür ist allerdings, dass das System mit allen relevanten Daten in

187 *Gausling*, PinG 2019, 61 (62).
188 So wohl auch *Conrad*, DuD 2017, 740.
189 *Gausling*, PinG 2019, 61 (62).

Echtzeit sicher versorgt wird, denn ohne diese kann keine datenbasierte Entscheidung getroffen werden.[190]

Daneben gibt es – zumindest in der Theorie – noch die Superintelligenz (*Artificial Super Intelligence*, kurz: ASI)[191], die in allen Bereichen menschlicher Intelligenz überlegen ist. Sie befindet sich außerhalb menschlichen Vorstellungsvermögens und hätte einen kaum vorstellbaren Einfluss auf die Gesellschaft. Es wird damit gerechnet, dass in der zweiten Hälfte des Jahrhunderts die Superintelligenz geschaffen wird.[192]

Derzeitige People Analytics-Systeme befinden sich zwischen Stufe 3 und 4 der Automatisierungs-Skala, da sie bereits in der Lage sind, mittels (schwacher KI) aus verschiedenen Datenquellen Informationen zu sammeln und Vorschlagslisten mittels Scorings und Rankings zu generieren. Letztlich entscheiden aber vor allem im Bereich Personalmaßnahmen (Einstellung, Versetzung, Kündigung) noch verantwortliche Entscheidungsträger im Unternehmen. Wie das eingangs genannte Beispiel von *Xerox* zeigt,[193] gibt es vor allem in den USA schon mutige Unternehmen, die Einstellungsentscheidungen vollständig einem intelligenten Computeralgorithmus überlassen. Das wäre dann Stufe 4 der Automation.

bb) Veränderungspotential durch KI und Entscheidungsautomatisierung

Durch die Automatisierung von Entscheidungen und Prozessen ist ein hohes Veränderungspotenzial in Organisationen zu erwarten. Sich wiederholende Aufgaben, die nach einem bestimmten Muster ablaufen und bislang von Menschen durchgeführt wurden, können durch intelligente Algorithmen in Computersystemen erledigt werden. Menschliche Entscheidungsträger haben mehr Zeit, innovative und kreative Aufgaben zu erledigen, da sie durch die automatisierten Prozesse entlastet werden.[194]

Mit einhergehend ist somit auch eine Veränderung des Tätigkeitsinhaltes der davon betroffenen Mitarbeiter. So werden beispielsweise HR-Mit-

---

190 *Holtel/Hufenstuhl/Klug*, Künstliche Intelligenz verstehen als Automation des Entscheidens, <www.bitkom.org/sites/default/files/file/import/Bitkom-Leitfaden-KI-verstehen-als-Automation-des-Entscheidens-2-Mai-2017.pdf>, S. 22 f.

191 Diese wurde vom Philosoph *Nick Bostrom* im Jahr 1998 definiert, vgl. *Bostrom*, How long before Superintelligence?, 1998, abrufbar unter: https://nickbostrom.com/superintelligence.html (letzter Abruf am: 11.10.2019).

192 *Gausling*, PinG 2019, 61 (62) m.w.N.

193 *Peck*, The Atlantic 2013 (Dezember 2013).

194 *Bitkom e.V.*, Entscheidungsfindung mit Künstlicher Intelligenz, S. 55.

arbeiter nicht mehr mit dem Sichten und Sortieren von Bewerbungsunterlagen beschäftigt sein, sondern mit dem Trainieren des Systems, ggf. Programmieren und Festlegen der Parameter des Algorithmus und dem Auswerten von gefundenen Mustern durch eingesetzte Software zur Optimierung des Systems. Bei sinnvollem Einsatz erhöht sich die Effizienz fundamental, da die automatisierbaren Prozesse, die zuvor etliche Stunden menschlichen Arbeitseinsatzes erfordert haben, binnen Sekunden durch datenbasierte Auswertungen vorgenommen werden können.

III. Reifegrade der Arbeitnehmeranalyse

Holthaus, *Park* und *Stock-Homburg* haben sich in ihrem Beitrag „People Analytics und Datenschutz - Ein Widerspruch?“[195] mit der Entwicklung der Arbeitnehmeranalyse im zeitlichen Verlauf beschäftigt und in Anlehnung an *Josh Bersin*[196] herausgearbeitet, dass es fünf unterschiedliche Reifegrade von People Analytics in der Praxis gibt.

Level 1 beschreibt den niedrigsten Grad der Auswertung und wird als Operationales Reporting beschrieben, bei welchem lediglich auf Unternehmensanforderungen reagiert wird, beispielsweise durch Auswertung von Lohn- und Gehaltsabrechnungen. Hierbei handelt es sich um einfaches Personalcontrolling, das der Beschreibung des Ist-Zustands dient.[197]

Auf **Level 2** findet bereits ein fortschrittliches Reporting statt, welches durch proaktives und selbstgesteuertes Handeln gekennzeichnet ist, indem das HRM u.a. Mitarbeiterbefragungen und ähnliches durchführt. Die Analyse von Daten erfolgt auf Basis einfacher Verfahren der deskriptiven Statistik, wie Auszählung und Verteilungsparameter wie Mittelwert und Standardabweichung. Beachtet werden muss insbesondere, dass ein statistischer Zusammenhang noch keinen Schluss auf eine Kausalbeziehung zulässt. Für strategische Personalarbeit haben diese Verfahren daher lediglich einen begrenzten Nutzen.[198]

---

195 *Holthaus/Park/Stock-Homburg*, DuD 2015, 676 (678 f.).

196 *Bersin*, Why People Management is Replacing Talent Management, 2015, abrufbar unter: http://joshbersin.com/2015/01/why-people-management-is-replacing-talent-management/ (letzter Abruf am: 17.10.2017).

197 *Mühlbauer/Huff/Süß*, People Analytics und Arbeit 4.0, in: Werther/Bruckner, Arbeit 4.0 aktiv gestalten, S. 110.

198 *Mühlbauer/Huff/Süß*, People Analytics und Arbeit 4.0, in: Werther/Bruckner, Arbeit 4.0 aktiv gestalten, S. 110.

Level 3 ist die strategische Nutzung von Analytics und die Entwicklung von „People Models", wobei auf dieser Stufe bereits Trendanalysen auf Basis vorhandener Daten für langfristige Top-Management-Entscheidungen erstellt werden.

Predictive Analytics ist **Level 4** und ermöglicht, wie der Name bereits erahnen lässt, auf Basis von Vergangenheits- sowie Echtzeitdaten, Prognosen für Zukunftsszenarien zu erstellen. Die Erweiterung zu Stufe 3 ist, dass nicht nur auf Basis bereits vorhandener Daten gearbeitet wird, sondern mithilfe von Echtzeitauswertungen (bspw. durch Sensorik und IT-Daten) schneller agiert und noch genauere Prognosen erstellt werden können.

Stufe 3 und 4 werden in vereinfachten Modellen als fortgeschrittene People Analytics bezeichnet,[199] die Fragen wie „*Beeinflusst die Einführung variabler Vergütung die Arbeitsleistung der Mitarbeiterinnen und Mitarbeiter?*", „*Wirkt sich die Rekrutierung über soziale Medien auf die Qualität der Bewerber für ausgeschriebene Stellen aus?*" etc. beantworten sollen. Mathematisch werden Verfahren der multivariaten Statistik eingesetzt, um Kausalbeziehungen überprüfen zu können. Voraussetzung ist aber eine höhere Datenqualität, sodass beispielsweise auch Längsschnittdaten erhoben werden sollten, m.a.W. die Daten über längere Zeitspannen aufgezeichnet werden, um eine breitere Datenbasis für Auswertungen zu erhalten. Eine Auswertung lediglich einzelner Vorgänge oder Zeitpunkte hingegen bietet keine ausreichende Datenqualität.

Der höchste Reifegrad nach diesem Modell ist **Level 5**, sog. Prescriptive Analytics. Hier beginnen nach *Holthaus*, *Park* und *Stock-Homburg* die sog. **Advanced People Analytics**, bei welcher bereits automatische personalbezogene Entscheidungen gefällt werden. Auf Basis der Analyse von unterschiedlichen Datenquellen sowie der automatisierten Ermittlungen von Szenarien sollen Entscheidungen weitgehend autonom vom System getroffen werden. Jedenfalls sollen diese Systeme relativ zuverlässige Schätzungen auch für noch unbekannte Analyseobjekte generieren.[200] Auf dieser Stufe kommen Verfahren des maschinellen Lernens zum Einsatz, um den Zusammenhang zwischen einzelnen Variablen und Datensätzen zu erkennen und in weiterer Folge den Algorithmus weiter zu optimieren. Die Ergebnisse werden im Einzelfall nicht immer zutreffen, sie haben aber

199 *Mühlbauer/Huff/Süß*, People Analytics und Arbeit 4.0, in: Werther/Bruckner, Arbeit 4.0 aktiv gestalten, S. 110 f.

200 *Mühlbauer/Huff/Süß*, People Analytics und Arbeit 4.0, in: Werther/Bruckner, Arbeit 4.0 aktiv gestalten, S. 112.

bereits einen Mehrwert, wenn die Schätzungen im Mittel häufiger zutreffen als nicht, d.h. die Systeme einen tatsächlichen Mehrwert generieren.[201]

Die vorliegende Arbeit beschäftigt sich mit fortgeschrittenen People Analytics-Modellen, die als Grundlage für EBPM basieren können. Nach dem eben vorgestellten Modell also Level 3, 4 und 5.

§ 3 Vor- und Nachteile bzw. Gefahren von People Analytics

I. Sicherere Prognosen / Erkennen bislang unbekannter Zusammenhänge

Wie bereits herausgearbeitet, können durch KI und Big Data in großen Datenmengen unbekannte Zusammenhänge erkannt und auf Basis der erkannten Muster Prognosen erstellt werden. Diese Prognosen sollen den Entscheidungsträgern im Unternehmen helfen, Entscheidungen zu treffen, indem sie eine (nachvollziehbare) Grundlage hierfür liefern.[202]

Beim Einsatz künstlicher Intelligenz müssen die Entscheider in der Praxis noch nicht einmal die maßgeblichen Entscheidungskriterien kennen, was an folgendem Beispiel verdeutlicht werden soll:[203]

Im Rahmen einer Stellenbesetzung wird eine Software eingesetzt, die in einem ersten Schritt das Arbeitszeugnis analysiert und alle Bewerber, die schlechter als ein „gut" in der Bewertung haben, aussortiert. In einem weiteren Schritt wird die Software mit den Daten aller Beschäftigten versorgt sowie den Fluktuationen. Mit diesen Daten soll das Programm lernen, welche Daten maßgeblich sind, um einen „guten Arbeitnehmer" für das Unternehmen zu rekrutieren. Mit Hilfe eines Scorings der Kriterien soll schlussendlich eine Rangfolge erstellt werden, wobei der beste schlussendlich eingestellt wird. Welche Faktoren in welcher Gewichtung letztendlich hierfür maßgeblich sind, ist Inhalt des neuronalen Netzwerkes, dass die Software beim Lernprozess mit vorhandenen Daten erstellt. Möglicherweise werden hierbei für einen Menschen unidentifizierbare Zusammenhänge erkannt, die zur besten Einstellung führen. Je mehr Daten die Software zur Entscheidung bekommt, desto präziser werden die getroffenen Vorhersagen.

---

201 *Mühlbauer/Huff/Süß*, People Analytics und Arbeit 4.0, in: Werther/Bruckner, Arbeit 4.0 aktiv gestalten, S. 112.

202 *Niklas/Thurn*, BB 2017, 1589.

203 Beispiel aus WHWS/*Broy/Heinson*, B. II. Die automatisierte Einzelfallentscheidung im Beschäftigungsverhältnis, Rn. 5.

Welche Kriterien vom dahinterstehenden neuronalen Netz aber warum in welchem Maße gewichtet wurden, bleibt dem Menschen verborgen. Dennoch führt diese Form der Entscheidung in aller Regel zu präziseren Ergebnissen wie menschliche Entscheidungen.

II. Nachvollziehbarkeit von Entscheidungen

Fortgeschrittenere Systeme, die mit KI arbeiten, haben das eben dargestellte Problem der Nachvollziehbarkeit der Logik. Damit geraten sie in Konflikt mit dem Gesetz. Nach Art. 13 Abs. 2 lit. f), Art. 14 Abs. 2 lit. g) und Art. 15 Abs. 1 lit. h) DSGVO müssen Datenverarbeitern in Fällen der automatisierten Entscheidungsfindung nach Art. 22 Abs. 1 bis 4 DSGVO dem Betroffenen *„aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person*" geben können. Auch bei Verarbeitungsvorgängen, die nicht in eine automatisierte Entscheidung münden, hat der Verarbeiter nach Art. 5 Abs. 2 DSGVO eine Rechenschaftspflicht. Neuronale Netze sind daher höchst problematisch, da diese für den Menschen in vielen Fällen eine Art „Black Box" darstellen.[204] Letzteres gilt im Übrigen auch für Spiele, die immer mehr im Rahmen von People Analytics eingesetzt werden, um Stärken und Schwächen der Bewerber herauszufinden.[205]

Allerdings können datenbasierte Entscheidungen ebenso umgekehrt genutzt werden: Im Rahmen von daten- und evidenzbasiertem Personalmanagement müssen sich Management bzw. Unternehmensführung nicht mehr auf persönliche Intuition verlassen, sondern können ihre Entscheidungen auf Basis von erkannten Mustern in vorhandenen Daten fällen. Der menschliche Entscheidungsprozess ist keine Art „black box" mehr, sondern Entscheidungen werden transparenter, nachvollziehbarer und einheitlich;[206] sie folgen einem ganz bestimmten, berechneten Muster. Vor-

204 Siehe insofern bereits **C. § 2 II. 2. a)**; ferner *Gausling*, PinG 2019, 61 ff.; *Körner*, 2.4 Nachvollziehbarkeit von KI-basierten Entscheidungen, in: Kaulartz/Ammann/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, Rn. 8.

205 *Bodie et al.*, Colorado Law Review 2017, 961 (983).

206 Hiergegen spricht *Wedde* ohne nähere Begründung, dass die menschliche Entscheidung transparenter als eine automatisierte Entscheidung sei, vgl. *Wedde*, Automatisierung im Personalmanagement - arbeitsrechtliche Aspekte und Beschäftigtendatenschutz, <*algorithmwatch.org/de/gutachten-arbeitsrecht-datenschutz-wedde/*>, S. 38.

aussetzung dafür ist, dass der Entscheidungsprozess oder Vorschlag der Software von dieser ausreichend transparent gestaltet ist und für Menschen verständlich begründet wird. Routinemäßige Prozesse lassen sich durch den Einsatz von Algorithmen ressourcensparend optimieren.[207]

Zu beachten ist, dass – wie bereits beschrieben – die Analyseverfahren ein bestimmtes Verhalten oder Ergebnis nicht mit absoluter Sicherheit vorhersagen können, sondern lediglich schätzen. Das Ergebnis solcher Verfahren ist daher nicht „der Weisheit letzter Schluss", sondern lediglich eine andere Methode, Entscheidungen zu treffen. Je nach Einsatzzweck sind die Entscheidungen oft besser als die von einem Menschen getroffenen, manchmal aber auch schlechter. Hinzu kommt, dass das Entscheiden eine Tätigkeit ist, die insbesondere durch menschliches Verhalten wie Erfahrung, Intuition und Hingabe dominiert wird und es hierfür aktuell noch keine plausiblen theoretischen Modelle gibt, die technisch implementiert werden könnten.[208]

III. Diskriminierungsfreie Entscheidungen

Ein weiterer Aspekt, der bei der Diskussion computerbasierten Entscheidungen immer wieder auf der Pro-Seite aufgeführt wird, ist die Verhinderung von Diskriminierungen.[209]

Gleichzeitig wird aber von breiter Seite auch das Risiko erkannt: Beinhaltet der Algorithmus selbst bereits (bewusst oder unbewusst) eine diskriminierende Funktion, so wird diese systematisiert.[210] Als Beispiel kann ein Bewerberauswahlalgorithmus bei Amazon genannt werden: Bereits im Jahr 2014 wurde versucht, einen Algorithmus zu entwickeln, der die Qualifikation von Bewerbern automatisch auf Basis der eingesendeten Lebensläufe bewertet. Das Tool sollte das Recruitment unterstützen, indem es auf Basis von Daten vergangener Bewerbungsprozesse die Kandidaten auf einer Fünf-Sterne-Skala einordnet. Zum Einsatz kam das System allerdings

207 *Bissels/Mayer-Michaelis/Schiller*, DB 2016, 3042.

208 *Bitkom e.V.*, Entscheidungsfindung mit Künstlicher Intelligenz, S. 61.

209 *Lützeler/Kopp*, ArbRAktuell 2015, 491 (492); *Kramer*, "Der Algorithmus diskriminiert nicht", 09.02.2018, abrufbar unter: https://www.zeit.de/arbeit/2018-01/roboter-recruiting-bewerbungsgespraech-computer-tim-weitzel-wirtschaftsinformatiker/komplettansicht?print (letzter Abruf am: 21.01.2019).

210 *Weichert*, ZD 2013, 251-259 (255); *Martini/Nink*, NVwZ 2017, 681 (682); *Martini*, JZ 2017, 1017 (1018); ausführlich *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, S. 81 ff.

nie, da es dazu tendierte, Frauen schlechter zu bewerten als Männer. Es wird vermutet, dass die Überzahl männlicher Arbeitskräfte im IT-Sektor dazu führte, dass der Algorithmus daraus „lernte" und die Schlussfolgerung zog, dass Männer geeigneter als Frauen seien.[211]

Aus diesem Beispiel wird auch die Problematik beim Einsatz von Algorithmen ersichtlich: Entweder finden Algorithmen Muster in bisherigen Entscheidungen oder basieren auf menschlichen Modellierungen, sodass sie auch dessen Vorurteile, Neigungen und Wertungen übernehmen.[212] Diskriminierungen sind Algorithmen grundsätzlich fremd, sie treffen aufgrund von Gruppenwahrscheinlichkeiten Aussagen über Einzelne, sodass strukturelle Ungleichheiten dadurch „zementiert" werden.[213] Indirekte Diskriminierungen sind im Einzelfall schwierig zu erkennen und zu beweisen,[214] da diese nicht auf offensichtlichen Diskriminierungskriterien wie Alter, Geschlecht etc. basieren.

Inzwischen gibt es zur Vermeidung von indirekten Diskriminierungen erste technische Möglichkeiten, die solche erkennen (sollen) und aus den Auswertungen der Algorithmen entfernen.[215] Diese sind jedoch noch nicht ausgereift und können Diskriminierungen noch nicht sicher verhindern.

Andererseits gibt es aber auch Fälle, in denen die Daten der Algorithmen gezielt dazu genutzt werden, um bewusste Diskriminierungen zu verschleiern (sog. „*Masking*").[216] In solchen Fällen werden mittels Algorithmen und Mustererkennung bewusst nicht-sensitive Daten gesucht, an denen der Entscheider seine diskriminierende Entscheidung festmachen und somit die vorsätzlich begangene und verbotene Diskriminierung hinter Daten verstecken kann.[217] So wurden früher insbesondere in den Vereinigten Staaten diskriminierende Entscheidungen oftmals an der Postleitzahl und der Entfernung zum Arbeitsort festgemacht, um hierdurch Minder-

211 Vgl. *Haufe Online Redaktion*, Künstliche Intelligenz im Recruiting: Das halten Bewerber davon, 07.01.2019, abrufbar unter: https://www.haufe.de/personal/hrmanagement/Kuenstliche-Intelligenz-im-Recruiting-Das-halten-Bewerber-davon_80_475156.html (letzter Abruf am: 21.01.2019).
212 *Bodie et al.*, Colorado Law Review 2017, 961 (1016).
213 *Martini*, JZ 2017, 1017 (1018).
214 *Wildhaber*, ZSR 2016, 315 (337).
215 *Wildhaber*, ZSR 2016, 315 (338); instruktiv *Ajunwa et al.*, SSRN Electronic Journal 2016, DOI: 10.2139/ssrn.2746078.
216 *Bodie et al.*, Colorado Law Review 2017, 961 (1025).
217 *Bodie et al.*, Colorado Law Review 2017, 961 (1025 f.).

heiten, die vorwiegend am Stadtrand lebten, auszugrenzen.[218] Im Rahmen des Kreditscorings wäre eine solche Vorgehensweise aufgrund § 31 Abs. 1 Nr. 3 BDSG zumindest in Deutschland verboten; unabhängig von der Europarechtswidrigkeit der Vorschrift[219] stellt sich jedoch die Frage, ob die Wertung des § 31 BDSG, der nach der Gesetzesbegründung nur auf Bonitätsauskünfte anwendbar ist,[220] auf Verarbeitungen im Beschäftigtenkontext ebenfalls angewendet werden kann.[221]

IV. Überwachung der Arbeitnehmer

Für effektive Analysen ist eine große Datenbasis erforderlich. Der Arbeitgeber ist daher dazu geneigt, möglichst viele Daten über den Arbeitnehmer zu speichern.[222] Ohnehin werden im Beschäftigungsverhältnis eine Reihe von Daten zu verschiedensten Zwecken erhoben und gespeichert. Hierzu zählen neben den aus gesetzlichen Gründen notwendigen Daten auch solche wie Zugangskontrolldaten, Kantinenabrechnung, Logdateien von benutzen Maschinen, Internetverlauf, An- und Abmeldedaten etc., die – zumindest aus technischer Sicht – nahezu beliebig miteinander verknüpft werden können. Hierdurch lassen sich zahlreiche neue Aussagen über den Arbeitnehmer gewinnen; der Arbeitgeber gewinnt an „Informationsmacht".[223]

Arbeitnehmer könnten sich hierdurch einem dauernden Überwachungsdruck ausgesetzt fühlen, welcher dazu führt, dass ihre Persönlichkeitsrechte hierdurch verletzt werden. Es muss daher bei der Umsetzung von People Analytics-Maßnahmen, bei denen mittels Überwachung Daten gesammelt werden, genau darauf geachtet werden, keinen unzulässigen Überwachungsdruck auf die Arbeitnehmer auszuüben und nur solche Daten zu sammeln, bei denen das Informationsinteresse des Arbeitgebers das Geheimhaltungsinteresse des Arbeitnehmers überwiegt.[224]

---

218 Vgl. *Bodie et al.*, Colorado Law Review 2017, 961 (1014).
219 Siehe hierzu unten **E. § 1 III. 2. c) bb) (1)**.
220 BT-Drs. 18/11325, S. 101.
221 Dazu später mehr, vgl. **E. § 1 III. 2. c) bb)**.
222 So ist das Erheben und Verknüpfen von Daten ein Umsetzungsschritt in Empfehlungen zu People Analytics-Initiativen, vgl. *Mühlbauer/Huff/Süß*, People Analytics und Arbeit 4.0, in: Werther/Bruckner, Arbeit 4.0 aktiv gestalten, S. 126.
223 *Däubler*, Gläserne Belegschaften, Rn. 36.
224 Zu den Abwägungskriterien und dem -maßstab siehe **D. § 1 III. 2. f)**, **D. § 1 IV. 2. b)**, **E. § 1 I. 1. b)**, **E. § 1 III. 2. a) cc) (4)**, **E. § 4 II. 1**.

V. Datensicherheit

Aufgrund der großen Ansammlungen an (personenbezogenen) Daten beim Arbeitgeber wird auch die Datensicherheit ein immer größeres Thema. Bereits in den Verarbeitungsgrundsätzen thematisiert dies die europäische Verordnung: Nach Art. 5 Abs. 1 lit. f DSGVO müssen Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich Schutz vor unbefugter und unrechtmäßiger Verarbeitung sowie vor unbeabsichtigter Zerstörung und Schädigung. Hierbei müssen geeignete technische und organisatorische Maßnahmen eingesetzt werden (Grundsatz der Integrität und Vertraulichkeit personenbezogener Daten).

Gelangen Unbefugte an solch weitreichende Datensätze, so sind die Mitarbeiter verschiedenen Gefahren wie beispielsweise Identitätsdiebstahl, Betrug oder Erpressung ausgesetzt. So erlangten Hacker bei Sony im Jahr 2014 aufgrund einer unzureichenden Absicherung der Daten über 100 Terrabyte an Beschäftigtendaten, die sie später für missbräuchliche Zwecke nutzten und wofür Sony an die Beschäftigten Schadensersatz leisten musste.[225]

Datenpannen sind in jedem Falle nach Art. 33 DSGVO an die Aufsichtsbehörde zu melden; unter Umständen sind auch die Betroffenen nach Art. 34 DSGVO zu informieren.

§ 4 Mögliche Einsatzszenarien und Werkzeuge von People Analytics

I. Verringerung der Fluktuationsquote

Großflächige Analysen und Untersuchungen können dazu eingesetzt werden, Wechselfaktoren zu finden und zu eliminieren. Dies ermöglicht es, gute Arbeitskräfte im Unternehmen zu halten, hierdurch Kosten zu sparen und Erfahrung sowie Wissen zu sichern. Beispielsweise setzen die Unternehmen *Microsoft* und *Xerox* Analytics im Retention Management ein und haben so bereits 2013 bzw. 2015 das Ziel erreicht, die Fluktuationsquote um 50 % zu verringern, indem sie u.a. Mentoren eingesetzt, spezielle Mitarbeiterbeteiligungsangebote geschaffen oder Gehaltserhöhungen auf Basis der Profile angeboten haben.[226]

---

225 *Bodie et al.*, Colorado Law Review 2017, 961 (1006).
226 *Holthaus/Park/Stock-Homburg*, DuD 2015, 676 (678) m.w.N.

II. Stimmungsbarometer

Durch People Analytics ist es ferner möglich, Stimmungsbarometer auf Team-, Abteilungs-, Unternehmens- oder Überunternehmensebene zu implementieren. So kann beispielsweise durch sog. *Employer Brand Analytics* die „Erfolgswirksamkeit der Arbeitgebermarke" analysiert werden. Ziel ist es, herauszufinden, wie attraktiv ein Arbeitgeber auf potenzielle Bewerber wirkt, um so gezielt an der Marke arbeiten zu können. Im Unternehmen ist es möglich, durch das Erfassen von Schlüsselwörtern in Foren oder Chats, die Meinungen von Beschäftigten zu erfassen, die bestimmte Stimmungen widerspiegeln (sog. *Sentiment Analyse* oder auch *Opinion & Engagement Mining* genannt).[227]

III. Kommunikationsdiagramme / Netzwerk-Analysen

Ebenfalls möglich ist es, die Kommunikation der Beschäftigten untereinander z.B. über E-Mails, Anrufe, interne soziale Netzwerke, Foren o.ä. zu untersuchen, um beispielsweise wichtige Aktoren im betrieblichen Kommunikationsgeflecht zu identifizieren (z.B. „Stimmungsmacher", Schlüsselpersonen).[228] Hierbei können nicht nur die Netzwerke dargestellt werden, sondern auch der Einfluss auf die individuelle Leistung gemessen werden, indem weitere Sensoren wie beispielsweise Smartwatches (sog. *Wearables*) eingesetzt werden.

So kann nicht nur festgestellt werden, wer mit wem kommuniziert. Es gilt auch zu erfahren, wie viele Verbindungen ein Arbeitnehmer zu anderen Arbeitnehmern hat, wie „eng" oder „weit" diese sind und über welche Hierarchieebenen sie sich erstrecken.

Hieraus lassen sich dann beispielsweise Aussagen zur optimalen Arbeitsplatzgestaltung (z.B. Anordnung von Sitzgruppen, offene oder geschlossene Büros etc.) oder aber auch zur optimalen Zusammensetzung von Teams treffen.[229]

---

227 *Holthaus/Park/Stock-Homburg*, DuD 2015, 676 (678).
228 Instruktiv *Höller/Wedde*, Die Vermessung der Belegschaft.
229 *Holthaus/Park/Stock-Homburg*, DuD 2015, 676 (678).

IV. Gesundheitsförderung

Die Analyseergebnisse und Prognosen können präventiv im Rahmen der Gesundheitsförderung eingesetzt werden. So wird es Unternehmen ermöglicht, Ausfall- und Krankheitsquoten zu verringern, indem Risikofaktoren frühzeitig erkannt und somit vermieden werden können. Durch den Einsatz von Künstlicher Intelligenz können Krankheitsmuster bei den Arbeitnehmern erkannt werden, die sich möglicherweise immer nach demselben Schema wiederholen, ein Zusammenhang jedoch durch den Menschen nicht erkannt werden konnte. Dies kann unzählige Ursachen haben: Teilweise genügen schon leicht unterschiedliche Ausgangsparameter, um das Problem zu verdecken. Insbesondere bei psychischen Erkrankungen ist es besonders schwierig, die Ursachen zu evaluieren. Hier könnten automatisierte Auswertungen auf Basis von Verkehrs- und Nutzungsdaten durchaus Rückschlüsse auf die Entstehung geben, die bislang unbekannt geblieben sind. Eine sehr interessante Entscheidung im Bereich der Prävention von Überbelastungen ist 2017 vor dem höchsten deutschen Arbeitsgericht gelandet: Der Arbeitgeber wollte eine Belastungsstatistik für alle Arbeitnehmer in den Außenstellen anfertigen. Insbesondere aufgrund zu umfangreicher und teilweise nicht geeigneter Auswertungen wurde das Vorgehen des Arbeitgebers als unzulässig beurteilt.[230]

V. Selbstkontrolle

Mithilfe von sog. „Dashboards" kann es Arbeitnehmern, Teamleitern oder Abteilungsleitern ermöglicht werden, sich selbst bzw. den eigenen Verantwortungsbereich mit anderen (ähnlichen) im Unternehmen zu vergleichen, um somit eine Selbstkontrolle vornehmen zu können. Hierbei kann beispielsweise die Einbindung in das soziale Netzwerk des Betriebs mit einem Score versehen werden, der eine Selbsteinschätzung ermöglicht sowie einen Vergleich mit anderen Arbeitnehmern des Betriebs (vgl. beispielsweise das *IBM Social Engagement Dashboard*)[231].

Ebenfalls können dem Arbeitnehmer durch ein solches Dashboard auch seine eigenen (schlechten) Gewohnheiten aufgezeigt werden, damit dieser

230 Vgl. BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205 (1205); im Detail unten **E. § 1 III. 2. a) cc) (4) (a).**

231 http://www-935.ibm.com/services/services-offerings/pdf/Intro-Social-Engagement-Dashboard(1).pdf, letzter Abruf am: 24.05.2018.

daran arbeiten kann. So kann beispielsweise anhand von Kalenderdaten und Auswertungen aus E-Mail-Programmen oder des Betriebssystems dem Benutzer angezeigt werden, wie viele Stunden er pro Woche in Meetings verbringt, wieviel Zeit beim Beantworten von E-Mails „verloren" geht und wie viel tatsächlich fokussiert gearbeitet wird.[232] Mit Graphen kann dargestellt werden, wie sich das Verhalten über einen bestimmten Zeitraum verändert hat und somit ggf. auch Prognosen für die Zukunft erstellt werden. Mit weiteren Auswertungen – beispielsweise des unternehmensinternen E-Mail-Servers – lassen sich Aussagen zur Effektivität der E-Mail-Kommunikation treffen, indem dem einzelnen Arbeitnehmer angezeigt wird, wie hoch der Prozentsatz der tatsächlich von anderen gelesenen, versandten E-Mails ist oder wie viele ankommenden E-Mails selbst gelesen werden.[233] Auch diese Auswertungen könnten wieder in einen Vergleich zu anderen (vergleichbaren) Arbeitnehmern im Unternehmen gebracht werden.

Sofern die Auswertungen über sich selbst nur vom Arbeitnehmer eingesehen werden können, dienen diese lediglich der Selbstkontrolle und -optimierung. Technisch möglich wäre es, diese Vergleichsbetrachtungen auf Team-, Abteilungs- und Unternehmensebene durchzuführen, um so die Arbeitnehmer zu überwachen und auf Basis dieser Daten Entscheidungen zu treffen.

VI. Spiele / Gamification

In jüngerer Zeit geht der Trend, insbesondere in den Vereinigten Staaten, dazu, Persönlichkeitseigenschaften von Bewerbern durch Spiele (insbesondere auf dem Mobilgerät) in Erfahrung zu bringen.[234] Hierdurch erhoffen sich die Unternehmer, ein neutraleres Bild von ihren Bewerbern zu bekommen, da die Spiele Spaß machen, die Bewerber hierdurch entspannter sind und sich möglicherweise nicht verstellen. Die Forscher *Bodie*, *Cherry*, *McCormick* und *Tang* haben in ihrer Untersuchung[235] verschiedene Spie-

232 So beispielsweise bei Microsoft Delve MyAnalytics, vgl. *Redmond*, Delve Analytics lets Office 365 users track (and maybe change) bad email habits, 02.03.2016, abrufbar unter: https://www.itprotoday.com/print/79221 (letzter Abruf am: 29.01.2019).

233 *Redmond*, Delve Analytics lets Office 365 users track (and maybe change) bad email habits, 02.03.2016, abrufbar unter: https://www.itprotoday.com/print/79221 (letzter Abruf am: 29.01.2019).

234 *Bodie et al.*, Colorado Law Review 2017, 961 (973 ff.).

235 *Bodie et al.*, Colorado Law Review 2017, 961.

le des Herstellers *Knack* getestet, da diese von namhaften Unternehmen wie *Tom*, *Krispy Kreme* oder *City*[236], aber auch *UBS*, *Daimler*, *Generali*, *DAF*[237] eingesetzt werden. Die Spiele fordern die Spieler auf, zahlreiche Entscheidungen zu treffen, Handlungen vorzunehmen und untersuchen die Reaktionen. Es werden tiefgreifende wissenschaftliche Erkenntnisse versprochen, die den Spielern helfen, ihre Talente zu entdecken und somit die richtigen Entscheidungen zu treffen. Zum Zeitpunkt der Untersuchung lieferten die Spiele jedoch nur wenig überzeugende Ergebnisse, insbesondere waren die Aussagen sehr vage und oberflächlich. Dazu kommt, dass die dahinterstehende Logik für den Benutzer größtenteils eine Black Box ist, da sie nicht wissen, wie ihre Eingaben gewichtet und bewertet werden. Letztlich bemängelten die Forscher auch, dass bei den von den Forschern getesteten Spielen auch „sensitive Informationen" wie Alter, Familienstand, Haushaltseinkommen oder Geschlecht abgefragt wurden. Insbesondere aufgrund der Abfrage von Alter und Geschlecht, Kriterien, die bei einer (üblichen) Bewerbungssituation keine Rolle spielen dürfen (vgl. § 1 AGG), müsste sich ein Arbeitgeber dem Vorwurf der Diskriminierung aussetzen, wenn ein Kandidat ausschließlich auf Basis des Ergebnisses des Spiels ablehnt und dies dem Bewerber so offenbart. Da der Arbeitgeber den dahinterstehenden Quellcode nicht kennt und dieser vom Hersteller nicht veröffentlicht wird, könnte er sich im Rahmen einer Antidiskriminierungsklage nur schwer entlasten, da er nicht beweisen könnte, dass diese unzulässigen Differenzierungskriterien keinen Ausfluss auf das Spielergebnis und somit die Einstellungsentscheidung hatten.

236 *Bodie et al.*, Colorado Law Review 2017, 961 (976) Fn. 89.

237 Auflistung auf der Website: https://www.knackapp.com/#careers, letzter Abruf am: 26.10.2019.

D. Rechtliche Rahmenbedingungen

Um die dargestellten Einsatzszenarien sowie Möglichkeiten und Gefahren rechtlich bewerten zu können, ist es erforderlich, zunächst die rechtlichen Rahmenbedingungen für den Einsatz moderner Technologien wie beispielsweise People Analytics zu klären. Im Fokus steht das Datenschutzrecht, das die Zulässigkeit der Verarbeitung personenbezogener Daten regelt. Ebenfalls muss das Betriebsverfassungsrecht einerseits als Erlaubnistatbestand im Rahmen der Datenverarbeitung als auch als eigenständige Regelung im Rahmen (zwingender) betrieblicher Mitbestimmung betrachtet werden. Am Rande könnte für den Einsatz von Überwachungstechnologien im Bereich des Telekommunikationsrechts auch das TKG bzw. das TMG einschlägig sein. Das Anti-Diskriminierungsrecht, insbesondere die Diskriminierung durch Algorithmen, soll im Rahmen dieser Untersuchung außer Betracht bleiben.

§ 1 Datenschutzrecht

I. Anwendbarkeit des Datenschutzrechts

Der Anwendungsbereich der Datenschutzgrundverordnung wird durch Art. 2 und 3 bestimmt, wobei zwischen dem sachlichen und räumlichen Anwendungsbereich zu differenzieren ist.

1. Sachlicher Anwendungsbereich (Art. 2 DSGVO)

Die DSGVO gilt gem. Art. 2 Abs. 1 für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. In Abs. 2 enthält die Verordnung Ausnahmen für Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen (lit. a), die das auswärtige Handeln der Union und die gemeinsame Außen- und Sicherheitspolitik betreffen (lit. b), durch natürliche Personen zur Ausübung ausschließlich persönlicher oder

familiärer Tätigkeiten (lit. c) sowie durch die zuständigen Behörden im Bereich der Strafverfolgung und öffentlicher Sicherheit (lit. d).

a) Personenbezogene Daten

Personenbezogene Daten im Sinne der DSGVO sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, wobei als identifizierbar eine natürliche Person angesehen wird, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind (Art. 4 Nr. 1 DSGVO).

Eine inhaltliche Änderung des Begriffs im Vergleich zur DS-RL ist nicht gegeben.[238] Es werden lediglich weitere zusätzliche Beispiele aufgeführt, wann ein Personenbezug hergestellt werden kann, wie beispielsweise die Zuordnung zu einer Kennung wie einem Namen, Standortdaten oder einer Online-Kennung.[239]

Der Begriff der personenbezogenen Daten wurde ursprünglich aus dem Übereinkommen Nr. 108 des Europarats[240] übernommen, allerdings mit der Modifikation, dass die Bestimmbarkeit als direkte oder indirekte Identifizierbarkeit verstanden werden soll.[241]

Angaben zu einer juristischen Person sind keine personenbezogenen Daten, da ausschließlich natürliche Personen erfasst sind.[242] Aus Erwägungsgrund 27 der Verordnung ergibt sich ferner, dass die Verordnung nur für lebende natürliche Personen gilt, die Mitgliedsstaaten allerdings

238 EuArbRK/*Franzen*, Art. 4 DSGVO Rn. 2; *Karg*, DuD 2015, 520 (521); *Buchner*, DuD 2016, 155.

239 *Buchner*, DuD 2016, 155 f.

240 Übereinkommen Nr. 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarats vom 28.01.1981; das Übereinkommen ist online unter https://www.coe.int/de/web/conventions/full-list/-/conventions/rms/0900001680078b38 abrufbar (letzter Abruf am: 20.06.2018).

241 *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 2 Rn. 2.

242 Paal/Pauly/*Ernst*, Art. 4 DSGVO Rn. 4 mit Verweis auf EuGH, Urt. v. 09.11.2010 – C-92/09, C-93/09, Tz. 52 – Schecke und Eifert zu Art. 7, 8 EU-GRCh.

Vorschriften für die Verarbeitung personenbezogener Daten von Verstorbenen vorsehen können.

b) Verarbeitung personenbezogener Daten

Eine Verarbeitung liegt nach Art. 4 Nr. 2 DSGVO bei jedem ausgeführten Vorgang oder jeder Vorgangsreihe im Zusammenhang mit personenbezogenen Daten vor, sei es mit oder ohne Hilfe automatisierter Verfahren.

Gesetzlich beispielhaft[243] genannt werden die folgenden Vorgänge: das Erheben, Erfassen, die Organisation, das Ordnen, die Speicherung, Anpassung oder Veränderung, das Auslesen, Abfragen, die Verwendung, Offenlegung durch Übermittlung, Verbreitung oder anderer Form der Bereitstellung, der Abgleich oder die Verknüpfung, Einschränkung, das Löschen oder Vernichten von personenbezogenen Daten.

Sprachlich ist der Verarbeitungsbegriff der DSGVO zwar weiter gefasst als jener der Vorgängerreglung, inhaltlich jedoch nahezu identisch.[244]

c) Dateisystem

Während die DS-RL den Begriff „Datei" verwendete, wurde mit der DSGVO der Begriff „Dateisystem" eingeführt, welcher in Art. 4 Nr. 6 DSGVO definiert ist als *jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.*

Da die Begriffsbestimmung des „Dateisystems" der Definition der Datei in der DS-RL entspricht, ist trotz Änderung der Begrifflichkeit nicht von einer sachlichen Änderung auszugehen.[245]

Das Dateisystem darf nicht mit dem Begriff des Computerdateisystems (wie beispielsweise NTFS, FAT32 etc.) verwechselt werden. Es bezeichnet eine „strukturierte Sammlung". Mithin ist das Kriterium vor allem für die

---

243 Die Aufzählung ist nicht abschließend, vgl. *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 2 DSGVO Rn. 14.

244 EuArbRK/*Franzen*, Art. 4 DSGVO Rn. 7; Paal/Pauly/*Ernst*, Art. 4 DSGVO Rn. 20:weiter gefasster Begriff als der Verarbeitungsbegriff des BDSG a.F. (jedoch ohne materielle Folgen).

245 So auch Paal/Pauly/*Ernst*, Art. 4 DSGVO Rn. 52.

nicht-automatisierte Verarbeitung relevant; das Computerdateisystem hingegen ist im Rahmen des Datenschutzes irrelevant, da letzteres lediglich die technische Weise regelt, wie Daten auf einer Festplatte abgespeichert werden.

Beispiele für das Vorliegen eines Dateisystems sind beispielsweise eine alphabetische Ordnung nach Personennamen oder eine nach Eingang geordnete Kundenliste,[246] aber auch Papier-Personalakten, Krankenblätter oder anderweitig strukturierte Karteikartensammlungen.[247]

Kein Dateisystem hingegen ist eine ungeordnete Sammlung an Post-Its, die am Rande eines Computerbildschirms kleben oder ein chaotischer Papierstapel auf dem Schreibtisch.[248]

d) Zwischenergebnis

Der sachliche Anwendungsbereich im privatrechtlichen Bereich ist grundsätzlich eröffnet, sofern bei den verarbeiteten Daten ein Personenbezug herstellbar ist. Da People Analytics-Verfahren in der Praxis ausschließlich computerbasiert sind, ist nicht weiter zu prüfen, ob die Daten eine gewisse Struktur (*Dateisystem*) aufweisen.

2. Räumlicher Anwendungsbereich (Art. 3 DSGVO)

Nach Art. 3 Abs. 1 DSGVO findet die Verordnung Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeit einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob der Verarbeitungsvorgang selbst in der Union stattfindet. Abs. 2 erweitert den Bereich auch auf einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter. Voraussetzung dafür ist, dass sich die betroffenen Personen in der Union befinden und die Datenverarbeitung im Zusammenhang damit steht, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffe-

246 GHN (40. Aufl. 2009)/*Brühann*, Art. 2 Richtlinie 95/46/EG Rn. 15.
247 Paal/Pauly/*Ernst*, Art. 4 DSGVO Rn. 54.
248 Zu beachten ist aber, dass nach § 26 Abs. 7 BDSG auch solche dem Datenschutzrecht unterliegen, wenn hierauf personenbezogene Daten von Beschäftigten enthalten sind.

nen Personen eine Zahlung zu leisten ist (lit. a) oder das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt (lit. b). Insbesondere die letztere Alternative ist für Arbeitgeber relevant, wenn sie Cloud- oder Analytics-Anbieter beispielsweise aus den Vereinigten Staaten einsetzen und die Verarbeitung dort stattfinden soll. Hierbei sind die Art. 44 ff. DSGVO zu beachten, die die Zulässigkeit der Übermittlung personenbezogener Daten an Drittländer regeln.

Im Gegensatz zur alten Regelung kommt es im Rahmen des räumlichen Anwendungsbereichs nunmehr auf den Aufenthaltsort des Betroffenen an, dessen Daten verarbeitet werden.[249] Es gilt das sog. Marktortprinzip. Der Anwendungsbereich der DSGVO gegenüber der Richtlinie wurde somit deutlich erweitert.[250] Streitigkeiten darüber, welches Datenschutzrecht anwendbar ist, sind somit obsolet;[251] der Schutzstandard der DSGVO wird hierdurch für Beschäftigte in der Europäischen Union weltweit garantiert.

3. Verhältnis zwischen der DSGVO und dem BDSG

Die Datenschutzgrundverordnung stellt aufgrund ihres vollharmonisierenden Charakters und dem weiteren Anwendungsbereich eine „Basisregelung" dar, deren Unanwendbarkeit explizit begründet werden muss.[252] Nationales Recht ist lediglich dann einschlägig, wenn eine Öffnungs- oder – wie im Bereich des Beschäftigtendatenschutzes (Art. 88 DSGVO) – Spezifizierungsklausel (dazu sogleich) den Mitgliedstaaten erlaubt, in bestimmten Bereichen eigene Regelungen zu treffen oder die abstrakten Vorgaben der DSGVO zu präzisieren.[253] Aufgrund des Vereinheitlichungsziels der DSGVO sind die Regelungsspielräume allerdings begrenzt, um das erstrebte Ergebnis nicht zu gefährden.[254]

249 *Härting*, DSGVO, Rn. 220.
250 Paal/Pauly/*Ernst*, Art. 3 DSGVO Rn. 13; EuArbRK/*Franzen*, Art. 3 DSGVO Rn. 4.
251 *Buchner*, DuD 2016, 155 (156).
252 *Wolff*, C. I. Die Regelungswerke im Überblick, in: Schantz/Wolff, Das neue Datenschutzrecht, Rn. 211.
253 Vgl. *Roßnagel*, § 1 II. Inhalte der Datenschutz-Grundverordnung, in: Roßnagel, Das neue Datenschutzrecht, Rn. 12 f.
254 *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 194.

4. Keine Anwendung bei nicht-personenbezogenen Daten

Das Datenschutzrecht findet keine Anwendung, sofern es sich um nicht-personenbezogene Daten handelt. Für die Entscheidung, ob ein Personenbezug besteht bzw. herstellbar ist, kommt es auf die Frage an, ob eine Person identifizierbar ist. Hierfür gibt Erwägungsgrund 26 weitere Hinweise. Demnach sollen für die Beurteilung alle Mittel berücksichtigt werden, die entweder von dem Verantwortlichen für die Verarbeitung oder von einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern.

Bereits unter dem alten Datenschutzregime war umstritten, wann eine Person als bestimmbar gilt, wobei zwischen dem objektiven (absoluten bzw. theoretischen) und relativen (praktischen) Ausschluss der Bestimmbarkeit unterschieden wurde.[255] Die Verfechter der absoluten Theorie wandten das Datenschutzrecht solange an, bis es objektiv unmöglich war, die Person zu re-identifizieren; nach dieser Theorie blieb es außer Betracht, welcher ökonomischer, zeitlicher und technologischer Aufwand erforderlich ist, um die Person zu bestimmen.[256] Die herrschende Meinung[257] schloss sich allerdings der relativen Theorie an, wonach das Datenschutzrecht nicht angewandt wurde, wenn das Risiko, dass die Person bestimmt wird, so gering ist, dass es „praktisch irrelevant erscheint".[258] Dieser Streit hat sich aufgrund der nahezu identischen Formulierung in der DSGVO (statt „bestimmbar" nunmehr „identifizierbar") leider immer noch nicht endgültig erledigt.[259]

Kernfrage ist weiterhin, inwieweit das Wissen Dritter bei der Frage der Identifizierbarkeit zu berücksichtigen ist, bzw. ab wann es „nach allgemeinem Ermessen wahrscheinlich genutzt wird". Hier hilft Erwägungsgrund 26 S. 4 weiter, welcher bestimmt, dass bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, alle objektive Faktoren, wie die Kosten der

255 *Dammann*, in: Simitis, Bundesdatenschutzgesetz, § 3 BDSG Rn. 23; *Boehme-Neßler*, DuD 2016, 419 (420).

256 Vgl. *Dammann*, in: Simitis, Bundesdatenschutzgesetz, § 3 BDSG Rn. 23; *Boehme-Neßler*, DuD 2016, 419 (420).

257 Statt aller LG Berlin, Urt. v. 31.01.2013 – 57 S 87/08, ZD 2013, 618 (619 f.) m.w.N.

258 *Dammann*, in: Simitis, Bundesdatenschutzgesetz, § 3 BDSG Rn. 23.

259 *Karg*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 1 DSGVO Rn. 7.

Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden sollen, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Fest steht jedenfalls, dass nicht nur das Wissen des Verantwortlichen, sondern auch von Dritten zu berücksichtigen ist.[260]

Die Berücksichtigung verfügbarer Technologie und Entwicklungen ist eine ausdrückliche Neuerung zum bisherigen Verständnis und zeigt auf, dass besonders auf die auf dem Markt verfügbaren technischen Möglichkeiten geachtet werden muss (bspw. die Problematik von *Big Data*).[261] Zu beachten ist allerdings, dass der Verantwortliche diese Technologie auch wahrscheinlich nutzen muss (Erwägungsgrund 26 S. 3), also solche Technologien außer Betracht bleiben, die „vernünftigerweise" nicht eingesetzt werden bzw. auch Dritte außer Betracht bleiben, an die sich der Verantwortliche „vernünftigerweise" nicht wendet.[262] Dies ist grundsätzlich dann der Fall, wenn ein unverhältnismäßiger Aufwand an Zeit, Kosten und Arbeitskräften erforderlich wäre, „sodass das Risiko einer Identifizierung *de facto* als vernachlässigbar" erscheint[263] oder wenn der Dritte schlichtweg nicht zur Verfügung steht. Hier schlägt sich der risikobasierte Ansatz der Datenschutzgrundverordnung nieder: Besteht kein Risiko für die Grundrechte der betroffenen Person, so muss ein Verarbeiter auch keine besonderen Schutzvorkehrungen treffen.

Voraussetzung ist allerdings, dass die Verknüpfung der Daten zur Identifikation rechtlich zulässig ist und der Zugriff auf die Mittel und das Wissen des bzw. der Dritten vernünftigerweise durch den Verantwortlichen vorgenommen werden könnte.[264] Nicht erforderlich ist, dass tastsächlich die Herstellung eines Personenbezugs erfolgt.[265]

---

260 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 2 f., die daraus fälschlicherweise auf die absolute Betrachtungsweise abstellen: „Wie schon die DS-RL folgt die DSGVO der absoluten Betrachtung.".

261 *Krügel*, ZD 2017, 455 (456).

262 Generalanwalt beim EuGH (Generalanwalt) Sánchez-Bordona, Schlussantrag v. 12.05.2016 – C-582/14, BeckRS, 2016, 81027 (Rn. 68) – Breyer.

263 EuGH, Urt. v. 19.10.2016 – C-582/14, NJW, 2016, 3579 (Rn. 46) – Breyer; kritisch *Richter*, EuZW 2016, 909 (913)

264 EuGH, Urt. v. 19.10.2016 – C-582/14, NJW, 2016, 3579 (Rn. 47-49) – Breyer.

265 *Karg*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 1 DSGVO Rn. 61.

a) Begriff der Identifikation

Obwohl im alltäglichen Sprachgebrauch unter Identifikation die Identifizierung einer Person mit ihrem Namen verstanden wird, geht mit der Änderung des Wortlauts gegenüber der DS-RL keine inhaltliche Änderung dahingehend einher, dass es erforderlich wäre, dass die Person mit ihrem Namen identifiziert werden kann, um das Datenschutzrecht anzuwenden.[266] Dies ergibt sich bereits aus dem Wortlaut der Vorschrift selbst, nachdem eine Person als identifizierbar angesehen wird, „die direkt oder indirekt mittels Zuordnung zu einer Kennung wie einem Namen, Kennnummer" etc. identifiziert werden kann.

Ein engeres Verständnis würde nicht nur dem Wortlaut widersprechen, sondern auch dem Schutzzweck der DSGVO erkennbar zuwiderlaufen.[267] Es ist daher wie bereits bei der Datenschutzrichtlinie[268] ausreichend, dass die Daten einer natürlichen Person zugeordnet werden können und somit individualisiert bzw. singularisiert sind (beispielsweise durch eine Passnummer, Telefonnummer, ein Foto o.ä.). Bereits aus solchen Daten kann „Stück für Stück ein Bild von der Persönlichkeit der Person" erstellt werden und diese aufgrund der vorliegenden Daten mit bestimmten Entscheidungen in Zusammenhang gebracht werden.[269]

Wie sich bereits aus Erwägungsgrund 26 ergibt, reicht bereits die negative Identifizierung durch das Aussondern aus, um eine Identifizierbarkeit anzunehmen. Dies stützt einerseits die Argumentation, dass die Kenntnis des Namens nicht erforderlich ist, verdeutlicht andererseits aber bereits an dieser Stelle, dass auch bei vermeintlich aggregierten bzw. anonymisierten Daten ein Personenbezug vorhanden sein kann, wenn eine Person aus der Gruppe so signifikante Merkmale hat, dass diese beispielsweise trotz Löschung personenbezogener Daten noch erkennbar bleibt.

---

266 Paal/Pauly/*Ernst*, Art. 4 DSGVO Rn. 8; EuGH, Urt. v. 19.10.2016 – C-582/14, NJW, 2016, 3579 (3581) – Breyer Rn. 41, 44; *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff "personenbezogene Daten", S. 16.

267 *Karg*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 1 DSGVO Rn. 49.

268 *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff "personenbezogene Daten", S. 16; *Karg*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 1 DSGVO Rn. 49; BeckOK DatenSR/*Schild*, Art. 4 DSGVO Rn. 17 f.

269 *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff "personenbezogene Daten", S. 16.

b) Anonymisierung

Erst wenn die Daten so anonymisiert sind, dass die betroffene Person nicht mehr identifiziert werden kann, finden die DSGVO und ihre Schutzprinzipien keine Anwendung mehr.[270]

Da People Analytics und ähnliche Verfahren zu einem großen Teil mit „anonymisierten" bzw. aggregierten Daten durchgeführt werden und nur im Ausnahmefall dazu dienen, Analysen zu einer bestimmten Person durchzuführen[271], ist genauer auf die Frage der wirksamen Anonymisierung im Sinne der DSGVO einzugehen, mit der Folge, dass das Datenschutzrecht keine Anwendung mehr findet.

Durch die Nutzung von immer effektiveren und leistungsstärkeren Auswertungsalgorithmen stehen selbst ursprünglich als sehr effektiv geltende Anonymisierungstechniken unter Verdacht, den Personenbezug nicht mehr ausreichend aus den Daten zu entfernen, um aus dem sachlichen Anwendungsbereich der DSGVO zu fallen.[272] Teilweise wird sogar davon gesprochen, dass jede Anonymisierung auf Dauer unmöglich gemacht wird,[273] wobei hier die relative Dimension der Identifizierbarkeit in aller Regel außer Acht gelassen wird.[274] Auf technischer Seite werden seit Jahren verschiedene Techniken der Anonymisierung (z.B. Löschen oder Aggregation von Identifizierungsmerkmalen, Verwenden einer Einweg-Verschlüsselung oder Verrauschen von Auswertungsergebnissen[275]) untersucht und getestet, wobei festgestellt wurde, dass es nicht „den einen" Anonymisierungsalgorithmus gibt, sondern je nach Einsatzszenario bei verschiedenen Techniken, verschiedene Vor- und Nachteile bestehen und daher im Einzelfall geprüft werden muss, welcher Algorithmus geeignet ist.[276]

---

270 Erwägungsgrund 26 S. 5.
271 *Reindl/Krügl*, People Analytics in der Praxis, S. 73 f.
272 *Karg*, DuD 2015, 520.
273 *Boehme-Neßler*, DuD 2016, 419; Beispiele bei *Katko/Babaei-Beigi*, MMR 2014, 360 (361 f.): Ein Personenbezug ist fast immer herstellbar.; wohl auch *Sarunski*, DuD 2016, 424 (427).
274 So beispielsweise auch bei *Dorschel*, Praxishandbuch Big Data, S. 191.
275 *Wójtowicz*, PinG 2013, 65 (67).
276 Einen Überblick gibt es im Annex des WP 216 der Art. 29-Datenschutzgruppe: *Article 29 Data Protection Working Party*, Opinion 05/2014 on Anonymization Techniques (WP 216), S. 16 ff.; weitere Anonymisierungstechniken sowie deren Vor- und Nachteile finden sich bei *Götz*, Big Data im Personalmanagement, S. 75 ff.

c) Pseudonymisierung

Zu unterscheiden ist die Anonymisierung von der Pseudonymisierung: Bei letzterer werden die Daten so verarbeitet, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen (im Folgenden: „Schlüssel") nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden (Art. 4 Nr. 5 DSGVO).

Ziel der Pseudonymisierung ist die Entkoppelung der ursprünglich personenbezogenen Daten von den betroffenen Personen, um vor allem dem Grundsatz der Datenminimierung Rechnung zu tragen.[277] Gleichzeitig handelt es sich auch um eine technisch-organisatorische Maßnahme zum Datenschutz, die das Risiko für die Betroffenen reduziert[278]; wenn nicht jeglicher Verarbeitungsvorgang mit Daten stattfindet, die einen direkten Personenbezug ermöglichen, sondern eine Zusammenführung des Schlüssels mit den Daten erst dort stattfindet, wo es unbedingt wieder notwendig ist. Somit unterstützt die Pseudonymisierung die Verantwortlichen bei der Einhaltung ihrer Datenschutzpflichten (Erwägungsgrund 28).

Im Vergleich zur Anonymisierung bietet die Pseudonymisierung für den Verarbeiter den Vorteil, dass es möglich ist, die Datensätze bzw. Nutzungsvorgänge weiterhin mit Hilfe des Pseudonyms (etwa einer ID) zu verketten und somit neue Daten korrekt zum selben Profil bzw. derselben ID zuzuordnen. Ebenfalls kann das Verwenden von Pseudonymen die Wahrnehmung von Betroffenenrechten unter dem Pseudonym unterstützen und eine gezielte Re-Identifizierung ermöglichen.[279]

Die Pseudonymisierung hat folglich mehrere Wirkungen:

aa) Risikomindernde Wirkung

Im Grundsatz hat die Pseudonymisierung eine risikominimierende Wirkung. Dies verdeutlicht auch Erwägungsgrund 28, welcher explizit davon spricht, dass die Anwendung der Pseudonymisierung die Risiken für die

277 *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 5 Rn. 1.
278 *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 5 Rn. 2.
279 *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 5 Rn. 20.

betroffenen Personen senken kann und die Verarbeiter und Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen kann. Es ist jedoch nicht beabsichtigt, andere Datenschutzmaßnahmen durch die Pseudonymisierung auszuschließen.

Im Kern stellt die Pseudonymisierung daher keine Anonymisierungs-, sondern eine Sicherungsmaßnahme dar.[280] Durch die Pseudonymisierung sollen insbesondere der Datenschutzgrundsatz der Datenminimierung (Art. 5 Nr. 1 lit. c DSGVO) sowie Datenschutz durch Technikgestaltung und *Privacy by Design* (Art. 25 DSGVO) verwirklicht werden. Ebenfalls wird die Datensicherheit erhöht (Art. 32 Abs. 1 lit. a DSGVO).[281]

bb) Keine anonymisierende Wirkung der Pseudonymisierung

Obwohl derjenige, der die pseudonymisierten Daten verarbeitet, ohne den Schlüssel keinen Personenbezug herstellen kann, bestimmt Erwägungsgrund 26 S. 2, dass pseudonymisierte Daten als Informationen über eine identifizierbare natürliche Person betrachtet werden sollten.[282]

(1) Relative Dimension der Identifizierbarkeit

Teile der Literatur kritisieren allerdings, dass diese Bestimmung zu pauschal gefasst sei:[283] Es sei die relative Dimension der Identifizierbarkeit[284] zu beachten, sodass bei der Übermittlung der Daten an einen Dritten diese für den Dritten durchaus anonymisierte Daten sein könnten, sofern nur der Übermittler den Schlüssel besitzt und der Dritte „vernünftigerweise"

280 *Article 29 Data Protection Working Party,* WP 203, S. 3; *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 266; *Helfrich/Forgó/Schneider*, Teil I. Kapitel 5. Grundsätze der datenschutzrechtlichen Prüfung, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Rn. 24: Pseudonymisierung als "datenschutzfreundlicher Umfang mit personenbezogenen Daten".

281 *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 5 Rn. 16.

282 Vgl. *Laue/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis, § 1 Rn. 22: „Einen Sonderfall personenbezogener Daten bieten pseudonymisierte Daten."; BeckOK DatenSR/*Schild*, Art. 4 DSGVO Rn. 78; *Härting*, DSGVO, Rn. 300; hiergegen *Götz*, Big Data im Personalmanagement, S. 82: „Daten, die Art. 4 Nr. 5 DSGVO unterfallen, sind nämlich gleichzeitig anonyme Daten, wenn der Verantwortliche nicht über die Zuordnungsregel verfügt."

283 *Roßnagel*, ZD 2018, 243 (244).

284 Siehe bereits oben **D. § 1 I. 4. a**).

keinen Zugriff darauf erhält.[285] In diesem Fall handle es sich nach Art. 4 Nr. 1 Hs. 2 DSGVO nicht mehr um personenbezogene Daten.

Insbesondere zur alten Rechtslage wurde vertreten, dass die Pseudonymisierung immer dann anonymisierende Wirkung hat, wenn der Verarbeiter, welchen den Schlüssel nicht besitzt, „vernünftigerweise" keinen Personenbezug mehr herstellen kann.[286] Auch unter Geltung der neuen Rechtslage wird weiterhin vertreten, dass sich dies bereits aus der Definition der personenbezogenen Daten gemäß Art. 4 Nr. 1 Hs. 2 DSGVO ergebe.[287] Gestützt wird die Argumentation teilweise darauf, dass die *Art. 29-Gruppe* dies bereits unter alter Rechtslage so für den Gesundheitsbereich angedeutet habe.[288] Ferner wird die Argumentation auf die – inzwischen überholte – Rechtsprechung des EuGHs zu dynamischen IP-Adressen gestützt:[289] In der Rs. *Breyer* stellte der EuGH darauf ab, dass IP-Adressen als Pseudonyme *jedenfalls* dann personenbezogene Daten sind, wenn die verantwortliche Stelle eine Möglichkeit hat, auf die Zusatzinformationen zuzugreifen, wobei auch das Wissen Dritter (hier die staatlichen Behörden) in die Betrachtung miteinzubeziehen ist. Im Umkehrschluss also dann keine personenbezogenen Daten wären, wenn der Provider die Information über die Zuordnung der IP-Adresse zum Anschluss bereits gelöscht hat oder eine Zugriffsmöglichkeit nicht besteht.

(2) Kritik

Die Vertreter dieser Auffassung übersehen allerdings, dass im Vergleich zu anonymen Daten bei pseudonymisierten Daten ein „Mehr" (nämlich der

285 *Schwartmann/Weiß*, Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für die Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017, S. 14; wohl auch *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 270.

286 Vgl. *Schwartmann/Weiß*, Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für die Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017, S. 14; zur alten Rechtslage *Scholz*, in: Simitis, Bundesdatenschutzgesetz, § 3 BDSG Rn. 217a ff.; kritisch *Buchner*, 2 Grundsätze des Datenschutzrechts, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 230 ff.; zur alten Rechtslage *Dammann*, in: Simitis, Bundesdatenschutzgesetz, § 3 BDSG Rn. 67.

287 *Roßnagel*, ZD 2018, 243 (244).

288 Vgl. Beispiel 13, in: *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff "personenbezogene Daten", S. 18.

289 EuGH, Urt. v. 19.10.2016 – C-582/14, NJW, 2016, 3579 – Breyer.

Schlüssel bei mindestens einem Verantwortlichen) vorhanden ist, welches zur Identifizierung führen kann; die Pseudonymisierung ist daher sauber von der Anonymisierung abzugrenzen. [290] Derjenige, der den Schlüssel besitzt, kann die pseudonymisierten Daten durchaus ohne großen Aufwand wieder einer natürlichen Person zuordnen,[291] sodass jedenfalls ein größeres Risiko der Re-Identifizierung besteht als bei vollständiger Anonymität. Auch ist die Zweckbestimmung der Daten eine andere: Pseudonymisierte Daten sind grundsätzlich dazu bestimmt, durch mindestens eine Stelle wieder zu einer natürlichen Person zugeordnet zu werden.[292] Falls nicht, liegt bereits in der Speicherung des Schlüssels ein Verstoß gegen den Grundsatz der Datenminimierung. Aus diesem Grund sind jedenfalls pauschalisierte Aussagen dahingehend, dass pseudonymisierte Daten für Dritte (ohne den Schlüssel) immer anonyme Daten sind, falsch.[293]

Auch der Verweis auf die EuGH-Rechtsprechung in der Sache *Breyer* geht fehl, da diese noch unter der Geltung der DS-RL entschieden wurde, welche im Gegensatz zur DSGVO eine dem Erwägungsgrund 26 entsprechende Bestimmung gerade nicht enthielt. Zudem ließ der EuGH offen, ob es sich um personenbezogene Daten handelt, wenn kein Zugriff des Verantwortlichen über Dritte möglich ist.

(3) Lösungsvorschlag von Buchner

Buchner schlägt folgende Lösung der Problematik vor: Pseudonymisierte Daten stellen auch im Verhältnis zu Dritten personenbezogene Daten dar, sofern es sich bei der datenverarbeitenden Stelle nicht um eine Stelle mit besonderen Vertraulichkeitspflichten und -rechten handelt[294] und somit auch mit hinreichender Wahrscheinlichkeit gesichert ist, dass Dritte keinen Zugriff auf die Daten erhalten. Erst wenn es sich um ein „selbstgeneriertes Pseudonym“ (durch den Betroffenen) oder ein irreversibles Pseudonymisierungsverfahren handle, das von Dritten nicht oder nur mit

290 *Laue/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis, § 1 Rn. 25, 28.
291 *Laue/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis, § 1 Rn. 27.
292 *Knopp*, DuD 2015, 527 (529).
293 *Knopp*, DuD 2015, 527 (529); so aber *Götz*, Big Data im Personalmanagement, S. 83, der auf eine "anonymisierende Wirkung der Pseudonymisierung" abstellt.
294 *Buchner* konkretisiert dies nicht, allerdings dürften hiermit Berufsgeheimnisträger i.S.d. nach § 203 StGB gemeint sein, die nach § 53 StPO auch ein Zeugnisverweigerungsrecht gegenüber Behörden haben.

einem unverhältnismäßig großen Aufwand wieder der Person zugeordnet werden kann, handle es sich um anonyme Daten.[295]

Dem könnte entgegengesetzt werden, dass es bei einer solchen Sichtweise möglich wäre, unter dem Pseudonym (beispielsweise pseudo0180@email.de) ein unbegrenzt großes und detailliertes Persönlichkeitsprofil zu erstellen, das später mitunter sehr einfach einer Person zugeordnet werden könnte (im obigen Beispiel: wenn die Person hinter der E-Mail-Adresse bekannt wird[296]).[297] Je mehr Informationen letztlich über eine konkrete Person gesammelt werden (z.B. zu einem Pseudonym), desto einfacher ist die Identifizierung. Ferner ist es für den Verarbeiter kaum zu kontrollieren, ob ein selbstgeneriertes Pseudonym einfach oder schwer einer identifizierbaren Person zugeordnet werden kann. So könnte es sein, dass ein beträchtlicher Personenkreis Pseudonym „pseudo0180@email.de" einer natürlichen Person zuordnen kann, da der Adressinhaber beim Versand von E-Mails unter dieser Adresse unter Klarnamen auftritt. Dies könnte dem Verarbeiter verborgen bleiben und die DSGVO wäre nach dieser Auffassung unerkannt anwendbar.

(4) Stellungnahme

Die bislang vertretenen Ansätze zur Lösung der Problematik gehen fehl und verorten das Problem auf der falschen Ebene, indem sie versuchen, bereits die Anwendbarkeit der DSGVO durch Pseudonymisierungsmaßnahmen auszuschließen.[298] Aus Erwägungsgrund 26 ergibt sich, dass – jedenfalls in Bezug auf die Pseudonymisierung – ein objektiver Ansatz vertreten wird, es also nicht darauf ankommt mit welcher Wahrscheinlichkeit der Betroffene hinter dem Pseudonym identifiziert werden kann. Dies wird dadurch deutlich, dass auch pseudonymisierte Daten grundsätzlich personenbezogene Daten darstellen, auch wenn diese an einen Dritten, der den Schlüssel nicht hat, weitergegeben werden.

---

295 *Buchner*, 2 Grundsätze des Datenschutzrechts, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 235 Rn. 38.

296 Auf diese Gefahr weist beispielsweise *Scholz*, in: Simitis, Bundesdatenschutzgesetz, § 3 BDSG Rn. 220a und Fn. 408 hin.

297 Diese Gefahr wird bereits in Erwägungsgrund 30 der DSGVO angesprochen, vgl. *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 59 Fn. 8; ferner *Schantz/Wolff*, Das neue Datenschutzrecht, Rn. 293 f.

298 In diese Richtung bereits *Knopp*, DuD 2015, 527 (530).

Übersehen wird hierbei, dass die Anwendbarkeit der DSGVO bei der Verwendung von Pseudonymen nicht jegliche Weitergabe an Dritte verhindert, sondern spätestens im Rahmen der Abwägungsklausel des Art. 6 Abs. 1 lit. f DSGVO[299] berücksichtigt werden muss.[300] Bei entsprechender Sicherheit der Pseudonymisierung kann diese durchaus ähnlich privilegierende Wirkung im Rahmen der Verarbeitung wie eine Anonymisierung haben.[301] Für diese Sichtweise spricht nicht nur die positive Berücksichtigung der Pseudonymisierung bei einer zweckändernden Verarbeitung gem. Art. 6 Abs. 4 lit. e DSGVO, sondern auch eine Betrachtung des Gesetzgebungsprozesses: Im Rahmen der Verhandlungen wurde eine generelle Privilegierung der Verarbeitung pseudonymisierter Daten vorgeschlagen, welche jedoch keinen Eingang in den Verordnungstext gefunden hatte.[302]

Durch die Anwendung der DSGVO ist sichergestellt, dass die betroffene Person ihre Betroffenenrechte nach den Art. 15 - 20 DSGVO, insbesondere das ihr zustehende Auskunftsrecht nach Art. 15 geltend machen kann. Der Verarbeiter wird dabei nicht vor unüberwindbare Hürden gestellt:[303] Nach Art. 11 Abs. 1 ist der Verantwortliche nicht dazu verpflichtet, zur Identifizierung der betroffenen Person zusätzliche Informationen einzuholen oder zu verarbeiten. Sofern der Verarbeiter nachweisen kann, dass er die betroffene Person unter dem Pseudonym nicht identifizieren kann, so unterrichtet er die betroffene Person hierüber; die Rechte aus den Art. 15 - 20 DSGVO sind insofern ausgeschlossen als die Person nicht die zur Identifizierung notwendigen Informationen bereitstellt (z.B. den „Schlüssel"), vgl. Art. 11 Abs. 2 DSGVO.[304]

---

299 *Rüpke* bezeichnet die Pseudonymisierung als Instrument möglichen Interessensausgleichs, vgl. *Rüpke*, § 10. Betroffene. Personenbezogene Informationen, in: Rüpke/von Lewinski/Eckhardt, Datenschutzrecht, S. § 10 Rn. 37.

300 *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 271 m.w.N.; *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 5 Rn. 17.

301 *Rüpke*, § 10. Betroffene. Personenbezogene Informationen, in: Rüpke/von Lewinski/Eckhardt, Datenschutzrecht, Rn. 39 spricht von „weitgehender Zulässigkeit der Weiterverwendung".

302 *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 5 Rn. 9 m.w.N.

303 So wohl auch *Rüpke*, § 10. Betroffene. Personenbezogene Informationen, in: Rüpke/von Lewinski/Eckhardt, Datenschutzrecht, § 10 Rn. 38 f.

304 Vgl. auch *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 5 Rn. 18.

Nichtsdestotrotz wird es der betroffenen Person ermöglicht, ihre Rechte unter dem Pseudonym geltend zu machen[305] und der Datenverarbeiter dazu verpflichtet, weitere Schutzmaßnahmen zu ergreifen (vgl. Art. 32 Abs. 1 DSGVO).

Lehnt man eine Anwendbarkeit der DSGVO ab, so bestünde für diese Daten überhaupt kein Schutz. Der Verantwortliche müsste daher nicht überprüfen, inwiefern auch ohne Rückgriff auf die gesondert aufbewahrten Informationen („Schlüssel") eine Re-Identifizierung möglich ist und eine weitergehende Verarbeitung oder Übermittlung daher zu unterbleiben hat.[306]

Pseudonymisierte Daten sind daher als personenbezogene Daten zu betrachten, für die die DSGVO allerdings Privilegierungen vorsieht. Voraussetzung ist allerdings, dass der Schlüssel getrennt aufbewahrt wird. Wird der Schlüssel nicht gesondert aufbewahrt und mittels technischer und organisatorischer Maßnahmen geschützt, die gewährleisten, dass kein Personenbezug wiederhergestellt werden kann, liegen noch nicht einmal pseudonymisierte Daten im Sinne von Art. 4 Nr. 5 DSGVO vor; die Privilegierungen gelten also nicht.

Auch aus einem weiteren Aspekt müssen die Daten der DSGVO unterliegen: *Per definitionem* sind verschlüsselte Daten, die sich auf eine natürliche Person beziehen, als pseudonymisierte Daten i.S.v. Art. 4 Abs. 5 DSGVO anzusehen. Denn mithilfe des Schlüssels (dem Passwort) kann der durch die Verschlüsselung verdeckte Personenbezug wiederhergestellt werden. Art. 32 Abs. 1 lit. a DSGVO bestimmt, dass der Verarbeiter eine dem Stand der Technik[307] entsprechende (sichere) Verschlüsselungsvariante zu verwenden hat[308] und gewährleistet somit den Schutz verschlüsselter Daten. Hierdurch haben auch Dritte auf die verschlüsselten Daten keinen Zugriff, jedenfalls ist der Zugriff auf die personenbezogenen Daten im Vergleich zur „einfachen" Pseudonymisierung um ein Vielfaches erschwert. Dennoch gelten auch solche Daten als personenbezogene Daten.

305 *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 5 Rn. 20.
306 Vgl. *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 5 Rn. 47.
307 Zu diesem unbestimmten Rechtsbegriff *Knopp*, DuD 2017, 663.
308 BeckOK DatenSR/*Schild*, Art. 4 DSGVO Rn. 80.

d) Ermöglichende Wirkung und Privilegierungen

Die Pseudonymisierung hat in der Regel eine ermöglichende Wirkung, als sie zu einer Zulässigkeit der Verarbeitung führen bzw. beisteuern kann. Insbesondere im Rahmen der zweckändernden Verarbeitung kann die Pseudonymisierung eine Zulässigkeit herbeiführen, wie sich aus Art. 6 Abs. 4 lit. e DSGVO ergibt. Im Rahmen der Interessensabwägung nach Art. 6 Abs. 1 lit. f DSGVO ist die Pseudonymisierung ebenfalls zu berücksichtigen.[309]

Darüber hinaus werden Datenverarbeiter bei pseudonymisierten Daten privilegiert:

So enthält Erwägungsgrund 29 eine Privilegierung pseudonymisierter Daten bei allgemeinen Analysen: Sofern mittels technisch-organisatorischer Möglichkeiten sichergestellt ist, dass die DSGVO eingehalten wird und die zusätzlichen Informationen gesondert aufbewahrt werden, sollen Pseudonymisierungsmaßnahmen, die allgemeine Analysen zulassen, bei demselben Verantwortlichen möglich sein, m.a.W. ist die Einschaltung eines Datentreuhänders nicht erforderlich.[310]

Bei Datenschutzverstößen muss der Datenverarbeiter gem. Art. 34 Abs. 3 lit. a DSGVO den Betroffenen nicht informieren, wenn durch Verschlüsselung (als Unterfall der Pseudonymisierung) sichergestellt ist, dass Dritte keinen unbefugten Zugriff auf die personenbezogenen Daten erlangen.[311]

Letztlich wird auch in Art. 89 Abs. 1 DSGVO die Pseudonymisierung als technisch-organisatorische Maßnahme angesehen, um die geforderten Garantien bei der Verarbeitung von personenbezogenen Daten für wissenschaftliche, statistische und archivarische Zwecke zu gewährleisten.[312]

5. Zwischenergebnis

Bei der Betrachtung, ob Datenschutzrecht Anwendung findet, ist zu differenzieren: Sofern anonyme Daten vorliegen und eine Identifizierbarkeit

309 Vgl. auch *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 5 Rn. 17.

310 Eigentlich würde die Kenntnis des Schlüssels dem Verantwortlichen zugerechnet, vgl. *Schantz*, C.II. Anwendungsbereich der DS-GVO, in: Schantz/Wolff, Das neue Datenschutzrecht, Rn. 305; *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 59.

311 *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 271.

312 *Roßnagel*, ZD 2018, 243.

der Person „vernünftigerweise" ausscheidet, d.h. die Person mit Mitteln, die vom Verantwortlichen oder Dritten nach allgemeinem Ermessen wahrscheinlich zur Identifizierung genutzt werden, nicht identifiziert werden kann, ist kein Datenschutzrecht anzuwenden.

Entgegen einer weit verbreiteten Auffassung in der Literatur liegen jedoch bei pseudonymisierten Daten personenbezogene Daten vor. Voraussetzung für die Pseudonymisierung ist allerdings, dass die zusätzlichen Informationen, die zur Identifizierung („Schlüssel") führen, gesondert und gesichert aufbewahrt werden. Nur in diesem Fall finden die in der DSGVO enthaltenen Privilegierungen Anwendung.

Für People Analytics muss daher genau untersucht werden, ob die Daten anonym sind oder lediglich pseudonym. In der Praxis wird oftmals fälschlicherweise davon ausgegangen, dass, sofern der Dritte den Zuordnungsschlüssel nicht hat, für diesen anonyme Daten vorliegen und er daher keine Pflichten nach der DSGVO hat. Dies kann nach Art. 83 DSGVO weitereichende Folgen haben, sofern hierdurch Datenschutzgrundsätze verletzt werden.

II. Legitimationsbedürftigkeit der Datenverarbeitung

Steht die Anwendbarkeit des Datenschutzrechts fest, so ist grundsätzlich für jeden Verarbeitungsvorgang gem. Art. 6 DSGVO gesondert zu überprüfen, ob die Verarbeitung rechtmäßig ist. Insofern handelt es sich um ein grundrechtlich geschütztes[313] Verbot mit Erlaubnisvorbehalt[314]; jede Datenverarbeitung muss von einem der in Art. 6 abschließend aufgezählten Erlaubnistatbeständen gedeckt sein.[315]

313 Vgl. Art. 7 und 8 EU-GRC.

314 Kritisch zum Einsatz dieser Figur und der Verwendung dieses Begriffs: BeckOK DatenSR/*Albers/Veit*, Art. 6 DSGVO Rn. 11 ff.: Die Verwendung impliziere ein generelles Verbot mit nur wenigen Ausnahmen, wovon im Datenschutzrecht aufgrund der weit gefassten Rechtmäßigkeitsvoraussetzungen keine Rede sein könne. Zudem impliziere der Begriff, dass eine gesonderte (administrative) Erlaubnis erforderlich sei. Derselben Auffassung sind *Scholz/Sokol*, in: Simitis, Bundesdatenschutzgesetz, § 4 BDSG Rn. 3.

315 *Albrecht*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 DSGVO Rn. 1; *Buchner*, 2 Grundsätze des Datenschutzrechts, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 240 Rn. 50 ff.; HK DSGVO/BDSG/*Schwartmann/Jacquemain*, Art. 6 Abs. 1 lit. a-f DSGVO Rn. 6; vgl. auch *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 50.

Die Definition des Verarbeitungsbegriffs ist dabei sehr weit gefasst (siehe **D. § 1 I. 1. b**)). Insofern wird in der EU sowie in Deutschland ein umfassender Regelungsansatz verfolgt und nicht lediglich ein punktueller wie beispielsweise in den USA.[316]

Durch die Legitimationsbedürftigkeit einer jeder Datenverarbeitung werden die Anforderungen des Art. 8 Abs. 2 S. 1 EU-GRC erfüllt.[317] Das sog. *Datenschutzgrundrecht* auf EU-Ebene fordert, dass Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden dürfen.

Die Erlaubnistatbestände decken sich mit denen aus Art. 7 der Vorgängerrichtlinie 95/46/EG, sodass sich insofern keine wesentlichen Änderungen zur bisherigen Rechtslage ergeben.[318] Neu ist jedoch, dass die Interessensabwägungsklausel des Art. 6 Abs. 1 lit. f DSGVO kein Erlaubnistatbestand für die Datenverarbeitung für Behörden in Erfüllung ihrer Aufgaben darstellt, wie sich aus Art. 6 Abs. 1 S. 2 DSGVO ergibt.[319]

III. Erlaubnistatbestände der DSGVO

Art. 6 regelt abschließend[320] Tatbestände, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist. Hierzu gehören die Einwilligung (lit. a), Erforderlichkeit für die Erfüllung eines Vertrags (lit. b), einer rechtlichen Verpflichtung (lit. c), zum Schutz lebenswichtiger Interessen (lit. d) oder zur Wahrnehmung einer Aufgabe im öffentlichen Interesse

316 Siehe hierzu *Buchner*, 2 Grundsätze des Datenschutzrechts, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 239 Rn. 49 Die meisten Datenschutzgesetze in den USA betreffen den Konsumentendatenschutz, vgl. *Bodie et al.*, Colorado Law Review 2017, 961 (986) Im Arbeitsleben gibt es nahezu keinen Schutz gegen Überwachung: „*privacy protection do not preclude […] management from observing electronically what it lawfully can see with the naked eye.*" (United States Court of Appeals, First Circuit, 08.04.1997, No. 96-2061 – *Vega-Rodriguez v. Puerto Rico Telephone Co.*)

317 *Albrecht*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 DSGVO Rn. 2.

318 So auch *Härting*, DSGVO, Rn. 321.

319 Vgl. *Buchner*, 2 Grundsätze des Datenschutzrechts, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 240 Fn. 50.

320 So bereits zu Art. 7 der DS-RL: EuGH, Urt. v. 24.11.2011 – C-468/10, C-469/10, CR, 2012, 29 – ASNEF Hinzu kommen selbstverständlich nationale Erlaubnistatbestände, die aufgrund von Öffnungsklauseln weitere Datenverarbeitungsvorgänge legitimieren können.

(lit. e) sowie zur Wahrnehmung von berechtigten Interessen des Verantwortlichen oder eines Dritten (lit. f). Bis auf die Einwilligung stehen somit alle Tatbestände unter dem Vorbehalt der Erforderlichkeit.[321]

1. Vorliegen mehrerer Erlaubnistatbestände

Fraglich ist, ob für einen Verarbeitungsvorgang gleich mehrere Erlaubnistatbestände vorliegen können oder die Verarbeitung immer auf einen bestimmten Erlaubnistatbestand gestützt werden muss. Dies ist dann von praktischer Bedeutung, wenn vom Betroffenen eine Einwilligung eingeholt wird, weil sich der Verarbeiter unsicher ist, ob ein gesetzlicher Erlaubnistatbestand greift.[322]

Die überwiegende Literaturauffassung ist, dass die Datenverarbeitung grundsätzlich auf mehrere Erlaubnistatbestände gleichzeitig gestützt werden kann. Dies ergebe sich aus dem Wortlaut bzw. der englischen Sprachfassung der Norm, in welcher es heißt „*…**at least** one of the following applies*“.[323]

In ihrem Arbeitspapier zur Einwilligung vertrat die *Artikel-29-Gruppe*[324] hingegen die Auffassung, dass sich der Verarbeiter nicht im Rahmen der Verarbeitung auf die Einwilligung als Rechtsgrundlage stützen und dann – falls diese unwirksam sein sollte – zu einer anderen Rechtsgrundlage wechseln könne: „*Es wäre gegenüber Einzelpersonen ein in höchstem Maß missbräuchliches Verhalten, ihnen zu sagen, dass die Daten auf der Grundlage der Einwilligung verarbeitet werden, wenn tatsächlich eine andere Rechtsgrundlage zugrunde gelegt wird.*“[325] Diese Auffassung stützt sich auf die Informa-

---

321 BeckOK DatenSR/*Albers/Veit*, Art. 6 DSGVO Rn. 16.

322 Vgl. HK DSGVO/BDSG/*Schwartmann/Jacquemain*, Art. 6 Abs. 1 lit. a-f DSGVO Rn. 8; *Buchner*, 4 Datenverarbeitung im nicht-öffentlichen Bereich, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 408 f. Rn. 16.

323 HK DSGVO/BDSG/*Schwartmann/Jacquemain*, Art. 6 Abs. 1 lit. a-f DSGVO Rn. 7; BeckOK DatenSR/*Albers/Veit*, Art. 6 DSGVO Rn. 18, 27; so wohl auch Paal/Pauly/*Frenzel*, Art. 6 DSGVO Rn. 8, der das Problem bei der Freiwilligkeit der Einwilligung sieht; *Skistims*, 8.2 Rechtsgrundlagen für datenverarbeitende KI, in: Kaulartz/Ammann/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, Rn. 10.

324 Die Artikel-29-Gruppe war ein unabhängiges Beratungsgremium der Europäischen Komission für Fragen des Datenschutzes und wurde mit Einführung der DSGVO durch den Europäisches Datenschutzausschuss (EDPB) abgelöst.

325 *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679 (WP 259), S. 27; dagegen *EDPB*, DRAFT Guidelines

tionspflicht in Art. 13 Abs. 1 lit. c DSGVO, wonach die Rechtsgrundlage der Verarbeitung anzugeben ist. Der Verantwortliche habe sich daher vor Erhebung zu entscheiden, welche Rechtsgrundlage anwendbar ist.[326]

Verortet wird die Diskussion in aller Regel bei der Rangfolge der verschiedenen Erlaubnistatbestände bzw. der Frage, ob der Erlaubnistatbestand der Einwilligung mit sonstigen gesetzlichen Tatbeständen gleichrangig ist.[327] Kritisiert wird dieses Vorgehen vor allem deshalb, weil dem Betroffenen letztlich eine freie Selbstbestimmung nur vorgetäuscht werde, wenn der Verantwortliche bei Verweigerung der Einwilligung schlicht auf die gesetzliche Ermächtigungsgrundlage zurückgreifen kann.[328] Aus diesem Grund sei es dem Verarbeiter verwehrt, sich auf einen alternativen Erlaubnistatbestand zu stützen, wenn er beim Betroffenen den Eindruck erzeugt hat, es komme auf seine Entscheidung an.[329]

Zu Recht moniert die Praxis, dass die gesetzlichen Erlaubnistatbestände aufgrund der sehr offenen Formulierung die notwendige Rechtssicherheit, auf die Datenverarbeiter – nicht zuletzt wegen der hohen Sanktionen nach Art. 83 DSGVO – angewiesen sind, in vielen Fällen nicht bieten können. Aus diesem Grund wird statt bzw. zusätzlich zu einem eventuell gesetzlich einschlägigen Tatbestand eine Einwilligung des Betroffenen eingeholt, um auf der „sicheren" Seite zu sein.[330]

2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Rn. 19, jedoch mit dem Hinweis, dass die Verarbeiter keine Unsicherheit über die angewandte Rechtsgrundlage aufkommen lassen sollen.

326 *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679 (WP 259), S. 27.

327 *Buchner*, 4 Datenverarbeitung im nicht-öffentlichen Bereich, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 408 f. Rn. 15 ff.; Paal/Pauly/*Frenzel*, Art. 6 DSGVO Rn. 8; zur Vorgängerregelung: *Scholz/Sokol*, in: Simitis, Bundesdatenschutzgesetz, § 4 BDSG Rn. 6 f.; *Roßnagel/Abel*, Handbuch Datenschutzrecht, Kap. 4.8 Rn. 16 ff.

328 *Menzel*, DuD 2008, 400 (405).

329 *Buchner*, 4 Datenverarbeitung im nicht-öffentlichen Bereich, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 409 Rn. 17; *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 23.

330 *Buchner*, 4 Datenverarbeitung im nicht-öffentlichen Bereich, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 409 Rn. 17; kritisch zu dieser Vorgehensweise: *Scholz/Sokol*, in: Simitis, Bundesdatenschutzgesetz, § 4 BDSG Rn. 6; sogar *EDPB*, DRAFT Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Rn. 17.

Schulz bringt richtigerweise vor, dass der Verordnungsgeber diesen Fall vorgesehen und gebilligt hat[331]: Die Löschverpflichtung des Verarbeiters im Falle eines Widerrufs der Einwilligung greift gem. Art. 17 Abs. 1 lit. b DSGVO nur dann, wenn es an einer „anderweitigen Rechtsgrundlage" fehlt. Insofern ist die DSGVO eindeutig.[332] Datenverarbeitungen sind deshalb auch bei einer verweigerten Einwilligung zulässig, sofern ein anderer Erlaubnistatbestand vorliegt. Im Rahmen einer etwaigen Interessensabwägung nach Art. 6 Abs. 1 lit. f DSGVO muss die verweigerte Einwilligung allerdings berücksichtigt werden, da in diesem Rahmen alle Umstände der Verarbeitung berücksichtigt werden müssen.[333] Die verweigerte Einwilligung hat hierbei eine ähnliche Wirkung wie ein Widerspruch nach Art. 21 Abs. 1 DSGVO, d.h. nur wenn der Verarbeiter zwingende schutzwürdige Gründe für eine Verarbeitung vorweisen kann, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, dürfen die Daten auf dieser Basis weiterhin verarbeitet werden.

Es ist erforderlich, dass der Verarbeiter bereits bei Einholung der Einwilligung die Situation und seinen Standpunkt klarmacht. Hierzu muss er dem Betroffenen mitteilen, dass er zwar der Ansicht ist, der gesetzliche Erlaubnistatbestand greife, jedoch unsicher ist, ob diese Auffassung einer rechtlichen Überprüfung standhält und er sich deshalb sicherheitshalber eine Einwilligung einholt.[334] Für diese Vorgehensweise sprechen auch die Prinzipien der Fairness und Zweckbindung.[335] Schließlich soll ein Verarbeiter auch nicht dafür bestraft werden, dass er mit der Einwilligung versucht, weitere Transparenz und Einbindung des Betroffenen zu schaffen.[336]

Unzulässig ist allerdings die Einholung einer Einwilligung, wenn der Verarbeiter aufgrund eines gesetzlichen Verarbeitungsgebots (z.B. Sozial-

331 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 11.

332 *Kremer*, § 2 Zulässigkeit der Verarbeitung, in: Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, Rn. 4.

333 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 11.

334 Ähnlich *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 12; *EDPB*, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, <edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf>, S. 20.

335 *EDPB*, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, <edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf>, S. 18.

336 *Götz*, Big Data im Personalmanagement, S. 56.

versicherungsrecht, Steuerrecht) verpflichtet ist, die Daten zu verarbeiten, denn in einem solchen Fall kann die Verweigerung der Einwilligung keine Folgen haben;[337] das Fragen nach einer Einwilligung wäre demnach treuwidrig.[338]

2. Die Erlaubnistatbestände im Einzelnen

a) Einwilligung

Als „genuine[r] Ausdruck der informationellen Selbstbestimmung“[339] ist die Einwilligung der zentrale Erlaubnistatbestand für die Verarbeitung personenbezogener Daten. Dies ist auch primärrechtlich in Art. 8 Abs. 2 EU-GRC verankert.[340] Zu beachten ist jedoch, dass die Einwilligung nicht vorrangig im Vergleich zu anderen Tatbeständen zu beurteilen ist.[341] Die Beweislast für das Vorliegen einer Einwilligung trägt nach Art. 7 Abs. 1 DSGVO der Verantwortliche.[342]

aa) Formelle Voraussetzungen

Die Einwilligung ist – wie sich bereits aus der Formulierung von Art. 7 Abs. 1 („*Beruht* die Verarbeitung auf einer Einwilligung, […]“) sowie Art. 6 Abs. 1 S. 1 lit. a DSGVO („Die betroffene Person *hat* ihre Einwilligung […] *gegeben*.“) – antizipiert abzugeben.[343]

Anders als im deutschen Recht bislang § 4a Abs. 1 S. 2 BDSG a.F. erforderte, ist die Schriftform (§ 126 BGB) für die Einwilligung nicht mehr explizit erforderlich.[344] Wird jedoch die Einwilligung beispielsweise auf-

337 *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 24.
338 *Helfrich/Forgó/Schneider*, Teil I. Kapitel 5. Grundsätze der datenschutzrechtlichen Prüfung, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Rn. 54.
339 *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 7, 72.
340 Sydow/*Ingold*, Art. 7 DSGVO Rn. 9.
341 *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 360.
342 Sydow/*Ingold*, Art. 7 DSGVO Rn. 6.
343 Sydow/*Ingold*, Art. 7 DSGVO Rn. 17.
344 *Kremer*, § 2 Zulässigkeit der Verarbeitung, in: Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, Rn. 4; Sydow/*Ingold*, Art. 7 DSGVO Rn. 22.

grund der Nachweispflicht aus Art. 7 Abs. 1 DSGVO schriftlich eingeholt, so stellt Absatz 2 der Norm besondere Voraussetzungen auf: Die Einwilligung muss, sofern die schriftliche Erklärung des Betroffenen noch andere Sachverhalte betrifft, in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache ersucht werden, sodass diese von anderen Sachverhalten klar zu unterscheiden ist. Mit anderen Worten darf die datenschutzrechtliche Einwilligung nicht in der Erklärung versteckt werden oder untergehen. Sie ist daher optisch abzugrenzen, was beispielsweise bei Online-Formularen durch eine gesondert anzuklickende Checkbox erfolgen kann.[345] Empfohlen wird zuweilen eine drucktechnische Hervorhebung der Einwilligungserklärung z.B. durch Fettdruck, Einrahmung oder Schattierung.[346]

Grundsätzlich können Einwilligungen nach der DSGVO in jeder beliebigen Form erteilt werden. Lediglich für das Beschäftigungsverhältnis stellt § 26 Abs. 2 BDSG in Deutschland das Schriftformerfordernis bzw. die elektronische Form[347] als Regel auf,[348] wobei auch hier Ausnahmen möglich sind, wenn wegen besonderer Umstände eine andere Form angemessen ist (§ 26 Abs. 2 S. 3 BDSG).

Vor Abgabe der Einwilligung ist die betroffene Person über das Widerrufsrecht in Kenntnis zu setzen, Art. 7 Abs. 3 DSGVO.

bb) Materielle Voraussetzungen

Eine Verarbeitung personenbezogener Daten ist nach Art. 6 Abs. 1 lit. a DSGVO möglich, wenn die betroffene Person ohne jeden Zweifel ihre Einwilligung gegeben hat. Der Begriff der Einwilligung ist in Art. 4 Nr. 11 DSGVO definiert als jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung,

345 Sydow/*Ingold*, Art. 7 DSGVO Rn. 24.

346 *Kremer*, § 2 Zulässigkeit der Verarbeitung, in: Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, Rn. 9; hierfür plädierte bereits *Jochen Schneider* im Jahr 2015, vgl. *Ehmann*, ZD 2015, 6 (9).

347 Hinzugefügt mit dem 2. DSAnpUG-EU, vgl. BT-Drs. 19/11181, S. 19: Ziel war die Digitaltauglichkeit des Gesetzes entsprechend dem Koalitionsvertrag zu prüfen, wobei das grundsätzliche Schriftformerfordernis hier als überflüssig erachtet wurde.

348 *Kremer*, § 2 Zulässigkeit der Verarbeitung, in: Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, Rn. 5.

mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Art. 6 Abs. 1 lit. a DSGVO bestimmt ferner, dass die Einwilligung „für einen oder mehrere bestimmte Zwecke" abgegeben werden muss. Aus diesem Grund muss der Betroffene über den beabsichtigten Verarbeitungszweck informiert werden. Dies ergibt sich auch aus Erwägungsgrund 42 S. 4.

(1) Eindeutig bestätigende Handlung

Eine eindeutig bestätigende Handlung liegt dann vor, wenn beispielsweise ein Kästchen in einer Software oder auf einer Internetseite angeklickt wird. Nicht ausreichend ist ein bereits vorangekreuztes Kästchen oder Stillschweigen bzw. Untätigkeit (bspw. bei „fingierten Einwilligungen" in Form von „Widerspruchslösungen"[349]).[350] Anders als bei § 4a BDSG a.F. ist keine Schriftform der Einwilligung erforderlich. Dies ergibt sich bereits aus Erwägungsgrund 32 der DSGVO, wonach die elektronische Form ausdrücklich angesprochen wird. Aus dem Zusatz einer „sonst eindeutigen bestätigen Handlung" geht hervor, dass die Einwilligung auch konkludent durch schlüssiges Verhalten erteilt werden kann.[351]

(2) Freiwilligkeit

Die Einwilligung muss freiwillig abgegeben worden sein, d.h. der Betroffene muss tatsächlich eine echte Wahl haben.[352] Er darf sich nicht in einer „faktischen Zwangssituation" befinden,[353] d.h. er muss in der Lage sein, die Einwilligung zu verweigern oder zurückzuziehen, ohne hierdurch Nachteile zu erleiden.[354] Eine Auslegungshilfe liefert Erwägungsgrund 43: „*Um sicherzustellen, dass die Einwilligung freiwillig erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem*

349 Paal/Pauly/*Ernst*, Art. 4 DSGVO Rn. 90.
350 BeckOK DatenSR/*Schild*, Art. 4 DSGVO Rn. 124.
351 Paal/Pauly/*Ernst*, Art. 4 DSGVO Rn. 89.
352 Paal/Pauly/*Ernst*, Art. 4 DSGVO Rn. 69.
353 *Buchner*, 4 Datenverarbeitung im nicht-öffentlichen Bereich, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 417 Rn. 35.
354 Erwägungsgrund 42.

Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern. Die Einwilligung gilt nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist."

Gesetzlich normiert ist dies in Art. 7 Abs. 4 DSGVO. Ergänzt wird diese Regelung im Beschäftigungskontext durch die nationale Regelung des § 26 Abs. 2 BDSG, wonach insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt wurde, zu berücksichtigen sind.

In § 26 Abs. 2 S. 2 BDSG wird klargestellt, dass die Einwilligung auch im Beschäftigungsverhältnis - entgegen Literaturstimmen zum BDSG a.F.[355] - nicht von vornherein ausscheidet: „*Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen*."[356]

Allerdings wird man davon ausgehen müssen, dass Beschäftigte vor Abschluss eines Arbeitsvertrages einer Drucksituation ausgesetzt sind, sodass beispielsweise im Bewerbungsverfahren eine Einwilligung in der Regel ausscheidet.[357] Der Bewerber wird in jegliche Form der Verarbeitung einwilligen, um keine Nachteile bei der Bewerberauswahl befürchten zu müssen.[358] Etwas anderes gilt aber dann, wenn der Arbeitgeber vom Bewerber nach einem erfolglosen Bewerbungsverfahren die Unterlagen für mögliche weitere Stellen speichern möchte.[359]

Die Einwilligung im laufenden Beschäftigungsverhältnis ist jedoch ebenfalls mit einem kritischen Auge zu betrachten. Speziell wenn das Arbeitsverhältnis selbst unmittelbar davon betroffen sein kann (z.B. im Rahmen von Versetzungen, Leistungsbewertungen etc.), scheidet eine Ein-

355 *Brink/Schmidt*, MMR 2010, 592 (593).
356 *Kainer/Weber*, BB 2017, 2740 (2741) m.w.N.
357 So bereits BT-Drs. 18/11325, S. 97; *Schwarz*, ZD 2018, 353 (355); *Maier*, DuD 2017, 169 (172); dagegen *Betz*, ZD 2019, 148 (151): Freiwillige Einwilligung in eine Sprachanalyse im Bewerbungsprozess möglich.
358 *Kainer/Weber*, BB 2017, 2740 (2741); so auch *Schwarz*, ZD 2018, 353 (355).
359 *Kort*, NZA-Beilage 2016, 62 (71); *Pötters*, in: Gola, Datenschutz-Grundverordnung, Art. 88 DSGVO Rn. 86.

willigung in aller Regel aus.[360] Zu beachten ist auch ein eventueller Gruppenzwang. So sieht Rechtsprechung und Literatur als Indiz für zusätzlichen Druck den Zwang zur Unterschrift auf einer gemeinsamen Erklärung an.[361]

Bei *People Analytics*-Maßnahmen hingegen kommt es maßgeblich auf den Umfang der gesammelten Daten sowie den konkreten Verwendungszweck an,[362] sodass keine pauschalisierten Aussagen zur Zulässigkeit bzw. Unzulässigkeit der Einwilligung bei solchen Analysen getroffen werden können.[363]

(3) In informierter Weise

Ein weiteres Erfordernis ist die Abgabe der Einwilligungserklärung „*in informierter Weise*". Hierzu ist es erforderlich, dass die betroffene Person mindestens weiß, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden (Erwägungsgrund 42 S. 4). Weitere Informationspflichten für den Verarbeiter ergeben sich aus den Art. 13 und 14 DSGVO. Die Nichterfüllung dieser Pflichten hat jedoch nicht zwingend die Unwirksamkeit der Einwilligung zur Folge,[364] wenn der Betroffene die Entscheidung auch ohne die Information in informierter Weise getroffen hat.

(4) Für einen oder mehrere bestimmte Zwecke

Die Einwilligung muss „*für einen oder mehrere bestimmte Zwecke*" (Art. 6 Abs. 1 S. 1 lit. a DSGVO) abgegeben worden sein. Dies ergibt sich bereits

360 Vgl. *Pötters*, in: Gola, Datenschutz-Grundverordnung, Art. 88 DSGVO Rn. 86 f.

361 VG Saarlouis, Urt. v. 29.01.2016 – 1 K 1122/14, PharmR 2016, 207 (213) = ZD 2016, 549 = BeckRS 2016, 42953; ebenso unter Verweis auf das Urteil *Blinn*, Wearables und Arbeitnehmerdatenschutz - Vom freiwilligen Selbstoptimierer zum Kontrollinstrument des Arbeitgebers?, in: Taeger, Smart world - smart law?, S. 531.

362 Siehe die untersuchten Einsatzszenarien unter **E.**

363 Ähnlich, aber zu pauschal: *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, S. 175: „So stellt die Einwilligung insgesamt betrachtet für eine Vielzahl von Big Data HR Analytics-Anwendungen keine gesicherte rechtliche Grundlage dar.".

364 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, Teil 3 Rn. 41.

auch aus der Definition der Einwilligung in Art. 4 Nr. 11 DSGVO, wonach die Einwilligung eine *für den bestimmten Fall* abgegebene Willensbekundung ist. Diese Voraussetzung überschneidet sich teilweise mit der vorherigen.

Aus Erwägungsgrund 32 ergibt sich, dass mit der Einwilligung alle Verarbeitungsvorgänge für den bestimmten Zweck abgedeckt werden sollen. Bei mehreren Zwecken muss sich die Einwilligung ohne Zweifel auf alle Zwecke beziehen, wobei die Zwecke so konkret wie möglich benannt werden müssen.[365] Etwaige Pauschal- oder Blankoeinwilligungen sind daher unzulässig.[366]

Höchst problematisch ist dies bei Big Data-Analysen mit Datenbanken, die ursprünglich für einen anderen Zweck angelegt wurden, wie dies in der Praxis häufig der Fall sein wird.[367] Die vorhandenen Einwilligungen umfassen in aller Regel keine Big Data-Analysen.[368] Ferner sind die mittels solcher Analysen gefundenen Muster vielfach nicht prognostizierbar, weshalb der spätere Zweck, für welchen die Daten verwendet werden sollen, ebenfalls nicht vorhersehbar ist und eine Einwilligung daher einer Pauschaleinwilligung gleichkommen würde. Selbst wenn der Verantwortliche „maximal transparent" darlegt, dass das Ergebnis der Analyse noch nicht feststeht, so könnte er im Vorfeld keine Angaben zu den Voraussetzungen, Konsequenzen und – im Falle einer Profilbildung – der inneren Logik des Automatismus machen, weshalb die Einwilligung ausscheidet.[369] Ein „allgemeines Profiling", welches auf Big Data aufbaut, ist daher mangels Spezifizität nicht einwilligungsfähig.[370]

b) Erforderlichkeit für die Erfüllung eines Vertrags

Die Datenverarbeitung ist nach Art. 6 Abs. 1 S. 1 lit. b DSGVO erlaubt, wenn sie zur Erfüllung eines Vertrags oder eines vorvertraglichen Schuldverhältnisses erforderlich ist. Dieser Erlaubnistatbestand ist mit Art. 7 lit. b

365 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 23 f.
366 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 7 DSGVO Rn. 34.
367 Zur Problematik der Zweckbindung und Big Data-Analysen (noch zur alten Rechtslage), siehe *Helbing*, K&R 2015, 145; *Dammann*, ZD 2016, 307 (313 f.).
368 *Katko/Babaei-Beigi*, MMR 2014, 360 (362).
369 Kritisch *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 7 DSGVO Rn. 35.
370 So bereits *Jochen Schneider und Michael Will* in einer Ad-Hoc-Diskussion im Jahr 2015, vgl. *Ehmann*, ZD 2015, 6 (10).

der DS-RL identisch.[371] Bereits bei Erlass der Richtlinie ging der europäische Gesetzgeber für solche Situationen davon aus, dass die Vorteile für den Betroffenen die Risiken der Verarbeitung überwiegen.[372] So muss es beispielsweise dem Datenverarbeiter gestattet sein, die Kundendaten zu verarbeiten, um bestellte Ware liefern zu können, gleiches gilt bei Kreditkartendaten für die Abwicklung der Zahlung.[373] Grundlage ist jedoch auch hier der Vertragsschluss bzw. die Vertragsanbahnung und somit eine autonome Willensentscheidung des Betroffenen.[374]

Es muss im Übrigen ein unmittelbarer Zusammenhang zwischen der Datenverarbeitung und dem konkreten Zweck des Schuldverhältnisses bestehen.[375] Nicht mehr vom Erlaubnistatbestand erfasst ist daher die Erstellung ausführlicher Benutzerprofile, um beispielsweise auf Basis von Bestellungen und Suchanfragen Vorschläge für weitere Produkte zu generieren.[376]

Die Erforderlichkeit der Datenverarbeitung ist von der reinen Zweckdienlichkeit zu unterscheiden. Der Erlaubnistatbestand greift nicht, wenn die Verarbeitung nur „dienlich" oder „nützlich" ist, um etwa ein Mehr an Service oder eine schnellere Abwicklung anbieten zu können. Es ist immer auf den „eigentlichen Kern" des Vertragsverhältnisses abzustellen.[377]

Allerdings darf die Erforderlichkeit nicht als „Unverzichtbarkeit" gesehen werden, sondern es muss eine wertende Betrachtung unter Berücksichtigung der Interessen aller Beteiligten vorgenommen werden, ob es eine zumutbare, gleichwertige – weniger Daten benötigende – Alternative gibt.[378]

---

371 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, Teil 3 Rn. 43.

372 GHN (40. Aufl. 2009)/*Brühann*, Art. 7 Richtlinie 95/46/EG Rn. 14.

373 *Article 29 Data Protection Working Party*, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), S. 16.

374 *Schantz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 1 DSGVO Rn. 15; *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 26 m.w.N.; *Albrecht*, CR 2016, 88 (92) bezeichnet diesen Erlaubnistatbestand auch als "Element der Selbstbestimmung".

375 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, Teil 3 Rn. 43.

376 *Article 29 Data Protection Working Party*, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), S. 17.

377 *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 43 f.

378 *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 45; in diese Richtung auch *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 38: Die Datenverarbeitung muss sich bei

Im Bereich des Beschäftigtendatenschutzes wird diese Vorschrift durch § 26 Abs. 1 BDSG als mitgliedsstaatliche Spezialregelung im Sinne von Art. 88 DSGVO verdrängt.[379]

c) Erforderlichkeit für die Erfüllung einer rechtlichen Verpflichtung

Ein weiterer Erlaubnistatbestand ist die Verarbeitung für die Erfüllung einer rechtlichen Verpflichtung, welcher der für die Verarbeitung Verantwortliche unterliegt. In diesem Zusammenhang wird davon ausgegangen, dass bereits die gesetzgeberische Entscheidung über die rechtliche Verpflichtung auf einer demokratischen Entscheidung beruht, die die Grundrechte der betroffenen Person berücksichtigt.[380] In Art. 6 Abs. 3 DSGVO wird spezifiziert, dass sich die Rechtsgrundlage aus dem Unionsrecht (lit. a) oder dem Recht des Mitgliedsstaats, dem der Verantwortliche unterliegt, (lit. b) ergeben kann und der Zweck der Verarbeitung in der Rechtsgrundlage festgelegt sein muss. Paradebeispiel hierfür ist die Verpflichtung des Arbeitgebers die Lohndaten seiner Arbeitnehmer an die Steuerbehörden sowie an die Sozialversicherungsträger zu übermitteln.[381]

d) Erforderlichkeit zum Schutz lebenswichtiger Interessen

Die Datenverarbeitung zum Schutz eines lebenswichtigen Interesses ist für die vorliegende Arbeit nicht von Bedeutung. Nur am Rande sei erwähnt, dass die Voraussetzungen sehr hoch sind und der Erlaubnistatbestand regelmäßig nur in Notfällen eingreift, in denen der Einzelne nicht mehr selbst einwilligen kann.[382]

---

vernünftiger Würdigung als objektiv sinnvoll im Kontext des Vertragszwecks erweisen.

379 *Benkert*, NJW-Spezial 2018, 562 (563).

380 GHN (40. Aufl. 2009)/*Brühann*, Art. 7 Richtlinie 95/46/EG Rn. 16.

381 *Article 29 Data Protection Working Party*, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), S. 19; GHN (40. Aufl. 2009)/*Brühann*, Art. 7 Richtlinie 95/46/EG Rn. 16; *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, Teil 3 Rn. 45.

382 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 45 ff.

e) Erforderlichkeit zur Wahrnehmung einer Aufgabe im öffentlichen Interesse

Der Erlaubnistatbestand in Art. 6 Abs. 1 lit. e DSGVO betrifft primär die Datenverarbeitung durch öffentliche Stellen,[383] weshalb dieser für die vorliegende Arbeit nicht von Bedeutung ist. Als Musterbeispiel wird hierbei oftmals die Ausübung hoheitlicher Gewalt genannt, wobei hierfür zunächst im nationalen Recht des Mitgliedsstaats ein entsprechender Erlaubnistatbestand geschaffen werden muss, da Art. 6 Abs. 1 lit. e DSGVO gemäß Erwägungsgrund 45 allein nicht als Erlaubnistatbestand dient, sondern mehr den Charakter einer Richtlinie hat.[384] Deutschland hat mit § 3 BDSG n.F. einen entsprechenden Erlaubnistatbestand geschaffen.

f) Erforderlichkeit zur Wahrnehmung von berechtigten Interessen des Verantwortlichen oder Dritten

Art. 6 Abs. 1 lit. f DSGVO, der die Datenverarbeitung erlaubt, wenn sie erforderlich zur Wahrnehmung von berechtigten Interessen des Verantwortlichen oder Dritten ist, ist „eine der zentralen Stellschrauben, die für einen gerechten Ausgleich zwischen den Interessen der Verbraucher und der Wirtschaft sorgen."[385] Hierbei ist eine Abwägung zwischen den Interessen und Grundrechten der betroffenen Person und den Interessen des Datenverarbeiters erforderlich.[386] Bloße Interessen der Allgemeinheit reichen nicht aus; zu den berechtigten Interessen zählen aber nicht nur rechtliche, sondern auch tatsächliche, wirtschaftliche oder ideelle Interessen.[387] Teilweise wird der Tatbestand als „unscharf" und „aufgeweicht" bezeichnet.[388]

383 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, Teil 3 Rn. 45.
384 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 48 f.
385 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, Teil 3 Rn. 51; *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 141.
386 *Nebel*, § 3 III. Erlaubnis zur Datenverarbeitung, in: Roßnagel, Das neue Datenschutzrecht, Rn. 99.
387 *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 147.
388 *Roßnagel/Nebel/Richter*, ZD 2015, 455 (457); vgl. auch *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 142 ff. m.w.N. zum Gesetzgebungsprozess.

Erforderlich ist eine Abwägung der Interessen im Einzelfall, d.h. eine wertende Betrachtungsweise oder rein kursorische Abwägungen sind somit nicht zulässig. Lediglich dort, wo eine Vielzahl künftiger Fälle abgedeckt werden muss, dürfen die Interessen der betroffenen Personen in einer typisierenden Betrachtungsweise verallgemeinert werden.[389]

Die Darlegungslast, dass die Interessen des Betroffenen nicht überwiegen, trägt der Verantwortliche.[390] Dies wird besonders relevant, wenn der Betroffene sein Widerspruchsrecht aus Art. 21 DSGVO ausübt.

Der Vorschlag der *Artikel-29-Arbeitsgruppe* zur Abwägung sieht vor, dass in mehreren Schritten vorgegangen wird:[391]

Zunächst muss überprüft werden, ob das Interesse „legitim" oder „illegitim" ist. Diese Kontrolle erfolgt danach, ob es rechtmäßig ist, hinreichend genau bestimmt, damit eine Interessensabwägung stattfinden kann sowie ein reales und gegenwärtiges Interesse repräsentiert. In einen zweiten Schritt muss die Erforderlichkeit der Maßnahme geprüft werden, insbesondere, ob es mildere Mittel gibt, die weniger in die Rechte der betroffenen Person eingreifen. In weiterer Folge wird eine vorläufige Abwägung vorgenommen, in welcher eine erste Einschätzung erfolgt, ob das Interesse des Verarbeiters durch Grundrechte und Grundfreiheiten des Betroffenen überlagert werden. Hierbei muss einerseits die Herkunft des Interesses des Datenverarbeiters evaluiert werden (z.B. Grundfreiheiten/-rechte, öffentliches Interesse etc.). Andererseits muss überprüft werden, um welche Datenarten es sich handelt (sensitive Daten, öffentlich zugängliche Daten etc.). Ferner müssen auch die Stellung des Betroffenen gegenüber dem Verarbeiter (z.B. Arbeitnehmer-Arbeitgeber) sowie die Art der Datenverarbeitung (z.B. Profiling, Data Mining, Big Data, Veröffentlichung an einen großen Personenkreis) berücksichtigt werden. Letztlich müssen diese Aspekte mit den möglichen Auswirkungen auf die Grundrechte und Interessen des Betroffenen abgewogen werden. Hierbei dürfen die Erwartungen des Betroffenen nicht außer Betracht bleiben. In einem letzten Schritt wird

389 GHN (40. Aufl. 2009)/*Brühann*, Art. 7 Richtlinie 95/46/EG Rn. 21 f. zur Vorgängernorm.

390 Vgl. *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 149 m.w.N.: Dies folgt aus der allgemeinen Rechenschaftspflicht nach Art. 5 Abs. 2, 24 Abs. 1 S. 1 DSGVO.

391 *Article 29 Data Protection Working Party*, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), S. 55 f.; ein "3x5-Modell" zur Nachvollziehbarkeit der Abwägung mit 15 Kriterien nennt *Herfurth*, ZD 2018, 514.

das Risiko für den Betroffenen mit den Vorteilen für den Datenverarbeiter abgewogen.

Nach Abschluss dieser vorläufigen Abwägung findet ein „endgültiger Abwägungsvorgang" statt, bei welchem noch weitere Sicherheitsmaßnahmen einbezogen werden wie beispielsweise technisch-organisatorische Maßnahmen, damit die Daten nicht für nicht-vorhergesehene Zwecke verwendet werden, die Nutzung von Anonymisierungstechniken, um eine Identifizierung der einzelnen Person zu verhindert, das Prinzip der Datenminimierung sowie die Erhöhung der Transparenz gegenüber der betroffenen Person inkl. Widerspruchsrechte[392] („Opt-Out").

Letztlich soll der Datenverarbeiter nach Ansicht der *Artikel 29-Gruppe* alle Schritte genau dokumentieren, bevor Daten verarbeitet werden. Im Übrigen sollen die Betroffenen darüber informiert werden, insbesondere, warum der Verarbeiter davon ausgeht, dass sein Interesse das Interesse des Betroffenen überwiegt bzw. die Interessen nicht beeinträchtigt.

Die Vorgaben der *Artikel-29-Gruppe* sind nicht verbindlich, jedoch eine Möglichkeit, im Streitfall das berechtigte Interesse mit hoher Wahrscheinlichkeit rechtssicher nachweisen zu können. Auch andere Ansätze wie beispielsweise das „3x5-Modell" von *Herfurth* werden in der Literatur diskutiert.[393] Bei letzterem Modell werden drei Dimensionen (Daten, Akteure, Verarbeitung) mit jeweils fünf Kriterien in einer Matrix dargestellt. Die Belastung wird für jedes Kriterium in die Stufen „gering", „mittel" und „schwer" eingeordnet. Anhand dieser „konkreten Abwägungstopoi"[394] soll es für Betroffene möglich sein, eine Bewertung nachzuvollziehen und der Verarbeiter – sollte ein Überwiegen der Betroffeneninteressen festgestellt werden – ggf. punktuelle Gestaltungsmaßnahmen entwickeln können. Bislang hat sich jedoch kein bestimmter Standard etabliert.

392 Diese sollen allerdings nur dann ermöglichend wirken, wenn ein über Art. 21 DSGVO hinausgehendes, beispielsweise vorbehaltloses Widerspruchsrecht gewährt wird, vgl. *Skistims*, 8.2 Rechtsgrundlagen für datenverarbeitende KI, in: Kaulartz/Ammann/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, Rn. 56 m.w.N.

393 *Herfurth*, ZD 2018, 514 (515 ff.).

394 *Herfurth*, ZD 2018, 514 (520).

IV. Beschäftigtendatenschutz

1. Öffnungsklausel der DSGVO für nationale Regelungen, Art. 88 DSGVO

Gemäß Art. 88 Abs. 1 DSGVO können die Mitgliedsstaaten durch Rechtsvorschriften oder Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigtenkontext vorsehen. Dies gilt insbesondere für den Zweck der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeiter oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses.

Nach Auffassung des europäischen Gesetzgebers, welcher die Vorschrift im Kapitel IX „Vorschriften für besondere Verarbeitungssituationen" verortet hat, handelt es sich bei der Datenverarbeitung im Beschäftigungskontext um eine besondere Verarbeitungssituation.[395]

Erwägungsgrund 155 bezieht sich speziell auf die Öffnungsklausel des Art. 88 und erklärt diese dahingehend, dass unter Kollektivvereinbarungen auch Betriebsvereinbarungen zu verstehen sind. Ferner sollen insbesondere Vorschriften über die Bedingungen, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen, von Art. 88 DSGVO erfasst sein. Gleiches gilt für Vorschriften über die Verarbeitung dieser Daten für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten etc. Zusätzlich zur Regelung des Art. 88 Abs. 1 DSGVO statuiert der Erwägungsgrund, dass die Einwilligung als zentraler Erlaubnistatbestand für die Verarbeitung im Beschäftigtenkontext näher ausgestaltet werden kann.[396]

---

395 Sydow/*Tiedemann*, Art. 88 DSGVO Rn. 1.
396 Sydow/*Tiedemann*, Art. 88 DSGVO Rn. 2.

Sofern Mitgliedsstaaten Regelungen zum Beschäftigungsdatenschutz erlassen, müssen sie den Anforderungen aus Art. 88 Abs. 2 DSGVO genügen, mithin angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person vorsehen. Dies gilt nach Abs. 2 insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeitausüben, und die Überwachungssysteme am Arbeitsplatz.

a) Reichweite der Öffnungsklausel

Umstritten ist in diesem Zusammenhang, wie der Wortlaut „spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigtenkontext" zu verstehen ist. Besonders kontrovers ist in diesem Zusammenhang, ob lediglich präzisierende Vorschriften zulässig sind und ob die Vorschriften in gewissem Umfang vom Schutzstandard der DSGVO nach oben bzw. nach unten abweichen dürfen.

aa) Regelungen in den Grenzen des Art. 88 Abs. 2 DSGVO möglich

Nach der Auffassung von *Taeger* und *Rose* ist die Öffnungsklausel in Art. 88 DSGVO sehr weitreichend. Die Mitgliedsstaaten könnten ihr eigenes Datenschutzregime entwickeln, welches außer an übergeordnete Grund- und Menschenrechte lediglich an Art. 88 Abs. 2 DSGVO gebunden sei.[397] Sie begründen ihre Auffassung damit, dass die im Kommissionsentwurf („*in den Grenzen der Verordnung*") und im Parlamentsentwurf („*im Einklang mit den Regelungen dieser Verordnung*") zunächst vorgesehene Beschränkung[398], dass Regelungen nur „in den Grenzen" der Verordnung möglich seien, mit den Trilogverhandlungen weggefallen wären und daher eine Bindung nur noch an Art. 88 Abs. 2 DSGVO bestehe.[399]

In dieselbe Richtung argumentiert auch *Traut*, der ferner anführt, dass „spezifisch" im Sinne von „sektorspezifisch" zu verstehen sei, wie sich aus

397 *Taeger/Rose*, BB 2016, 819 (830).
398 Vgl. hierzu Paal/Pauly/*Pauly*, Art. 88 DSGVO Rn. 3.
399 *Taeger/Rose*, BB 2016, 819 (830).

Erwägungsgrund 155 ergebe. Im Übrigen wäre die Regelung des Art. 88 Abs. 2 DSGVO nicht erforderlich, wenn die Spezifizierungsrechtsakte die Regelungen der DSGVO „nur näher ausfüllen würden (oder gar den Datenschutz nur verstärken könnten)".[400] Im Übrigen spreche auch dafür, dass der EuGH bereits bei der DS-RL 95/46/EG den Gestaltungsspielraum der Mitgliedsstaaten gem. Art. 5 der RL für weit hielt.[401]

Riesenhuber stellt fest, dass die Verwendung des Terminus „spezifischere Vorschriften" nicht pauschal eine Absenkung des Schutzniveaus der Verordnung verbiete, denn vielfach lasse sich eine spezifischere Regelung nicht mit der „allgemeinen" vergleichen, da sie ggf. andersartige, aber nicht „stärkere" oder „schwächere" Schutzmechanismen eröffne. Bereits der in Art. 88 DSGVO selbst angesprochene Schutzmechanismus des Kollektivs in Analogie zur Lehre von der Richtigkeitsgewähr des Tarifvertrags illustriere, dass die kollektive Regelung in geeigneten Fällen ausreichenden Schutz biete. Die Mitgliedsstaaten hätten deshalb einen eigenen Regelungsspielraum, den sie mit Rücksicht auf die besonderen „Sachgesetzlichkeiten des Beschäftigungsverhältnisses" kreativ ausfüllen könnten.[402]

Düwell und *Brink* schließen sich ebenfalls dieser Auffassung an; dies sei schon deswegen überzeugend, da Art. 88 Abs. 1 DSGVO mit seiner umfänglichen Aufzählung von Verarbeitungszwecken auf die sehr ausdifferenzierten Regelungssachverhalte im Beschäftigungskontext verweise und erst Absatz 2 das Schutzniveau definiere. Sobald ein Mitgliedsstaat eigene Regelungs- und Lösungsansätze für besondere Sachverhalte (im Beschäftigtenkontext) verfolgen, seien daher Mitgliedsstaaten befugt, Normen zu erlassen.[403]

400 *Traut*, RDV 2016, 312 (314).
401 *Traut*, RDV 2016, 312 (314) mit Hinweis auf EuGH, Urt. v. 06.11.2003 – C-101/01, EuZW, 2004, 245 (251) – Lindqvist Rn. 81; Urt. v. 24.11.2011 – C-468/10, C-469/10, CR, 2012, 29 (31) – ASNEF Rn. 35.
402 BeckOK DatenSR/*Riesenhuber*, Art. 88 DSGVO Rn. 66 ff.
403 *Düwell/Brink*, NZA 2017, 1081 (1082).

bb) Keine Abweichung vom Schutzniveau der DSGVO möglich

Deutlich enger legen *Spelge*[404], *Benecke* und *Wagner*[405] sowie *Maschmann*[406] die Öffnungsklausel des Art. 88 Abs. 1 DSGVO aus. Abweichungen vom Schutzniveau der DSGVO seien weder nach oben noch nach unten zulässig.[407]

Spelge begründet ihre Auffassung damit, dass der EuGH bereits zur Vorgängerregelung der DSGVO, der RL 95/46/EG, es den Mitgliedsstaaten untersagt hat, strengere Anforderungen an den Datenschutz als die Richtlinie zu stellen.[408] Für die DSGVO gelte nichts anderes. Dies ergebe sich bereits aus dem Rechtscharakter der Verordnung sowie aus den Erwägungsgründen 9 und 10 der DSGVO, wonach ein einheitliches Datenschutzniveau für erforderlich gehalten wird, um Wettbewerbsverzerrungen zu vermeiden und die Vorschriften der Verordnung unionsweit einheitlich angewendet werden sollen. Zwar seien Abweichungen im Rahmen von Öffnungsklauseln grundsätzlich zulässig, Art. 88 Abs. 1 DSGVO erlaube jedoch lediglich „spezifischere Regelungen", also konkretisierende Vorschriften, mit denen die Anwendung der DSGVO genauer festgelegt werden, nicht aber Regelungen, mit denen der Schutzstandard über- oder unterschritten werde.

Benecke und *Wagner* sehen im Wortlaut der Regelung ebenfalls die Intention des europäischen Gesetzgebers, die Vollharmonisierungswirkung der Verordnung in besonderem Maße zum Ausdruck kommen zu lassen.[409] Dies stützen sie u.a. darauf, dass in der Endfassung die Ermächtigung der Mitgliedsstaaten, die Einwilligungsmöglichkeiten im Beschäftigtenkontext zu erweitern, weggefallen ist und die Rückbindung nationaler Bestimmungen auf Mindest- und Maximalvorgaben sich in die Systematik der Öffnungsklauseln einfüge.

Deutlich ausführlicher begründet *Maschmann* seine Auffassung. Der Wortlaut von Art. 88 DSGVO sei nicht sehr aussagekräftig, da sich der Be-

404 *Spelge*, DuD 2016, 775 (778).
405 *Benecke/Wagner*, DVBl 2016, 600 (603).
406 *Maschmann*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 88 DSGVO Rn. 32 ff.
407 Ebenfalls bejahend unter Bezugnahme auf die genannten Autoren *Kainer/Weber*, BB 2017, 2740; ohne weitere Begründung und etwas widersprüchlich *Imping*, CR 2017, 378 (380).
408 Hierauf stützt sich auch Ehmann/Selmayr/*Selk*, Art. 88 DSGVO Rn. 16 ff., der in der Vorauflage noch von einer Mindestharmonisierung ausgegangen ist.
409 *Benecke/Wagner*, DVBl 2016, 600 (603).

griff „spezifisch“ nicht steigern ließe und im Übrigen auch in Erwägungsgrund 155 lediglich der Begriff „spezifisch“ verwendet werde. Letztlich spreche auch Erwägungsgrund 10, in dem es heißt, dass die Verordnung Vorschriften von Mitgliedsstaaten nicht ausschließe, in denen die Umstände besonderer Verarbeitungssituationen, einschließlich einer genaueren Bestimmung der Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist, dafür, „spezifischer“ nicht im Sinne von strenger zu verstehen.[410] Auch aus der Entstehungsgeschichte ließe sich nichts herleiten, da sich letztlich die Entwurfsfassung des Rates – eine Kompromissformel – in der endgültigen Fassung niedergeschlagen habe und es an aussagekräftigen Belegen fehle, die für eine vollständige Freigabe des Beschäftigtendatenschutzrechtes sprechen.[411] Die Systematik der DSGVO spreche ebenfalls für eine Vollharmonisierung: Eine Reihe von Klauseln erlaube einen Spielraum für eigenständige Regelungen, der nur durch allgemeine Grundsätze eingeengt werde. So werde beispielsweise in Art. 9 Abs. 4 DSGVO den Mitgliedsstaaten ausdrücklich die Erlaubnis erteilt, zusätzliche Bedingungen, einschließlich Beschränkungen, einzuführen. Im Rahmen der bereichsspezifischen Öffnungsklauseln gehe Art. 85 DSGVO für den Pressebereich am weitesten, der lediglich das Ziel vorgebe und ersichtlich keine Vollharmonisierung anstrebe. Eine solche Freigabe fehle jedoch bei Art. 88 DSGVO für den Beschäftigtendatenschutz.[412] Letztlich sei das Telos der Norm, wie sich aus Erwägungsgrund 10 ergebe, die Gewährleistung eines gleichmäßigen und hohen Datenschutzniveaus, zugleich aber auch die Beseitigung von Hemmnissen für den Verkehr personenbezogener Daten innerhalb der Union, weshalb die Vorschriften zum Datenschutz unionsweit gleichmäßig und einheitlich angewandt werden sollen. Ein vollkommen eigenständiges Datenschutzrecht der Mitgliedsstaaten sei damit kaum vereinbar.[413] Auch das Primärrecht gebiete keine andere Auslegung, da einerseits ein gewisser Mindeststandard nach Art. 8 EU-GRC eingehalten werden müsse, andererseits der Grundsatz des freien Datenverkehrs und die Grundrechte der für den Datenschutz verantwortlichen Stelle bestimmte Höchstgrenzen verlangen; überdies hinaus

410 *Maschmann*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 88 DSGVO Rn. 33.
411 *Maschmann*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 88 DSGVO Rn. 34.
412 *Maschmann*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 88 DSGVO Rn. 35.
413 *Maschmann*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 88 DSGVO Rn. 36.

fehle den Mitgliedsstaaten wegen des Anwendungsvorrangs der DSGVO schlicht die Regelungsbefugnis.[414] Auch das teilweise in der Literatur[415] eingebrachte Argument, dass sich weitrechende Vorgaben für mitgliedsstaatliche Vorschriften nicht mehr auf Art. 16 Abs. 2 AEUV stützen ließen, sondern lediglich auf Art. 153 Abs. 2 UAbs. 1 lit. b AEUV, welche die Befugnisnorm zum Erlass arbeitsrechtlicher Vorschriften darstelle, sei schließlich nicht schlagkräftig. Zwar werde die DSGVO tatsächlich nur auf Art. 16 Abs. 2 AEUV gestützt und der von Art. 153 Abs. 1 AEUV erfasste Bereich der „Arbeitsbedingungen" und „Schutz der Arbeitsumwelt" mitgeregelt. Dies geschehe allerdings lediglich als Annex; der Schwerpunkt der DSGVO hingegen liege im Schutz personenbezogener Daten sowie im freien Datenverkehr, der unter Art. 16 Abs. 2 AEUV falle. Der Ausgleich von Arbeitnehmer- und Arbeitgeberinteressen sei von der DSGVO nicht in erster Linie bezweckt, auch wenn sich die DSGVO als Querschnittsregelung auf das Arbeitsrecht und andere Rechtsgebiete auswirke.[416]

Auch *Gola*, *Pötters* und *Thüsing* treten dem grundsätzlich bei, dass die Richtlinie eine Vollharmonisierung des Datenschutzes bewirkt und der Wortlaut eindeutig nur „spezifischere" Vorschriften erlaube und daher grundsätzlich Abweichungen vom Schutzstandard der DSGVO nicht zulasse. Sie legen sich jedoch nicht derart fest, dass Abweichungen nach oben generell unzulässig seien.[417]

cc) Festlegung eines Mindeststandards für den Beschäftigtendatenschutz

Die wohl überwiegende Auffassung sieht in Art. 88 Abs. 1 DSGVO lediglich die Festlegung eines Mindeststandards für den Beschäftigtendatenschutz.[418] Begründet wird dies damit, dass die bereits genannten Einschränkungen der Parlaments- sowie Kommissionsfassung in der endgülti-

414 *Maschmann*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 88 DSGVO Rn. 38.

415 Ehmann/Selmayr/*Selk*, Art. 88 DSGVO Rn. 13 ff.; Plath/*Stamer/Kuhnke*, Art. 88 DSGVO Rn. 2; *Franzen*, DuD 2012, 322 (326); *Körner*, ZESAR 2013, 153 (154).

416 *Maschmann*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 88 DSGVO Rn. 39.

417 Vgl. *Gola/Pötters/Thüsing*, RDV 2016, 57 (59).

418 Sydow/*Tiedemann*, Art. 88 DSGVO Rn. 3; *Düwell/Brink*, NZA 2016, 665 (668); Paal/Pauly/*Pauly*, Art. 88 DSGVO Rn. 4; *Wybitul/Sörup/Pötters*, ZD 2015, 559 (561); *Kort*, DB 2016, 711 (714); *Tiedemann*, ArbRB 2016, 334; *Körner*, NZA 2019, 1389; Plath/*Stamer/Kuhnke*, Art. 88 DSGVO Rn. 7.

gen Regelungen gerade keinen Einschlag gefunden haben.[419] Im Übrigen sei eine Mindestharmonisierung im Arbeitsrecht ausreichend, um ein hinreichendes Schutzniveau zu garantieren und gleichzeitig die Vorteile eines Regulierungswettbewerbs zu nutzen.[420] Ferner sei die Öffnungsklausel im Vergleich zu anderen Öffnungsklauseln, wie beispielsweise dem Art. 85 DSGVO für den Ausgleich von Meinungs- und Pressefreiheit mit dem Datenschutz, weiter gefasst.[421] Art. 85 DSGVO bestimmt, dass die nationalen Vorschriften mit der DSGVO „in Einklang" zu bringen sind. Auch der Schutzzweck der DSGVO – Schutz der Grundrechte und Grundfreiheiten der Betroffenen – spreche dafür, lediglich einen Mindeststandard vorzusehen, da strengere Regelungen naturgemäß das Ziel noch besser erreichen.[422] Letztlich sei es auch eine Kompetenzfrage: Der Union stehe zum Beschäftigtendatenschutz keine Kompetenz für eine Vollharmonisierung in einer Verordnung zu, weswegen in Art. 88 DSGVO eine Öffnung vorgesehen sei. Die Vorgabe, nicht strenger sein zu dürfen, ginge stark in die Richtung einer Vollharmonisierung und stünde im Widerspruch mit Art. 153 Abs. 2 lit. b AEUV, wonach nur eine Mindestharmonisierung möglich ist, vor allem aber auch mit Art. 153 Abs. 4 AEUV, der ausdrücklich regle, dass eine aufgrund von Art. 153 AEUV erlassene Bestimmung, die Mitgliedsstaaten nicht daran hindern darf, strengere Schutzmaßnahmen beizubehalten oder zu treffen.[423]

dd) Abweichung nach oben nur in einem bestimmten Rahmen möglich

Nolte ist schließlich der Auffassung, dass Abweichungen nach unten keinesfalls, Abweichungen nach oben grundsätzlich, jedoch nicht unbegrenzt, möglich sein sollen.[424] Er begründet seine Auffassung damit, dass durch unterschiedliche Standards die Gewährleistung des freien Datenverkehrs innerhalb der Mitgliedsstaaten und damit das reibungslose Funktionieren des Binnenmarkts beeinträchtigt seien. Dies sei aber gerade auch

419 Paal/Pauly/*Pauly*, Art. 88 DSGVO Rn. 4; *Wybitul/Sörup/Pötters*, ZD 2015, 559 (561); Plath/*Stamer/Kuhnke*, Art. 88 DSGVO Rn. 6.
420 *Wybitul/Sörup/Pötters*, ZD 2015, 559 (561).
421 *Gola/Pötters/Thüsing*, RDV 2016, 57 (59 f.).
422 So noch Ehmann/Selmayr (2017)/*Selk*, Art. 88 DSGVO Rn. 59.
423 So noch Ehmann/Selmayr (2017)/*Selk*, Art. 88 DSGVO Rn. 61.
424 *Nolte*, in: Gierschmann et al., Kommentar Datenschutz-Grundverordnung, Art. 88 DSGVO Rn. 22.

ein Ziel der DSGVO, wie Art. 1 Abs. 3[425] zeige. *Nolte* stellt allerdings klar, dass die Entscheidungen des EuGH zur Vollharmonisierung bei der bisherigen Richtlinie im Rahmen von Art. 88 DSGVO gerade nicht gelten kann und die Rechtsprechung daher nur behutsam übertragen darf.[426] Auch *Forst* schränkt das zulässige „Mehr" an Datenschutz im Hinblick auf die Rechtsprechung des EuGH zur Richtlinie 95/46/EG dahingehend ein, dass das bestehende Recht zur Datenverarbeitung nicht unverhältnismäßig begrenzt werden darf.[427]

In dieselbe Richtung argumentiert auch *Körner*, die feststellt, dass aus der Konzeption, Entstehungsgeschichte und dem Telos hervorgehe, dass die Verordnung jedenfalls als Mindeststandard gemeint ist und daher die allgemeinen Datenschutzregelungen der Verordnung nicht unterschritten werden dürften; ein vollständiges Verbot der Verarbeitung von Daten im Beschäftigungsverhältnis würde jedoch gegen Art. 1 Abs. 3 DSGVO verstoßen und wäre nicht mehr von Art. 88 Abs. 1 DSGVO gedeckt.[428] Grundsätzlich seien die Öffnungsklauseln einer Verordnung zwar eng auszulegen, um dem Harmonisierungsziel gerecht zu werden. Auf die konkrete Formulierung der Klausel müsse jedoch immer geachtet werden. Dem Berichterstatter des Europäischen Parlaments sei die Formulierung der Kommission zu eng gewesen, weil er nationale Regelungen „nach oben" zulassen wollte, weshalb er in den Entwurf einfügte, dass die nationalen Bestimmungen „in Übereinstimmung mit den Bestimmungen der Verordnung" sein sollen. Selbst diese Beschränkung sei nun jedoch weggefallen, was zeige, dass die ursprünglich vorgesehene Beschränkung gerade nicht beibehalten werden sollte. Jedenfalls die Grundprinzipien aus Art. 5 DSGVO sowie die Einschränkungen des Art. 88 Abs. 2 DSGVO müssten aber eingehalten werden. Da jedoch in Art. 88 Abs. 2 – anders als in Art. 1 Abs. 3 DSGVO - der Persönlichkeitsschutz und die Informationsfreiheit gerade nicht gleichwertig nebeneinander gestellt werden, sondern die nationalen Regelungen zum Beschäftigtendatenschutz „die Grundrech-

425 Wortlaut: „Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden."

426 *Nolte*, in: Gierschmann et al., Kommentar Datenschutz-Grundverordnung, Art. 88 DSGVO Rn. 22.

427 Auernhammer (5. Aufl. 2017)/*Forst*, Art. 88 DSGVO Rn. 4; interessanterweise findet sich diese Einschränkung in der aktuellen Auflage jedoch nicht mehr, vgl. Auernhammer/*Forst*, Art. 88 DSGVO Rn. 4 ff.

428 *Körner*, Wirksamer Beschäftigtendatenschutz im Lichte der Europäischen Datenschutz-Grundverordnung (DS-GVO), S. 54 f.

te der betroffenen Person“ schützen müssen, scheide eine Abwägung mit der unternehmerischen Freiheit in Art. 16 EU-GRC aus und eine negative Abweichung vom Niveau der DSGVO sei daher unzulässig.[429] Der Beschäftigtendatenschutz müsse jedoch vor dem Hintergrund der DSGVO geregelt werden.[430] Zwar sei es dem europäischen Gesetzgeber vor dem Hintergrund des Art. 153 i.V.m. Art. 114 Abs. 2 AEUV nicht erlaubt, eine Höchstgrenze für den arbeitsrechtlichen Schutz in einer EU-Verordnung festzulegen, der widersprüchliche Ansatz der DSGVO sei jedoch ebenfalls zu bedenken. So wolle die Verordnung gem. Art. 1 Abs. 1 einerseits den Binnenmarkt durch den freien Datenverkehr fördern und andererseits dem Einzelnen Datenschutz gewähren.[431]

b) Stellungnahme

aa) Wortlaut

Es ist der Literatur zuzustimmen, dass der Wortlaut im vorliegenden Fall keine große Auslegungshilfe darstellt. Wie bereits an der Diskussion in der Literatur ersichtlich kann „spezifischere“ im Sinne von „sektorspezifisch“, also im Hinblick auf die Verarbeitung im Beschäftigungskontext, zu verstehen sein,[432] aber auch dergestalt, dass lediglich die recht allgemeinen Vorschriften der DSGVO konkretisiert werden, aber inhaltlich keine Abweichung stattfinden dürfen.[433] Letztlich könnte man hier – wie *Düwell* und *Brink* – dem Verordnungsgeber auch vorwerfen, dass er „nur dem weit verbreiteten Trend erlegen ist, die Größe der Bedeutung, die jemand einer Sache beimisst, durch die sinnlose Steigerung von Adjektiven und Adverbien zum Ausdruck zu bringen“[434]. Letzteres Argument überzeugt insofern, als der Verordnungsgeber im verbundenen Erwägungsgrund 155 diese sprachliche Steigerungsform gerade nicht verwendet. Der Steigerung

429 *Körner*, Wirksamer Beschäftigtendatenschutz im Lichte der Europäischen Datenschutz-Grundverordnung (DS-GVO), S. 56 f.
430 *Körner*, Wirksamer Beschäftigtendatenschutz im Lichte der Europäischen Datenschutz-Grundverordnung (DS-GVO), S. 67.
431 *Körner*, NZA 2016, 1383.
432 *Traut*, RDV 2016, 312 (314).
433 *Spelge*, DuD 2016, 775 (778); *Maschmann*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 88 DSGVO Rn. 32.
434 *Düwell/Brink*, NZA 2017, 1081 (1082).

des linguistischen Positivs „spezifisch" sollte daher keine zu große Bedeutung beigemessen werden.

bb) Systematik

Zwar spricht die Handlungsform der Verordnung grundsätzlich für eine Vollharmonisierung.[435] Allerdings ist es sehr wohl möglich, auch in einer Verordnung Mitgliedsstaaten Abweichungen in einem gewissen Spektrum zu gestatten und somit für bestimmte Bereiche nur einen Mindeststandard festzulegen.[436] Aufgrund der zahlreichen Öffnungsklauseln, die letztlich im Rahmen der Trilog-Verhandlungen eingefügt wurden, ist eine Vollharmonisierung ohnehin nicht mehr erreichbar, weshalb die Verordnung auch gerne als „Hybrid" bezeichnet wird.[437] Ein Vergleich mit der Regelung in Art. 85 Abs. 2 DSGVO zur „Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit" zeigt, dass der Verordnungsgeber durchaus Regelungen in der DSGVO vorgesehen hat, die den Mitgliedsstaaten ausdrücklich explizite Abweichungen oder Ausnahmen von bestimmten Kapiteln der DSGVO – insbesondere auch von den Grundsätzen (Kapitel II) erlauben. Eine solche Ausnahmebestimmung enthält Art. 88 DSGVO nicht, was dafürspricht, keine sehr weite Regelungsbefugnis der Mitgliedsstaaten anzunehmen.

cc) Telos

Gegenstand und Ziel der Verordnung werden in Art. 1 DSGVO geregelt. Gegenstand sind nach Absatz 1 Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten. Die Ziele sind in den Absätzen 2 und 3 geregelt, wonach einerseits die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere deren Recht auf Schutz personenbezogener Daten ge-

435 So auch *Maschmann*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 88 DSGVO Rn. 34; *Micklitz/Rott*, H. V. Verbraucherschutz, in: Dauses/Ludwigs, Handbuch des EU-Wirtschaftsrechts, Rn. 41.

436 *Micklitz/Rott*, H. V. Verbraucherschutz, in: Dauses/Ludwigs, Handbuch des EU-Wirtschaftsrechts, Rn. 42: Hier wird auf die VO EG 2006/2004 verweisen, die ebenfalls im Bereich des Verbraucherschutzes lediglich einen Mindeststandard festlegt.

437 Vgl. *Buchner/Kühling*, DuD 2017, 544 (546); *Kühling/Martini*, EuZW, 448 (449).

schützt werden sollen, andererseits der Verkehr personenbezogener Daten aus Gründen des Schutzes jedoch weder eingeschränkt noch verboten werden soll. Die Formulierung ist, wie *Körner* bereits kritisiert hat, tatsächlich widersprüchlich[438], spiegelt jedoch im Ergebnis lediglich die Abwägung des Grundrechts aus Art. 8 EU-GRC auf Schutz personenbezogener Daten mit dem Grundrecht aus Art. 16 EU-GRC, der unternehmerischen Freiheit, unter Wahrung des Verhältnismäßigkeitsprinzips wider. Diese sind in praktische Konkordanz zu bringen, vgl. Art. 52 Abs. 1 S. 2 EU-GRC. In Erwägungsgrund 4 der DSGVO wird dies ebenfalls klargestellt: „*Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden.*" Dass die Vereinheitlichung durch die DSGVO ein angestrebtes Ziel ist, da die Richtlinie nicht zur gewünschten Angleichung des Rechts und somit zu einem bestimmten Schutzniveau geführt hat, machen Erwägungsgrund 9 und 10 deutlich. Nichtsdestotrotz spricht gerade Erwägungsgrund 10 von der Gewährleistung eines „gleichwertigen Schutzniveaus", das auch als Mindeststandard verstanden werden kann. Ferner heißt es dort, dass es „in den Mitgliedsstaaten mehrere sektorspezifische Rechtsvorschriften in Bereichen, die spezifischere Bestimmungen erfordern", gibt und diese Verordnung den Mitgliedsstaaten einen Spielraum für die Spezifizierung ihrer Vorschriften gebe. So sollten gemäß Erwägungsgrund 52 gerade im Arbeitsrecht Ausnahmen vom Verbot der Verarbeitung sensitiver Daten erlaubt sein, wenn sie im Unionsrecht oder dem Recht der Mitgliedsstaaten vorgesehen sind. Erwägungsgrund 155 erwähnt die Öffnungsklausel für spezifische Vorschriften für Mitgliedsstaaten, bringt jedoch im Hinblick auf die Reichweite keinen weiteren Erkenntnisgewinn.

Es lässt sich festhalten, dass trotz des Zwecks der DSGVO – Vereinheitlichung des Datenschutzes – nicht eindeutig klargestellt ist, dass die Verordnung *vollständige* Harmonisierung des Datenschutzrechts in den Mitgliedsstaaten abzielt. Vielmehr muss davon ausgegangen werden, dass ein Mindeststandard festgelegt werden soll, der nicht unterschritten werden darf, gleichzeitig aber auch eine Begrenzung der Regelungsbefugnis durch die unternehmerische Freiheit erfolgt. Letztlich darf das Schutzniveau der Mitgliedsstaaten nicht dazu führen, dass der unionsweite freie Verkehr der Daten behindert wird und somit ein Hemmnis für die unionsweite Ausübung von Wirtschaftstätigkeiten geschaffen wird, welches den Wettbe-

438 *Körner*, NZA 2016, 1383.

werb verhindert.[439] Es stellt sich jedoch die Frage, ob ein höheres Schutzniveau beim Beschäftigtendatenschutz tatsächlich zu Wettbewerbsverzerrungen führen würde. Dies wurde in der Literatur bislang kaum beachtet. Lediglich *Pötters* führt hierzu aus, dass regelmäßig ein binnengrenzüberschreitender Bezug im Verhältnis Arbeitgeber und Beschäftigtem fehle, denn die spezifischen Probleme des Arbeitsrechts, wie Fragerecht, Videoüberwachung am Arbeitsplatz, Erhebung sensibler Daten über die Gesundheit etc. seien regelmäßig Probleme, die sich auf nationale Sachverhalte beschränken. Aus diesem Grund sei nicht ersichtlich, weshalb durch unterschiedlich hohe Datenschutzstandards Marktbeschränkungen verursacht werden könnten.[440] Dem ist grundsätzlich zuzustimmen; es wird kaum Beschäftigte geben, die aufgrund spezifischer Regelungen zum Beschäftigtendatenschutz eine Art *Forum Shopping* danach betreiben, welcher Mitgliedsstaat den höchsten Datenschutzstandard hat und somit problematische (spürbare) Wettbewerbsverzerrungen entstehen würden. Ganz anders sieht es hierbei beispielsweise bei Betreibern von sozialen Netzwerken, Cloud-Diensten etc. aus – hier führen verschiedene nationale Datenschutzstandards selbstverständlich zu Marktverzerrungen. Ein (neues) Unternehmen wird sich dort niederlassen, wo die geringsten Standards und somit die geringsten Kosten entstehen. Für den Arbeitnehmer entstehen einerseits keine (Mehr-)Kosten durch unterschiedliche Datenschutzstandards, noch wird er seinen Lebensmittelpunkt danach richten.

Das *Telos* gebietet daher keine vollständige Vereinheitlichung des Datenschutzes für Beschäftigte.

dd) Historie

Auch die historische Auslegung führt zu keinem anderen Ergebnis. Es ist *Maschmann* zu folgen, dass es an aussagekräftigten Belegen fehlt, dass durch die Änderung des Wortlauts eine vollständige Freigabe des Beschäftigtendatenschutzes stattfinden sollte. Zwar behauptet *Körner*, dass dem Berichterstatter des EP die Formulierung zu eng gewesen sei und Vorschriften nach oben zugelassen werden sollten.[441] Nachweise hierfür gibt es jedoch nicht. Vielmehr hatte das EP nicht unerhebliche inhaltliche

439 Vgl. Erwägungsgrund 9.
440 *Pötters*, RDV 2015, 10 (12 f.).
441 *Körner*, Wirksamer Beschäftigtendatenschutz im Lichte der Europäischen Datenschutz-Grundverordnung (DS-GVO), S. 56 f.

Ergänzungen zur inhaltlichen Regelung des Arbeitnehmerdatenschutzes vorgeschlagen.[442] Auch dies spricht dafür, dem Wegfall bzw. den zahlreichen Änderungen am Wortlaut durch die verschiedenen Entwürfe und schließlich dem Wegfall der Ergänzung „in den Grenzen der Verordnung" in den Trilog-Verhandlungen keine zu große Aussagekraft beizumessen.

Der Verweis auf die Vorgängerrichtlinie und der hierzu ergangenen Rechtsprechung des EuGH[443] hilft nur bedingt weiter. Es ist zwar zutreffend, dass die DSGVO ausweislich Erwägungsgrund 9 dieselben Ziele wie die RL 95/46/EG verfolgt und der EuGH bei der Entscheidung über die vollharmonisierende Wirkung der Richtlinie auf die Ziele abgestellt hat.[444] Anders als die DSGVO mit Art. 88 enthielt diese jedoch keine Öffnungsklausel zugunsten der mitgliedsstaatlicher Regelungen, sodass die hierzu ergangene Rechtsprechung nicht einfach übertragen werden kann,[445] denn eine solche Klausel eröffnet für Mitgliedsstaaten gerade die Möglichkeit abweichende Vorschriften zu erlassen. Sicherlich ist bei der Auslegung der vollharmonisierende Charakter der Vorgängerregelung zu beachten. Daraus darf jedoch nicht schlussgefolgert werden, dass trotz der Existenz von Art. 88 DSGVO keinerlei Abweichungsmöglichkeit der Mitgliedsstaaten bzw. Parteien von Kollektivvereinbarungen besteht.

ee) Primärrechtskonforme Auslegung

Vielfach wird gegen eine vollharmonisierende Wirkung der DSGVO im Bereich des Arbeitsrechts vorgebracht, dass einer solchen Art. 153 i.V.m. Art. 114 AEUV entgegenstehe, wonach die Europäische Union nur Mindeststandards in Form von Richtlinien erlassen dürfe.[446] Hierbei wird – wie *Maschmann* bereits richtig erkannt hat – übersehen, dass die Regelung des Arbeitnehmerdatenschutzes lediglich als Annex stattfindet und die DSGVO nicht bezweckt, spezifisch den Arbeitnehmerdatenschutz zu

442 EuArbRK/*Franzen*, Art. 88 DSGVO Rn. 3 mit Hinweis auf Standpunkt des EP vom 12.03.2014, P7_TC1 COD [2012] 011, S. 69 f.
443 EuGH, Urt. v. 24.11.2011 – C-468/10, C-469/10, CR, 2012, 29 – ASNEF.
444 EuGH, Urt. v. 24.11.2011 – C-468/10, C-469/10, CR, 2012, 29 (30) – ASNEF.
445 So auch *Nolte*, in: Gierschmann et al., Kommentar Datenschutz-Grundverordnung, Art. 88 DSGVO S. 22.; a.A. EuArbRK/*Franzen*, Art. 88 DSGVO Rn. 9.
446 *Kersting*, Moderner Beschäftigtendatenschutz nach der DS-GVO und dem BDSG-neu?, in: Buhl et al., Der erwachte Gesetzgeber, S. 73 f.; *Wroblewski*, NZA 2015, Editorial zu Heft 21; so wohl auch Plath/*Stamer/Kuhnke*, Art. 88 DSGVO Rn. 2; *Franzen*, DuD 2012, 322 (326); *Körner*, ZESAR 2013, 153 (154).

regeln.[447] Dem widerspricht zwar *Wroblewski*[448] und behauptet, dass die Regelung des Beschäftigtendatenschutzes nicht lediglich Annex zum allgemeinen Datenschutz sei. Zur Begründung führt er an, dass beispielsweise das Fragerecht des Arbeitgebers ein wesentlicher Bestandteil des Arbeitsrechts ist und nicht einfach unter das allgemeine Datenschutzrecht subsumiert oder an dieses angehängt werden kann. Dabei wird jedoch übersehen, dass Art. 88 DSGVO die spezifische Regelung arbeitsrechtlicher Besonderheiten durch die Mitgliedsstaaten, Tarifpartner und Betriebspartner erst möglich macht und darauf nicht speziell Bezug nimmt. Vielmehr geht es bei der Reichweite der Öffnungsklausel um die Frage, ob die festgelegten Standards der DSGVO *auch* im Bereich des Arbeitsrechts eingehalten werden müssen oder ob die Mitgliedsstaaten hierbei ein vollständig eigenständiges Datenschutzregime schaffen können.

Man könnte in diesem Zusammenhang allenfalls überlegen, ob der Rechtsgedanke des Art. 153 AEUV auch auf Öffnungsklauseln in Verordnungen anzuwenden ist, denn unmittelbar ist die Norm, die sich ausschließlich auf Richtlinien bezieht, nicht anwendbar. Ausweislich des Erwägungsgrunds 12 ist die DSGVO auf Basis der Ermächtigungsgrundlage in Art. 16 Abs. 2 AEUV erlassen worden. Können für einen Rechtssetzungsakt mehrere Rechtsgrundlagen herangezogen werden, ist der Schwerpunkt, also das vorherrschende oder hauptsächliche Regelungsziel, zu ermitteln. Inhalt und Zweck der Maßnahme bestimmen dies und müssen bei der Wahl der Rechtsgrundlage objektiv und gerichtlich überprüfbar sein.[449] Die DSGVO enthält keine arbeitsrechtlichen Regelungen, sondern lediglich eine Öffnungsklausel für den Arbeitnehmerdatenschutz. Sie stellt jedoch als „Querschnittsregelung“[450] grundsätzliche Rahmenbedingungen für den Arbeitnehmerdatenschutz auf. Da Art. 153 Abs. 2 UAbs. 1 lit. b AEUV mit „Arbeitsbedingungen“ auch den spezifischen Arbeitnehmerdatenschutz erfasst, hat die Union auf dieser Grundlage lediglich die Kompetenz zur Mindestharmonisierung durch Richtlinien, wie sich aus dem expliziten Wortlaut ergibt. Aufgrund der Querschnittswirkung wirkt die DSGVO auch für den Bereich des Datenschutzes von Beschäftigten vollharmonisierend, soweit die Öffnung für „spezifische Regelungen“

447 *Maschmann*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 88 DSGVO Rn. 39.
448 *Wroblewski*, NZA 2015, Editorial zu Heft 21.
449 EuGH, Urt. v. 27.02.2014 – C-656/11, BeckRS 2014, 80469, Rn. 47 – Kommission / Vereinigtes Königreich m.w.N.; ferner EuArbRK/*Franzen*, Art. 153 AEUV Rn. 70.
450 EuArbRK/*Franzen*, Art. 153 AEUV Rn. 76.

nach Art. 88 Abs. 1 DSGVO nicht greift.[451] Im Bereich der Spezifizierungsklausel spricht aber vieles dafür, in Anlehnung an die Begrenzung der Kompetenz in Art. 153 Abs. 2 UAbs. 1 lit. b AEUV dem unionalen Rechtsetzer auch nur eine Kompetenz zur Festlegung von Mindeststandards zuzubilligen.

Dies führt aber dennoch nicht dazu, dass es den Mitgliedsstaaten freisteht, nach „oben offen" zu regulieren. Hier stünde Art. 153 Abs. 4 AEUV entgegen, wonach strengere Schutzmaßnahmen mit den Verträgen vereinbar sein müssen. In diesem Zusammenhang hat der EuGH bereits in der Entscheidung *Alemo-Herron* klargestellt, dass der Regelungsspielraum der Mitgliedsstaaten im Rahmen der Betriebsübergangs-Richtlinie 2001/23/EG durch die unternehmerische Entscheidungsfreiheit des Art. 16 EU-GRC beschränkt ist.[452] Dies gilt aufgrund des Vorrangs des EU-Rechts und Art. 6 Abs. 3 EUV, 52 Abs. 1 EU-GRC auch für die Ausfüllung der Öffnungsklauseln der DSGVO durch die Mitgliedsstaaten.

c) Ergebnis

Die Öffnungsklausel in Art. 88 Abs. 1 DSGVO für „spezifischere Vorschriften" ist im Sinne des Grundsatzes *„lex specialis derogat legi generali"* zu verstehen.[453] Sofern die Mitgliedsstaaten/Tarifpartner/Betriebspartner „sektorspezifische", m.a.W. spezielle Vorschriften für den Datenschutz von Beschäftigten aufstellen, wie beispielsweise das Fragerecht des Arbeitgebers, gehen diese Vorschriften der DSGVO vor. Dabei sind die Normgeber selbstverständlich nicht völlig frei, denn die Grundrechte der EU-GRC sind beim Erlass von Vorschriften zu beachten, ebenso die (Mindest-)Anforderungen des Art. 88 Abs. 2 DSGVO. Zwar sind im Grundsatz nach Art. 88 Abs. 1 DSGVO Abweichungen sowohl nach oben als nach unten grundsätzlich möglich; Art. 88 Abs. 2 DSGVO begrenzt den Handlungsspielraum jedoch dahingehend, dass ein negatives Abweichen vom Schutzniveau der DSGVO kaum denkbar ist.[454]

---

451 Vgl. *Seifert*, EuZA 2018, 51 (55 f.); *Franzen*, DuD 2012, 322 (326).

452 EuGH, Urt. v. 18.07.2013 – C-426/11, NZA, 2013, 835 (836) – Alemo-Herron Rn. 28, 32 ff.; EuArbRK/*Franzen*, Art. 153 AEUV Rn. 58.

453 So auch BeckOK DatenSR/*Riesenhuber*, Art. 88 DSGVO Rn. 16; *Niklas/Thurn*, BB 2017, 1589 (1594); *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, Art. 88 DSGVO Rn. 15; so i.E. wohl nunmehr auch Plath/*Stamer/Kuhnke*, Art. 88 DSGVO Rn. 3.

454 Vgl. *Jerchel/Schubert*, DuD 2016, 782 (783).

Unzulässig wäre es im Hinblick auf Art. 88 Abs. 2 i.V.m. Art. 5 Abs. 1 lit. c DSGVO daher, das Fragerecht des Arbeitgebers dahingehend zu erweitern, dass jede Frage – sei sie noch so unerheblich für das Arbeitsverhältnis – zugelassen wird. Hierin läge ein evidenter Verstoß gegen den Grundsatz der „Datenminimierung". Im Übrigen würde die nach Art. 51 Abs. 1 EU-GRC vorzunehmende Abwägung von Art. 8 EU-GRC und Art. 16 Abs. 1 AEUV übergangen werden.

Überträgt man den Rechtsgedanken des Art. 153 AEUV auf die Öffnungsklausel, so darf aber genauso nicht jegliche Überwachung der Arbeitnehmer durch den Arbeitgeber vollständig durch nationales Datenschutzrecht verboten werden, da hierdurch die unternehmerische Freiheit des Arbeitgebers aus Art. 16 EU-GRC verletzt würde, die nach Art. 153 Abs. 4 AEUV i.V.m. Art. 6 Abs. 3 EUV, Art. 51 Abs. 1 AEUV ebenfalls beim Erlass normkonkretisierender Vorschriften zu beachten ist. Art. 88 Abs. 2 DSGVO hingegen, welcher nur von der „Wahrung der Interessen und Grundrechte der betroffenen Person", nicht aber derer des Verarbeiters spricht, stünde dem wiederum nicht entgegen.

Zulässig bleiben aber jedenfalls alternative Regelungsmechanismen, die die Grundrechte und Interessen aller Beteiligten, insbesondere den Verhältnismäßigkeitsgrundsatz sowie die Vorgaben des Art. 88 Abs. 2 DSGVO wahren.[455] So könnten Mitgliedsstaaten beispielsweise für die Einwilligung bestimmte Szenarien vorsehen, in denen eine Freiwilligkeit (widerleglich) vermutet wird, auch wenn die DSGVO eine solche Vermutung zugunsten des Verarbeiters nicht vorsieht.

2. Nationaler Erlaubnistatbestand für den Beschäftigtendatenschutz: § 26 BDSG

Mit § 26 BDSG hat der deutsche Gesetzgeber auf Grundlage des Art. 88 Abs. 1 DSGVO einen eigenständigen Erlaubnistatbestand für das Beschäftigtendatenschutzrecht geschaffen, der bis auf einzelne Erweiterungen weitgehend identisch mit der alten Regelung des § 32 BDSG 2009 ist.[456] Dieser Erlaubnistatbestand konkretisiert hierbei die allgemeine Bestim-

455 So im Ergebnis auch *Imping*, CR 2017, 378 (381); wohl auch *Klösel/Mahnhold*, NZA 2017, 1428 (1431).

456 Vgl. hierzu die Gesetzesbegründung, BT-Drs. 18/11325, S. 96 f.: „§ 26 führt die spezialgesetzliche Regelung des § 32 BDSG a.F. fort."

mung des Art. 6 Abs. 1 lit. b DSGVO hinsichtlich der Datenverarbeitung im Rahmen eines rechtsgeschäftlichen Schuldverhältnisses.[457]

a) Der Begriff des Beschäftigten im Sinne des Datenschutzrechts

§ 26 Abs. 1 BDSG normiert eine Spezialregelung für die Verarbeitung von personenbezogenen Daten bei Beschäftigten. Der Begriff des Beschäftigten ist vom arbeitsrechtlichen Arbeitnehmerbegriff zu unterscheiden. Dies ergibt sich bereits aus § 26 Abs. 8 Nr. 8 BDSG, wonach Bewerberinnen und Bewerber ebenfalls als Beschäftigte im Sinne des BDSG angesehen werden müssen. Aufgrund des Umstands, dass § 26 BDSG auf Basis der Öffnungsklausel des Art. 88 DSGVO geschaffen wurde, ist der europarechtliche Beschäftigtenbegriff maßgeblich.[458] Anders als in anderen Bestimmungen des europäischen Sekundärrechts[459] erlaubt es die DSGVO den Mitgliedsstaaten gerade nicht Inhalt, Reichweite und Bedeutung des Begriffs des Beschäftigten zu konkretisieren.[460] Andernfalls wäre der Zweck der Datenschutzgrundverordnung, die (weitgehende) Vereinheitlichung des Datenschutzschutzrechts konterkariert: Die Mitgliedsstaaten könnten durch eigene Begriffsbildungen die Reichweite der Öffnungsklauseln und somit die Anwendbarkeit der DSGVO bestimmen.[461]

b) Erforderlichkeit der Datenverarbeitung gem. § 26 Abs. 1 BDSG

Im Kern ist die Zulässigkeit der Datenverarbeitung weiterhin am Begriff der *Erforderlichkeit* zu messen. Es ist eine Interessensabwägung vorzunehmen, die den Verhältnismäßigkeitsgrundsatz berücksichtigen muss.[462] Im

457 *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 18.
458 *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, S. 139.
459 Bspw. Art. 2 Nr. 1d der RL 2001/23/EG (Betriebsübergangsrichtlinie).
460 *Maschmann*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 88 DSGVO Rn. 8.
461 *Maschmann*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 88 DSGVO Rn. 9; *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, S. 139.
462 *Gola/Thüsing/Schmidt*, DuD 2017, 244 (245); *Kort*, ZD 2017, 319 (320).

Rahmen der Erforderlichkeitsprüfung[463] sind die widerstreitenden Grundrechtspositionen abzuwägen und in praktische Konkordanz zu bringen, d.h. die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten sind zu einem schonenden Ausgleich zu bringen.[464]

Zu beachten ist, dass im Rahmen der (Grundrechts-)Abwägung grundsätzlich die europäischen und nicht die nationalen Grundrechte maßgeblich sind.[465] In der Entscheidung *Recht auf Vergessen II* hat das Bundesverfassungsgericht insofern klargestellt, dass der europäische Grundrechtsschutz nicht dem nationalen in allen Einzelheiten gleicht. Würden die DSGVO als vollvereinheitlichtes Unionsrecht am Maßstab des Grundgesetzes gemessen, bestünde die Gefahr, innerstaatliche Maßstäbe vorschnell auch dem Unionsrecht zu unterlegen.[466] Dies gilt auch im Bereich von Öffnungsklauseln, sofern die Öffnung für die vorliegende Konstellation nicht maßgeblich ist.[467]

§ 26 Abs. 1 BDSG stellt prima facie lediglich eine andere Formulierung des allgemeinen Tatbestands des Art. 6 Abs. 1 lit. c DSGVO für den Beschäftigtendatenschutz dar. Dort, wo das nationale Recht vollständig den Vorgaben der DSGVO entspricht, verdrängen die europäischen Grundrechte die nationalen.[468] Allerdings muss beachtet werden, dass der europäische Gesetzgeber im Bereich des Beschäftigtendatenschutzes – wie bereits dargestellt – nur eine Kompetenz zur Mindestharmonisierung hat. Insofern ist der Bereich des Beschäftigtendatenschutzes nicht vollständig durch das Unionsrecht (die DSGVO) determiniert. Aus diesem Grund sind Prüfungsmaßstab primär die nationalen Grundrechte, die allerdings im Lichte der EU-GRC auszulegen sind.[469] Erst wenn das Schutzniveau der unionalen Grundrechte ausnahmsweise nicht gewährleistet ist, hat die Prüfung unmittelbar anhand der EU-GRC zu erfolgen.[470]

---

463 Zur Kritik am Begriff der „Erforderlichkeit", vgl. *Kort*, ZD 2017, 319 (320) m.w.N.
464 BT-Drs. 18/11325, S. 97.
465 BVerfG, Beschl. v. 06.11.2019 – 1 BvR 276/17, NJW 2020, 314 (316) Rn. 41; so auch *Traut*, § 7. Überwachung der Nutzung von Internet und Social Media - Datenschutzrechtliche Grenzen, in: Thüsing/Wurth, Social Media im Betrieb, Rn. 32.
466 BVerfG, Beschl. v. 06.11.2019 – 1 BvR 276/17, NJW 2020, 314 (317) Rn. 45.
467 BVerfG, Beschl. v. 06.11.2019 – 1 BvR 276/17, NJW 2020, 314 (316) Rn. 41.
468 BVerfG, Beschl. v. 06.11.2019 – 1 BvR 276/17, NJW 2020, 314 (316) Rn. 41.
469 BVerfG, Beschl. v. 06.11.2019 – 1 BvR 16/13, NJW 2020, 300 (301) Rn. 42 f.
470 BVerfG, Beschl. v. 06.11.2019 – 1 BvR 16/13, NJW 2020, 300 (304) Rn. 63.

Während auf nationaler Ebene vor allem das allgemeine Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) sowie die allgemeine Handlungsfreiheit (Art. 2 Abs. 1 GG) auf Seiten des Beschäftigten mit der Berufsfreiheit (Art. 12 GG) und der Eigentumsgarantie (Art. 14 GG) auf Seiten des Arbeitgebers abzuwägen sind, sind Gegenstand der Abwägung auf europäischer Ebene das Recht auf Privatheit und dem Schutz personenbezogener Daten (Art. 7 f. EU-GRC[471]) und das Recht auf unternehmerische Freiheit (Art. 16 EU-GRC) sowie die Eigentumsgarantie (Art. 17 EU-GRC).[472] Trotz feingliedriger Unterschiede, die eine Prüfung europäischer Akte am Maßstab der nationalen Rechte verbieten, ist das Abwägungs*ergebnis* im Bereich des Beschäftigtendatenschutzes identisch,[473] sodass auf die dogmatischen Feinheiten dieser Differenzierung nicht näher eingegangen werden muss.

Der nationale Gesetzgeber hatte jedenfalls die Absicht, die spezialgesetzliche Regelung des § 32 BDSG a.F. fortzuführen;[474] insofern soll nach überwiegender Auffassung auch die bisherige BAG-Rechtsprechung weiter Geltung beanspruchen.[475]

Ausweislich der Gesetzesbegründung behält sich der Gesetzgeber vor, „Fragen des Datenschutzes im Beschäftigungsverhältnis innerhalb dieser Vorschrift oder im Rahmen eines gesonderten Gesetzes konkretisierend bestimmte Grundsätze, die im Rahmen der Rechtsprechung zum geltenden Recht bereits angelegt sind, zu regeln. Dies gilt insbesondere für das Fragerecht bei der Begründung eines Beschäftigungsverhältnisses, den expliziten Ausschluss von heimlichen Kontrollen im Beschäftigungsverhältnis, die Begrenzung der Lokalisierung von Beschäftigten sowie den Ausschluss von umfassenden Bewegungsprofilen, den Ausschluss von Dau-

471 Zum Verhältnis zwischen Art. 7 und 8 EU-GRC, *Michl*, DuD 2017, 349.

472 Vgl. *Nebel*, ZD 2018, 520 (522), die daneben auch noch die nationalen Grundrechte sowie die Meinungsfreiheit nach Art. 11 EU-GRC (und Art. 5 GG) nennt.

473 So bereits für die vollharmonisierende Datenschutz-Richtlinie, *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 18 unter Verweis auf BAG, Urt. v. 12.02.2015 – 6 AZR 845/13, NZA 2015, 741 Das Gericht ließ es hierbei im Rahmen einer Verdachtskündigung dahinstehen, ob § 32 Abs. 1 S. 1 BDSG a.F. oder § 28 Abs. 1 S. 1 Nr. 2 BDSG a.F. einschlägig ist.

474 BT-Drs. 18/11325, S. 96 f.

475 *Gola/Thüsing/Schmidt*, DuD 2017, 244 (245) mit zweifelhaftem Verweis auf *Wybitul/Pötters*, RDV, 10 (14); für eine „weitgehende Übertragbarkeit" *Wybitul*, NZA 2017, 413 (415); wohl auch *Gaul/Pitzer*, ArbRB 2017, 241 (242); Paal/Pauly/*Gräber/Nolden*, § 26 BDSG Rn. 14; *Kainer/Weber*, BB 2017, 2740 (2741).

erüberwachungen und die Verwendung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken."[476]

Einen spezifischen Beschäftigtendatenschutz hat der nationale Gesetzgeber jedoch über § 26 Abs. 1 BDSG hinaus (noch) nicht geschaffen; Sonderregelungen gelten nur im Umfang ihres Regelungsgehalts und soweit in der Folge die Öffnungsklausel des Art. 88 DSGVO ausgeschöpft wurde.[477] Sofern ein Sachverhalt von § 26 BDSG nicht erfasst ist, gilt die DSGVO, mit der Folge, dass für solche Verarbeitungszwecke Art. 6 (und Art. 9) anwendbar bleiben und keine Verdrängung durch nationales Recht stattfindet.[478]

§ 26 BDSG ist daher ebenfalls nicht anwendbar, wenn Personaldaten für beschäftigungsfremde Zwecke verwendet werden. In einem solchen Fall gelten die allgemeinen Vorschriften und somit im Grundsatz Art. 6 DSGVO zur Legitimation der Datenverarbeitung.[479] Je weiter die in § 26 Abs. 1 S. 1 BDSG genannten Zwecke auszulegen sind, desto eher fällt eine Verarbeitung unter den nationalen Erlaubnistatbestand und es muss kein Rückgriff auf Art. 6 Abs. 1 lit. f DSGVO erfolgen.[480]

476 BT-Drs. 18/11325, S. 97.

477 Paal/Pauly/*Gräber/Nolden*, § 26 BDSG Rn. 9; *Gola*, BB 2017, 1462 (1463); *Niklas/Thurn*, BB 2017, 1589 (1594).

478 Paal/Pauly/*Gräber/Nolden*, § 26 BDSG Rn. 10 ff.

479 *Gola/Thüsing/Schmidt*, DuD 2017, 244 (245).

480 Hierzu *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 18; zu den einzelnen Zweckbestimmungen des § 26 Abs. 1 S. 1 BDSG siehe weiter unten, **E. § 1 I. 1. b**); zum Verhältnis zwischen § 26 Abs. 1 S. 1 BDSG und Art. 6 Abs. 1 lit. f DSGVO, **E. § 1 III. 2. a**) **bb**) (**2**).

V. Sonderregelungen

1. Sensitive Daten (Art. 9 Abs. 1 DSGVO)

Bestimmte Kategorien von Daten, die besonders das Persönlichkeitsrecht von Betroffenen tangieren[481] (sog. sensitive Daten[482]) unterliegen gem. Art. 9 Abs. 1 DSGVO einem grundsätzlichen Verarbeitungsverbot. Dies betrifft Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit betreffen, aber auch genetische und biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung. Insofern stellt Art. 9 Abs. 1 im Kern auch ein sog. „informationelles Diskriminierungsverbot" dar.[483] Jedenfalls ist es ein Element des Diskriminierungsschutzes.

Der deutsche Gesetzgeber hat mit § 22 BDSG ebenfalls eine besondere Regelung für sensitive Daten geschaffen. Diese Regelung basiert auf Art. 9 Abs. 1 lit. j DSGVO, wobei in Abs. 2 der Regelung eine Reihe an angemessenen und spezifischen Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person genannt werden, wie beispielsweise technisch-organisatorische Maßnahmen, Zugangsbeschränkungen oder Verschlüsselung und Pseudonymisierung[484].

---

481 Siehe Erwägungsgrund 51 S. 1 der DSGVO: „*Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, verdienen einen besonderen Schutz, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können.*"; ferner Paal/Pauly/*Frenzel*, Art. 9 DSGVO Rn. 6: Höchstpersönlicher Charakter der Daten und identitätsstiftender Charakter der Daten für die Betroffenen.

482 Zum Begriff beispielsweise *Weichert*, DuD 2017, 538; kritisch zu diesem Begriff: BeckOK DatenSR/*Albers/Veit*, Art. 9 DSGVO Rn. 7: sensible Daten statt sensitive Daten unter Rückgriff auf die Formulierung des europäischen Gesetzgebers in Erwägungsgrund 10 S. 5 DSGVO; der deutsche und der europäische Gesetzgeber verwenden jedoch den (komplizierteren) Terminus „besondere Kategorien personenbezogener Daten".

483 Das jedoch weitergehend ist, vgl. BeckOK DatenSR/*Albers/Veit*, Art. 9 DSGVO Rn. 4.

484 Wobei diese eigentlich zu den technisch-organisatorischen Maßnahmen gehören, vgl. Art. 32 Abs. 1 lit. a DSGVO.

Eine spezifische, aber nicht abschließende[485] Legitimationsgrundlage im Beschäftigtendatenschutz[486] hat der Gesetzgeber mit § 26 Abs. 3 BDSG in Umsetzung von Art. 9 Abs. 1 lit. b DSGVO geschaffen, wonach die Verarbeitung für Zwecke des Beschäftigungsverhältnisses zulässig ist, wenn sie zur Ausübung von Rechten und Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. In § 26 Abs. 3 S. 2 BDSG verdeutlich der Gesetzgeber, dass die Einwilligung zur Verarbeitung sensitiver Daten auch im Beschäftigungsverhältnis grundsätzlich möglich ist, sofern sie sich ausdrücklich auf diese Daten bezieht.

Art. 9 DSGVO bzw. §§ 22, 26 Abs. 3 BDSG sind jedoch immer im Zusammenhang mit den allgemeinen Erlaubnistatbeständen aus Art. 6 DSGVO bzw. § 26 Abs. 1 BDSG zu lesen; zusätzlich zu den allgemeinen Verarbeitungsanforderungen kommen weitere Voraussetzungen, wenn sensitive Daten verarbeitet werden sollten.[487]

Mit der Verarbeitung sensitiver Daten sind weitgehende Rechtsfolgen verknüpft: So dürfen sie grundsätzlich nicht als Grundlage für automatisierte Einzelfallentscheidungen genutzt werden (Art. 22 Abs. 4 DSGVO). Bei einer „umfangreichen Verarbeitung" sensitiver Daten ist zwingend eine Datenschutzfolgeabschätzung erforderlich (Art. 35 Abs. 3 lit. b DSGVO). Die Bestellung eines Datenschutzbeauftragten ist verpflichtend, wenn die Kerntätigkeit des Verarbeiters oder Auftragsverarbeiters in der „umfangreichen Verarbeitung" solcher Daten liegt (Art. 37 Abs. 1 lit. c DSGVO).[488]

485 BT-Drs. 18/11325, S. 98: „*Die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten für andere Zwecke bleibt unberührt; zum Beispiel richtet sich diese im Fall der Verarbeitung zu Zwecken der Gesundheitsvorsorge nach § 22 Absatz 1 Nummer 1 Buchstabe. b [BDSG].*"

486 Paal/Pauly/*Gräber/Nolden*, § 26 BDSG Rn. 40 f.

487 BeckOK DatenSR/*Albers/Veit*, Art. 9 DSGVO Rn. 1 sprechen in diesem Zusammenhang von einer Überlagerung durch "des die speziellen Freiheitsgewährleitungen konkretisierenden Art. 9 Abs. 2 DSGVO".

488 Zu den weiteren Folgen siehe *Weichert*, DuD 2017, 538 (540 f.), der zu Recht Kritik am unklaren Regime der DSGVO zu den sensitiven Daten ausübt.

2. Erlaubnistatbestand der Kollektivvereinbarung (Art. 88 Abs. 1 Alt. 2 DSGVO)

Im Bereich des Beschäftigtendatenschutzes können die Mitgliedsstaaten durch Kollektivvereinbarungen *spezifischere* Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten treffen. Einige Regelungsbeispiele werden bereits in der Norm selbst benannt: Einstellung von Beschäftigten, Erfüllung des Arbeitsvertrags, Beendigung des Beschäftigungsverhältnisses, Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, Managementzwecke, Planung und Organisation der Arbeit, Gleichheit und Diversität am Arbeitsplatz, Gesundheit und Sicherheit am Arbeitsplatz, Schutz des Eigentums der Arbeitgeber oder der Kunden sowie Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen.

Erwägungsgrund 155 stellt klar, dass vom Begriff „Kollektivvereinbarungen" auch Betriebsvereinbarungen erfasst sind. Neben jeder Form von Betriebsvereinbarungen sind auch Sprecherausschussrichtlinien nach § 28 SpAuG ebenso wie Dienstvereinbarungen nach § 73 BPersVG taugliche Rechtsgrundlagen für die Spezifizierung.[489] Erforderlich ist nach Art. 22 Abs. 2 DSGVO, dass die Kollektivvereinbarungen geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen umfassen.

In diesem Zusammenhang stellt sich das begriffliche Problem der „*spezifischeren* Vorschriften". Wie bereits unter **D. § 1 IV** ausführlich diskutiert, ist das Verständnis im Sinne von „*lex specialis derogat legi generali*" zu verstehen, m.a.W. sind die Betriebspartner und Tarifparteien frei, Regelungen zum Beschäftigtendatenschutz zu treffen, sofern diese die Datenschutzgrundsätze wahren und nach Art. 88 Abs. 2 DSGVO nicht hinter dem Datenschutzniveau der DSGVO zurückbleiben.[490] Ein „Kuhhandel" in der Form, dass beispielsweise ein Betriebsrat oder eine Gewerkschaft beim Datenschutzniveau nachgibt, um an anderer Stelle ein „mehr" für die Mitglieder / Beschäftigten zu erreichen, scheidet damit aus.

Dennoch besteht der Vorteil, dass die Verhandlungspartner nicht an den Interessensausgleich von DSGVO und BDSG gebunden sind, sondern

489 *Seifert*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 88 DSGVO Rn. 27.
490 Ähnlich *Klösel/Mahnhold*, NZA 2017, 1428 (1431).

eigenständige Regelungen verhandeln können,[491] wobei selbstverständlich nach § 75 Abs. 2 BetrVG ebenfalls eine Verhältnismäßigkeitsprüfung unter Abwägung der (nationalen) Grundrechte vorgenommen werden muss,[492] hierbei aber eine Einschätzungsprärogative besteht.[493] Dies rührt auch aus dem „Schutzmechanismus des Kollektivs", das mitunter im Hinblick auf die besonderen Umstände des Arbeitsverhältnisses oder Betriebs das möglicherweise an manchen Stellen unzureichende Schutzniveau der DSGVO bzw. des BDSG oder unpassende Regelungen ausgleichen kann.[494] So bestimmt auch die Gesetzesbegründung, dass solche Vereinbarungen *„die Ausgestaltung eines auf die betrieblichen Bedürfnisse zugeschnittenen Beschäftigtendatenschutzes ermöglichen [sollen]"*.[495]

In Deutschland wurde dieses Recht in § 26 Abs. 4 BDSG spezifiziert: Nach dieser Norm kann die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses auf der Grundlage einer Kollektivvereinbarung erfolgen. Zu beachten ist hierbei, dass § 26 Abs. 4 BDSG aufgrund der Regelung in § 26 Abs. 7 BDSG, wonach sich das Recht über den Beschäftigtendatenschutz auch auf personenbezogene Daten erstreckt, die nicht in einem Dateisystem gespeichert sind, nicht lediglich deklaratorisch ist.[496]

---

491 BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 54; BeckOK DatenSR/*Riesenhuber*, Art. 88 DSGVO Rn. 69.

492 BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205 Rn. 13; Beschl. v. 09.07.2013 – 1 ABR 2/13 (A), NZA 2013, 1433 (1435) Rn. 21 ff.; BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 55.

493 Bejahend einen Beurteilungsspielraum im Hinblick auf die Erforderlichkeit der Datenverarbeitung (im Rahmen von § 75 Abs. 2 BetrVG) bei der Abwägung nationaler Grundrechte, BAG, Beschl. v. 29.06.2004 – 1 ABR 21/03, NZA 2004, 1278 (1280) = BAGE 111, 173 = AP BetrVG § 87 1972 Überwachung Nr. 41 (m. Anm. Ehmann); ebenso *Fitting*, § 75 Rn. 138; *Maier*, DuD 2017, 169 (172); a.A. wohl *Götz*, Big Data im Personalmanagement, S. 60, der einen Rückgriff auf § 26 Abs. 1 BDSG nimmt und den Betriebsparteien nur insoweit einen Spielraum gibt, als nach § 26 Abs. 1 BDSG die Datenverarbeitung erforderlich ist.

494 Aus diesem Grund einen Regelungsspielraum bejahend BeckOK DatenSR/*Riesenhuber*, Art. 88 DSGVO Rn. 68 f.

495 BT-Drs. 18/11325, S. 98.

496 *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 247; a.A. *Gola*, BB 2017, 1462 (1469), der diesen Umstand offensichtlich verkennt und daher von einer rein klarstellenden Funktion des § 26 Abs. 4 BDSG ausgeht.; ebenso von einer nur klarstellenden Funktion sprechend *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 168.

In Kollektivvereinbarungen sollten aufgrund der Formulierung des Art. 88 Abs. 2 die Auskunftsrechte und Informationspflichten detailliert geregelt werden, sofern hierfür spezifische Systeme zur Verfügung gestellt werden.[497]

Letztlich lässt sich aus Erwägungsgrund 155 auch entnehmen, dass in Kollektivvereinbarungen spezifische Vorschriften über die Bedingungen, unter denen personenbezogene Daten im Beschäftigungskontext auf Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen (analog hat das der deutsche Gesetzgeber mit § 26 Abs. 2 BDSG gesetzlich umgesetzt), zulässig sind.

3. Das grundsätzliche Verbot automatisierter Einzelfallentscheidungen (Art. 22 DSGVO)

Art. 22 Abs. 1 DSGVO bestimmt, wie bereits Art. 15 der DS-RL, dass die betroffene Person das Recht hat, nicht einer ausschließlich auf einer automatisierten Verarbeitung - einschließlich Profiling - beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Bei Art. 22 DSGVO handelt es sich um eine Verfahrensregelung, die die Art der Nutzung des Datenverarbeitungsergebnisses regelt, nicht jedoch die Verarbeitung selbst legitimiert.[498]

Zweck der Vorschrift ist es, „Betroffene nicht zum bloßen Objekt künstlicher Intelligenz zu machen“[499]. Aus diesem Grund handelt es sich nicht primär um eine Datenschutzregelung, sondern eine Regelung zum Schutz der Menschenwürde.[500] In der Literatur wird diese Regelung teilweise kritisiert, da sie die Innovation bremse und lediglich das tiefe Misstrauen in die Technik widerspiegle.[501]

Nach Abs. 2 der Regelung gilt Abs. 1 nicht, wenn die Entscheidung für den Abschluss oder die Erfüllung eines Vertrages erforderlich ist (lit. a),

---

497 Vgl. *Wurzberger*, ZD 2017, 258 (261); Regelungsvorschläge bei *Körner*, NZA 2019, 1389; *Grimm*, ArbRB 2018, 78.

498 *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 477.

499 *Gausling*, PinG 2019, 61 (69); *Arning*, Kapitel 6: Umgang mit Betroffenen, in: Moos/Schefzig/Arning, Die neue Datenschutz-Grundverordnung, Rn. 345.

500 *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, <www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/BSt_DSGVOundADM_dt.pdf>, S. 18, 29.

501 *Zarsky*, Seton Hall Law Review 2017, 995 (1017).

aufgrund von Rechtsvorschriften der Union oder Mitgliedsstaaten zulässig ist (und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie berechtigten Interessen der betroffenen Person enthalten (lit. b) oder mit ausdrücklicher Einwilligung der betroffenen Person erfolgt (lit. c). In den Fällen a) und c) hat der Verantwortliche angemessene Maßnahmen zu treffen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört (Art. 22 Abs. 3 DSGVO). Zuletzt darf dürfen Entscheidungen nach Abs. 2 nicht – bis auf wenige Ausnahmen – auf besonderen Kategorien personenbezogener Daten („sensitive Daten")[502] beruhen.

Konkretisiert wird Art. 22 DSGVO durch Erwägungsgrund 71, wonach die betroffene Person ein Recht haben soll, keiner Entscheidung – was eine Maßnahme einschließen kann – zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Als Beispiele werden dort die Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen genannt.

Gerade im Arbeitsrecht ist die Eingriffsintensität besonders hoch, weil Beschäftigte und Bewerber eine geringere Entscheidungsfreiheit besitzen als in anderen Situationen: Sie können sich solchen Maßnahmen nicht ohne weiteres entziehen, wie beispielsweise in anderen Fällen im Rahmen der Ausübung der Privatautonomie. Bei einem (alltäglichen) Vertragsschluss können sich Betroffene in aller Regel für ein anderes Unternehmen entscheiden, wenn sie einer automatisierten Einzelfallentscheidung nicht zustimmen.[503]

Obwohl die Vorschrift mit jener der DS-RL nahezu inhaltsgleich ist[504] und lediglich in Erwägungsgrund 71 weitere Konkretisierungen erfährt, ist Streit entstanden, beispielsweise darüber, ob die Vorschrift ein subjektives

502 Art. 9 Abs. 1 DSGVO.
503 WHWS/*Broy/Heinson*, B. II. Die automatisierte Einzelfallentscheidung im Beschäftigungsverhältnis, Rn. 21.
504 EuArbRK/*Franzen*, Art. 22 DSGVO Rn. 1.

Recht[505] oder ein gesetzliches Verbot mit Erlaubnisvorbehalt statuiert[506] sowie wie der Einschub „einschließlich Profiling" zu beurteilen ist.

a) Gesetzliches Verbot mit Erlaubnisvorbehalt

Franzen ist der Ansicht, dass Art. 22 kein gesetzliches Verbot statuiere, sondern der betroffenen Person das subjektive Recht gebe, nicht einer solchen Entscheidung unterworfen zu sein und sie deshalb einen Unterlassungsanspruch gegen den für die Datenverarbeitung Verantwortlichen habe, sofern die Voraussetzungen des Abs. 1 vorliegen und kein Erlaubnistatbestand nach Abs. 2 eingreife.[507] Dies hätte zur Folge, dass der Verarbeiter die Daten grundsätzlich in dieser Form verarbeiten könnte, solange der Betroffene sein Recht aus Art. 22 Abs. 1 DSGVO nicht ausübt; die Verarbeitung per se also zulässig wäre.

Die überwiegende Ansicht[508] geht hingegen von einem grundsätzlichen Verbot aus. *Martini* kritisiert zwar, dass Art. 22 systematisch als Betroffenenrecht ausgestaltet sei und Missverständnisse über seinen Reglungsgehalt erzeuge. Letztlich stellt er aber fest, dass es sich um ein Verbot handle, das nicht von einer Geltendmachung im Einzelfall abhängt.[509] *Deuster* begründet das Verbot damit, dass im Parlamentsentwurf in Art. 20 Abs. 1 und Erwägungsgrund 58 dem Betroffenen lediglich ein Widerspruchsrecht zugestanden hätte, in Abkehr von diesem nunmehr jedoch eine andere Regelungstechnik, die auf ein absolutes Verbot mit Ausnahmefällen hindeutet, Eingang in die DSGVO gefunden hat, die dem deutschen Verständnis aus dem BDSG a.F. entspricht.[510]

505 Vgl. bereits die Nachweise unter Fn. 21
506 Vgl. bereits die Nachweise unter Fn. 20.
507 EuArbRK/*Franzen*, Art. 22 DSGVO Rn. 3.
508 *Eichler*, RDV 2017, 10 (11); *Taeger*, RDV 2017, 3; wohl auch *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 78 Rn. 61; *Sörup/Marquardt*, ArbRAktuell 2016, 103 (106); Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 29b; Sydow/*Helfrich*, Art. 22 DSGVO Rn. 39 f.; *Deuster*, PinG 2016, 75 (77); *Eckhardt*, § 16. Automatisierte Entscheidungsfindung einschließlich Profiling, in: Rüpke/von Lewinski/Eckhardt, Datenschutzrecht, S. 238 Rn. 44; *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 477; *Gausling*, PinG 2019, 61 (70); *Arning*, Kapitel 6: Umgang mit Betroffenen, in: Moos/Schefzig/Arning, Die neue Datenschutz-Grundverordnung, Rn. 344: Betroffenenrecht, das faktisch als Verbotsnorm wirkt.; *Götz*, Big Data im Personalmanagement, S. 156 f.
509 Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 1, 29a f.
510 *Deuster*, PinG 2016, 75 (77).

Die herrschende Auffassung verdient den Vorzug: Das Ziel des Verbots ist es, Entscheidungen persönlich zu verantworten und nicht Computerprogrammen oder Algorithmen zu überlassen und somit zu vermeiden, dass der Betroffene lediglich aufgrund seines Persönlichkeitsprofils Objekt einer Datenverarbeitung wird.[511] So war bereits bei der Schaffung von Art. 15 der DS-RL die Gefahr der missbräuchlichen Anwendung von Computersystemen und deren nachteilige Folgen für die Betroffenen Teil der Überlegungen der *Kommission*: *„Die Gefahr einer missbräuchlichen Verwendung der Informatik bei der Entscheidungsfindung ist eine der Hauptgefahren der Zukunft: Das von der Maschine gelieferte Ergebnis, die immer höher entwickelte Software und Expertensystemen zugrunde liegt, hat einen scheinbar objektiven und unbestreitbaren Charakter, dem der menschliche Entscheidungsträger übermäßige Bedeutung beimessen kann, wenn er seiner Verantwortung nicht nachkommt.*“[512]

Fasste man Art. 22 DSGVO so auf, dass es nur noch ein subjektives Recht des Betroffenen ist, welches er zunächst geltend machen müsste, änderte dies nichts daran, dass er zunächst von einem Computer bewertet würde und – das ist bedeutend – bereits eine für ihn nachteilige Entscheidung getroffen wurde, die die Entscheidungsträger möglicherweise nicht mehr voreingenommen entscheiden lässt sowie den Betroffenen zu einer (Widerspruchs-)Handlung zwingt. Sofern lediglich eine Bewertung vorgenommen wird, aber noch keine Entscheidung, so muss ein menschlicher Entscheider eine für den Betroffenen negative Entscheidung selbst treffen und verantworten. Die emotionalen Hürden sind somit vielfach höher als eine bereits getroffene Entscheidung zu verteidigen. Zudem schrecken viele Betroffene davor zurück, sich gegen negative Maßnahmen zu wehren und ihre Rechte geltend zu machen. Insbesondere im Beschäftigungsbereich, wo eine persönliche und finanzielle Abhängigkeit besteht, entsteht hierdurch oftmals die (vielfach berechtigte) Angst, hierdurch anderen Repressalien ausgesetzt zu werden.

Ferner spricht für herrschende Auffassung auch die Möglichkeit der ausdrücklichen Einwilligung nach Abs. 2 lit. c; bei einem subjektiven Recht wäre diese Legitimationsgrundlage überflüssig: Nach Art. 7 Abs. 3 DSGVO hat die betroffene Person die Möglichkeit, ihre Einwilligung jederzeit zu widerrufen. Wenn eine automatisierte Entscheidung im Einzelfall bereits

511 *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 478.

512 Begründung der Kommission zu Art. 16 Abs. 1 des Geänderten Vorschlags der Kommission, ABl. EG Nr. C 311 v. 27.11.1992, S. 26 (zit. nach *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 15 Fn. 1).

ohne Einwilligung zulässig wäre, dann wäre die Geltendmachung des Rechts ebenfalls als Widerruf der Einwilligung auszulegen; Art. 22 Abs. 2 lit. c DSGVO hätte damit keine eigenständige rechtliche Bedeutung mehr.

Hinzu kommt letztlich, dass bei automatischen Entscheidungen die Betroffenen zunächst davon Kenntnis erlangen müssen. Zwar ist der Verarbeiter grundsätzlich nach Art. 12 Abs. 2 lit. f und Art. 13 Abs. 2 lit. g DSGVO zur Information darüber verpflichtet. Dennoch werden Datenschutzerklärungen vielfach nicht gelesen; Betroffene wissen daher mitunter überhaupt nicht über die Möglichkeit der Geltendmachung ihrer subjektiven Rechte. Problematischer wird dies, wenn der Verarbeiter datenschutzwidrig eine solche Entscheidung „heimlich" oder unbewusst durchführt, da der menschliche „Entscheider" nicht die ausreichenden Befugnisse hat, dem Computervorschlag zu widersprechen (dazu sogleich).

b) Kein Verbot von Profiling durch Art. 22 DSGVO

Strittig ist, ob Art. 22 DSGVO aufgrund des Einschubs „einschließlich Profiling" im Normtext auch den Vorgang des Profilings verbietet oder lediglich ausschließlich darauf basierende Entscheidungen.

Der Begriff des Profilings ist in Art. 4 Nr. 4 DSGVO bestimmt. „Profiling" ist demnach jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

Erwägungsgrund 71 bestimmt, dass zu einer derartigen Verarbeitung (nach Art. 22 DSGVO) auch das „Profiling" zählt, das in jeglicher Form automatisierter Verarbeitung personenbezogener Daten unter Bewertung der persönlichen Aspekte in Bezug auf eine natürliche Person besteht, insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person, soweit dies rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Zur Vorgängerregelung führte die *Kommission* aus, dass die strikte Anwendung der von dem System erzielten Ergebnisse durch den Benutzer verboten sei, da die Informatik nicht die einzige Grundlage für eine Entscheidung sein dürfe, sondern Raum für menschliche Beurteilung vorhan-

den sein müsse.[513] Hierzu im Widerspruch stünde beispielsweise, wenn ein Arbeitgeber die Bewerbung eines Arbeitsuchenden lediglich aufgrund der Ergebnisse eines psychotechnischen Computertests ablehnen oder Listen über derartige Beurteilungssoftware produzieren würde, bei der Noten zugewiesen und die Bewerber in einer bestimmten Reihenfolge auf der Grundlage ihres Persönlichkeitstests eingeordnet werden.[514]

Obwohl die Begründung der *Kommission* darauf schließen lässt, dass bereits ein Profiling nach der Altregelung verboten war, griff die Regelung nicht, wenn keine automatisierte Einzelfallentscheidung vorlag und die Einstellung eines Bewerbers durch einen Menschen getroffen wurde, m.a.W. die Maschine nur behilflich war, die menschliche Entscheidung vorzubereiten.[515]

Teilweise wird (vor allem in der vergleichsweise älteren Literatur zur DSGVO) vertreten, dass Art. 22 Abs. 1 DSGVO weit zu verstehen sei und deshalb nicht zwingend eine automatisierte Entscheidung vorliegen müsse, sondern schon das Bilden eines Wahrscheinlichkeitswerts bzw. eines Profils unter Art. 22 DSGVO zu fassen sei.[516] Für diese Sichtweise spräche die Begründung der *Kommission* zu Art. 15 DS-RL. Nach Auffassung von *Härting* sind bereits „rechtliche Wirkungen" oder jedenfalls „erhebliche Beeinträchtigungen" anzunehmen, wenn jemandem ein Vertragsschluss mit dem Betroffenen aufgrund eines Profilings verweigert wird, z.B. ein negativer Score maßgeblich die Entscheidung beeinflusst.[517] *Deuster* begründet ihre Auffassung mit der weiten Formulierung des Erwägungsgrunds 71 (vormals 58).[518] Eine weitere Auffassung spricht sich dafür aus, Art. 22 DSGVO nach dem Verständnis von Art. 15 DS-RL zu verstehen und den Regelungsgegenstand auf die „Bewertung persönlicher Merkmale" zu fixieren. [519]

---

513 So ferner die Kommission, vgl. *Dammann*, in: Dammann/Simitis, EG-Datenschutzrichtlinie, Art. 15 Vor Rn. 1.

514 Vgl. *Dammann*, in: Dammann/Simitis, EG-Datenschutzrichtlinie, Art. 15 Vor Rn. 1.

515 *Dammann*, in: Dammann/Simitis, EG-Datenschutzrichtlinie, Art. 15 Rn. 3.

516 *Härting*, DSGVO, Rn. 607, 610, 617; *Härting*, ITRB 2016, 209 (211); *Härting*, Internetrecht, S. 290; wohl ebenso *Piltz*, K&R 2016, 629 (635 f.); *Deuster*, PinG 2016, 75 (77); EuArbRK/*Franzen*, Art. 22 DSGVO Rn. 2.

517 *Härting*, DSGVO, Rn. 617.

518 *Deuster*, PinG 2016, 75 (77).

519 *von Lewinski/Barros Fritz/Biermeier*, Bevorstehende und künftige Regelungen des Einssatzes von Alogrithmen im HR-Bereich, <*algorithmwatch.org/de/rechtsgutachten-von-lewinski/*>, S. 26.

Die überwiegende Auffassung fasst das Profiling selbst, ohne dass hierdurch bereits eine automatisierte Entscheidung gefällt wird, noch nicht unter Art. 22 Abs. 1 DSGVO, sondern verlangt vielmehr, dass auch tatsächlich alle Merkmale einer „automatisierten Entscheidung im Einzelfall" erfüllt sind.[520]

Eckhardt begründet dies damit, dass die Gegenauffassung im Wortlaut der Norm keine Stütze finde und ebenso wenig der Schutzzweck eine Anwendung auf die bloße Profilbildung erfordere. Schließlich spreche auch Erwägungsgrund 71 dafür, da hierin ausdrücklich angesprochen werde, dass Art. 22 DSGVO das Profiling nur *insoweit* erfasst, als dieses eine rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.[521]

Taeger führt hierzu aus, dass allein durch die Berechnung eines Wahrscheinlichkeitswerts „noch niemand einer Entscheidung unterworfen wird" und ferner, dass die EU-Gesetzgeber für „Profiling" noch keine eigenständige Rechtsgrundlage beschließen wollten.[522]

Auch *Veil* verdeutlicht, dass das Profiling im Sinne von Art. 4 Nr. 4 und Entscheidungen im Sinne von Art. 22 Abs. 1 DSGVO zu unterscheiden sind und das Profiling nicht gleichbedeutend mit einer automatisierten Entscheidung ist. Profiling ist auf Seite der Datenanalyse anzusiedeln. Art. 22 Abs. 1 DSGVO würde auch ohne den Zusatz „einschließlich Profiling" auskommen. Erwägungsgrund 71 S. 1 stelle klar, dass Profiling

---

520 *Eckhardt*, § 16. Automatisierte Entscheidungsfindung einschließlich Profiling, in: Rüpke/von Lewinski/Eckhardt, Datenschutzrecht, Rn. 14; *Taeger*, RDV 2017, 3 (6); Plath/*Kamlah*, Art. 22 DSGVO Rn. 1a; *Kühling et al.*, Die Datenschutz-Grundverordnung und das nationale Recht, S. 441 f.; *Veil*, in: Gierschmann et al., Kommentar Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 52 ff.; Auernhammer/*Herbst*, Art. 22 DSGVO Rn. 12; *Roßnagel/Richter/Nebel*, ZD 2013, 103 (108), die allerdings Kritik an dem Umstand ausüben, dass das reine Profiling nicht von der Vorschrift erfasst ist; *Laue/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis, § 2 Rn. 83 f.; *Müller*, § 8 V. Auskunfteien, Bonitätsauskünfte, Scoring, in: Roßnagel, Das neue Datenschutzrecht, § 8 V Rn. 241; *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 4 Nr. 4 DSGVO Rn. 1; *DSK*, Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO, <www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/12/20191209_Erfahrungsbericht-zur-Anwendung-der-DS-GVO.pdf>, S. 24, jedoch mit der Empfehlung das generelle Verbot aus Art. 22 DSGVO auch auf die Profilbildung auszuweiten; *Rudkowski*, NZA 2019, 72 (75).

521 *Eckhardt*, § 16. Automatisierte Entscheidungsfindung einschließlich Profiling, in: Rüpke/von Lewinski/Eckhardt, Datenschutzrecht, Rn. 15.

522 *Taeger*, RDV 2017, 3 (6).

den Vorschriften der DSGVO unterliegt und daher für das Profiling dieselben Vorschriften gelten wie für jede andere Form der Verarbeitung. Die Erwähnung habe daher lediglich politische Signalwirkung. Für die Anwendbarkeit des Art. 22 Abs. 1 DSGVO bedürfe es jedoch weiterhin einer automatisierten Entscheidung aufgrund des durchgeführten Profilings.[523]

Einfacher wird das Verständnis der Vorschrift, wenn man die Entstehungsgeschichte näher betrachtet (siehe **Anhang I** für den Normtext): Während die ursprüngliche Kommissionsfassung der Vorschrift nahezu wortgleich mit Art. 15 Abs. 1 der Datenschutzrichtlinie war, legte das Europäische Parlament einen Schwerpunkt auf das Profiling, führte die Norm jedoch im Grundsatz als Widerspruchsrecht statt als Verbot aus, verbunden mit einer ausdrücklichen Hinweispflicht auf dieses Recht. Lediglich ein Profiling, das Maßnahmen zur Folge hat, durch die sich rechtliche Konsequenzen für die betroffene Person ergeben, oder das ähnlich erhebliche Auswirkungen auf die Interessen, Rechte oder Freiheiten der betroffenen Person hat, war grundsätzlich verboten und nur unter den weiteren Voraussetzungen des Absatz 2 (Einwilligung, Erforderlichkeit, Erlaubnisnorm) zulässig.

Die endgültige Fassung berücksichtigt nur noch die Entscheidung, die ausschließlich auf einer automatisierten Verarbeitung einschließlich Profiling basiert. Hieraus wird deutlich, dass die Intention des Gesetzgebers war, das Profiling an sich nicht zu verbieten, sondern lediglich Entscheidungen die ausschließlich auf einem Profiling beruhen.

Dies bekräftigt auch Art. 21 DSGVO, der in Abs. 1 S. 1 das Widerspruchsrecht für Profiling, welches in der Fassung des Europäischen Parlaments in Art. 20 Abs. 1 DSGVO-E vorgesehen war, statuiert. Das Widerspruchsrecht ist nunmehr beschränkt auf Profilingmaßnahmen, die sich auf Art. 6 Abs. 1 lit. e und f DSGVO stützen.

Zum selben Ergebnis führt ein Vergleich mit Art. 35 Abs. 3 lit. a DSGVO. Nach dieser Vorschrift ist eine Datenschutzfolgenabschätzung erforderlich, wenn eine „*systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen*" erfolgt, die u.a. auf Profiling gründet und die ihrerseits als „*Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen.*" Eine Datenschutzfolgenabschätzung ist demnach bereits erforderlich, wenn Profiling als Entscheidungsgrundlage dient; die Voraussetzungen sind geringer als jene des Verbots aus Art. 22 Abs. 1 DSGVO,

523 *Veil*, in: Gierschmann et al., Kommentar Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 52 ff.

wonach eine ausschließlich auf einer automatisierten Entscheidung beruhende Entscheidung vorliegen muss.[524]

Die Erstellung eines Persönlichkeitsprofils ist daher nicht an Art. 22 DSGVO, sondern an allgemeinen Erlaubnistatbeständen wie Art. 6 DSGVO oder im Beschäftigtenkontext § 26 BDSG zu messen. Lediglich ausschließlich automatische Entscheidungen auf Basis eines solchen Profils müssen den strengeren Voraussetzungen des Art. 22 DSGVO genügen.

Entgegen der ursprünglichen Fassung des Europäischen Parlaments ist bei Profilingmaßnahmen keine „persönliche Prüfung", also menschliche Interaktion, erforderlich. Eine solche kann allerdings im Rahmen einer Interessenabwägung bei Art. 6 Abs. 1 lit. f DSGVO zu berücksichtigen sein.

c) Voraussetzungen des Verbots

aa) Ausschließlich auf automatisierter Verarbeitung beruhende Entscheidung

Verboten ist eine automatisierte Entscheidung gemäß Art. 22 Abs. 1 DSGVO, wenn sie ausschließlich auf automatisierter Verarbeitung beruht. Der Empfehlung des Wirtschafts- und Sozialausschusses, das damals noch auf das Profiling bezogene Verbot nicht lediglich auf eine „automatisierte" Datenverarbeitung zu erstrecken,[525] wurde nicht gefolgt. Der Ausschuss hat damals auf die Empfehlung des Ministerkomitees des Europarats Bezug genommen.[526] Nach Ziff. 3.4 der Empfehlung sollte bereits die Sammlung und Verarbeitung von Daten im Kontext von Profiling unter Erlaubnisvorbehalt stehen.

Die Norm soll sicherstellen, dass Entscheidungen grundsätzlich nicht ohne menschliche Interaktion getroffen werden, m.a.W. letztlich eine natürliche Person die Entscheidung trifft und diese zu verantworten hat. Voraussetzung hierfür ist allerdings, dass die entscheidende Person eine „wertende Auswahl" trifft und tatsächlich die Befugnis hat, zu entscheiden.[527]

---

524 A.A. wohl *Veil*, in: Gierschmann et al., Kommentar Datenschutz-Grundverordnung, Art. 4 DSGVO Vor Rn. 1.
525 Vgl. ABl. EU 2012, C 229/95.
526 *Council of Europe*, CM/Rec(2010)13, S. 10.
527 Sydow/*Helfrich*, Art. 22 DSGVO Rn. 43.

Das Verbot ist nicht einschlägig, wenn ein Algorithmus lediglich Vorschläge für eine vom Menschen letztlich vorzunehmende Entscheidung bereitstellt,[528] etwa in Form eines „Rankings" von Bewerbern.[529] Dies ergibt sich bereits aus dem Wortlaut: Aus dem Terminus „Entscheidung" geht hervor, dass ein „aus mindestens zwei Varianten auswählender, gestaltender Akt mit einer in gewisser Weise abschließenden Wirkung"[530] vorliegen muss. Computergestützte Entscheidungen, in denen Algorithmen nur in der Entscheidungsvorbereitung wirken, bleiben daher (weiterhin) erlaubt.[531]

Ebenfalls vom Verbot nicht erfasst sind Vorgänge, bei denen Computer leidglich Vereinbarungen oder Anordnungen der betroffenen Personen durchführen, z.B. bei einer Abhebung am Geldautomaten oder bei der Auszahlung monatlicher Bezüge im Rahmen des Arbeitsverhältnisses, die zuvor zwischen den Parteien vereinbart wurden.[532]

Eine wertende Auswahl wird vom Entscheider allerdings nur dann vorgenommen, wenn er nicht ohne weitere Überlegungen den Vorschlag des Computers übernimmt,[533] sondern unter Berücksichtigung der Datengrundlage eine eigene Wertung vornimmt und auf Basis dieser entscheidet.[534] Andernfalls würde die Norm letztlich ins Leere laufen.[535] Bei einem gut funktionierenden Algorithmus wird die Entscheidung des Menschen in aller Regel dem Computervorschlag entsprechen, was die Gefahr schafft, dass nach mehrmaligem Entsprechen des Vorschlags mit

528 Ehmann/Selmayr/*Hladjk*, Art. 22 DSGVO Rn. 6.

529 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 13.

530 *Abel*, ZD 2018, 304 (305).

531 *Martini/Nink*, NVwZ-Extra 2017, 1 (3); WHWS/*Broy/Heinson*, B. II. Die automatisierte Einzelfallentscheidung im Beschäftigungsverhältnis, Rn. 27, die aber darauf hinweisen, dass es in der Praxis vielfach untaugliche Konstellationen gibt (z.B. Stichprobenkontrolle).

532 *Klar*, BB 2019, 2243 (2249); *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 19; mit etwas anderer Begründung i.E. ebenso *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 479.

533 Sydow/*Helfrich*, Art. 22 DSGVO Rn. 43; *Martini/Nink*, NVwZ-Extra 2017, 1 (3): "lediglich formale Bearbeitung" nicht ausreichend.; Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 17; unklar *Reibach*, RDV 2018, 198 (200): Dazwischenschalten eines Menschen ausreichend.

534 *Hoeren/Niehoff*, RW 2018, 47 (53); ebenso wohl auch *Block*, 23. Datenschutz- und Informationsfreiheitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, S. 62; zu pauschal daher *Wojak*, DuD 2018, 553 (556), die es ausreichen lässt, dass ein Mensch den Vorschlag akzeptiert.

535 *Hoeren/Niehoff*, RW 2018, 47 (53).

der eigenen Wertung der Vorschlag inhaltlich nicht mehr oder allenfalls stichprobenartig überprüft wird.[536] Dann läge wiederum eine legitimationsbedürftige automatisierte Einzelfallentscheidung vor.[537]

Zu weitgehend wäre es allerdings zu fordern, dass im Falle eines Bewerberprofilings alle Bewerberinnen und Bewerber beispielsweise noch zu einem Vorstellungsgespräch eingeladen werden müssen, um nicht von einer legitimationsbedürftigen Artikel-22-Entscheidung auszugehen,[538] da auch ohne Einsatz eines Profilingsystems nur aussichtsreiche Bewerber zu einem solchen eingeladen würden. Es ist daher grundsätzlich ausreichend, wenn ein menschlicher Entscheider die dem Profil zugrundeliegenden Daten überprüft (z.B. Anschreiben, Lebenslauf und Zeugnisse) und auf dieser Basis entscheidet, damit es sich nicht um eine automatisierte Einzelfallentscheidung handelt. Es ist nicht ersichtlich, weshalb im Falle eines unterstützenden Profilings strengere Vorschriften gelten sollten.

Ebenfalls nicht erfasst sein soll nach einer verbreiteten Auffassung in der Literatur die bloße Vorauswahl bzw. bloße Vorentscheidungen dergestalt, dass Personen aussortiert werden, die der Mindestqualifikation o.ä. nicht entsprechen.[539] Hier handle es sich um eine einfache Wenn-Dann-Entscheidungen, die „als bloßer Automatismus" nicht vom Anwendungsbereich des Art. 22 DSGVO erfasst seien.[540] Während des Gesetzgebungsverfahrens sei die aus der Verhaltensanalyse berechnete Prognose künftigen Verhaltens im Fokus gestanden, über das jedoch im Trilog keine Einigkeit erzielt werden konnte, weshalb man sich an der Formulierung des Art. 15 DS-RL orientiert habe.[541] Im Übrigen hätte das Verbot solch schlichter Entscheidungen nichts mit dem Schutzzweck des Art. 22 DSGVO, dem Schutz des Persönlichkeitsrechts von Betroffenen, zu tun.[542] *Schulz* ist da-

536 Diese Gefahr sehen auch WHWS/*Broy/Heinson*, B. II. Die automatisierte Einzelfallentscheidung im Beschäftigungsverhältnis, Rn. 27.

537 *Arning*, Kapitel 6: Umgang mit Betroffenen, in: Moos/Schefzig/Arning, Die neue Datenschutz-Grundverordnung, Rn. 347 m.w.N.

538 So aber *Block*, 23. Datenschutz- und Informationsfreiheitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, S. 62; *Gola*, RDV 2018, 24 (27).

539 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 14; *Abel*, ZD 2018, 304 (305 f.); *Hamann*, Kapitel 6: Datenschutzrecht, in: Arnold/Günther, Arbeitsrecht 4.0, Rn. 43.

540 Der Algorithmus treffe insofern keine inhaltliche Entscheidung, vgl. *Hamann*, Kapitel 6: Datenschutzrecht, in: Arnold/Günther, Arbeitsrecht 4.0, Rn. 43.

541 *Abel*, ZD 2018, 304 (305 f.).

542 *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 22 DSGVO Rn. 18; *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 22

her der Ansicht, dass eine teleologische Reduktion geboten sei, wonach nur noch dem Profiling vergleichbare Sachverhalte erfasst sein sollen, die ein „Mindestmaß an Komplexität" aufweisen.[543]

Diese Sichtweise überzeugt nicht: Zum einen findet sie keine Stütze im Wortlaut.[544] Zum anderen könnte sich dann das Verbot – wie ursprünglich vorgeschlagen – lediglich auf das Profiling beschränken.[545] Art. 22 DSGVO soll aber Betroffene gerade davor schützen, dass sie zum Objekt einer Computerentscheidung werden. Diese Gefahr besteht unabhängig einer etwaigen Komplexität der Ausgangsdaten und Entscheidungsparameter. Auch bei einfachen Wenn-Dann-Entscheidungen besteht das Risiko, dass die vom Computer als Grundlage der Entscheidung herangezogenen Daten sich als falsch erweisen.

Für diese Fälle sieht Art. 22 Abs. 3 DSGVO das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen sowie auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung vor. Fasste man beispielsweise die Ablehnung eines Bewerbers im Rahmen einer Vorauswahl aufgrund vermeintlich mangelnder Qualifikation nicht unter Art. 22 DSGVO, so hätte dieser Bewerber keinen Anspruch auf eine menschliche Intervention und müsste sich mit der offensichtlich fehlerhaften Computerentscheidung abfinden („*Der Computer sagt: Nein!*"[546]).[547] Zwar hätte der betroffene Bewerber auch keinen Anspruch, wenn ein Mensch denselben Fehler machen würde; in diesem Fall bestünde das technikspezifische Risiko allerdings nicht, vor dem Art. 22 DSGVO schützen möchte und das u.a. Grundlage für das heutige Datenschutzrecht ist: Das Datenschutzrecht schützt grundsätzlich nicht vor (negativen) (Fehl-)entscheidungen, sondern davor, bloßes Objekt einer (fehlerhaften) automatisierten Verarbeitung zu sein. Letztlich besteht auch nach Aus-

---

DSGVO Rn. 20; BeckOK DatenSR/*von Lewinski*, Art. 22 DSGVO Rn. 13 bezeichnet dies als "wenig sachgerecht".

543 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 20; so wohl i.E. auch *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 22 DSGVO Rn. 21.

544 So wohl auch *Dammann*, ZD 2016, 307 (312 f.); *Veil*, in: Gierschmann et al., Kommentar Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 51.

545 *Arning*, Kapitel 6: Umgang mit Betroffenen, in: Moos/Schefzig/Arning, Die neue Datenschutz-Grundverordnung, Rn. 348 sowie Fn. 333.

546 Allgemeine Bekanntheit hat dieser Satz über Soziale Medien durch die britische Comedy-Serie „*Little Britain*" erlangt; vgl. hierzu auch *Martini*, JZ 2017, 1017 (1020 f.).

547 Ähnlich *Schantz*, D. V. Verbot automatisierter Einzelfallentscheidungen und Profiling, in: Schantz/Wolff, Das neue Datenschutzrecht, Rn. 729.

übung des Widerspruchsrechts aus Art. 22 Abs. 3 DSGVO kein Anspruch auf Durchführung der gewünschten Entscheidung.

Anders ist dies in den Fällen der Durchführung von Verträgen, wie beispielsweise im Bereich der Zutrittskontrolle, der Geldabhebung am Geldautomaten, Genehmigungen von Kreditkartenverfügungen o.ä.[548]. Hier besteht das Recht auf Leistung und im Falle der Nichterbringung jedenfalls auf menschliche Interaktion aus dem zugrundeliegenden Vertragsverhältnis.

Diese Sichtweise führt auch nicht zu einer unzumutbaren Belastung für den Verarbeiter, da trotz Vorliegen einer automatisierten Einzelfallentscheidung in einfachsten Fällen der Erforderlichkeit (Art. 22 Abs. 2 lit. a DSGVO) keine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO vorzunehmen ist. Dies ergibt sich aus der Formulierung des Art. 35 Abs. 3 lit. a DSGVO, der auf eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen abstellt und nicht – wie in der Literatur teilweise ungenau geschlussfolgert[549] – auf das Vorliegen einer automatisierten Einzelfallentscheidung nach Art. 22 DSGVO.

bb) Rechtliche Wirkung oder ähnlich erhebliche Beeinträchtigung

Art. 22 DSGVO bietet nur vor automatisierten Entscheidungen einen Schutz, die gegenüber der betroffenen Person eine rechtliche Wirkung entfalten oder diese in ähnlicher Weise erheblich beeinträchtigen.[550] Für den genannten Fall der Verweigerung des Zutritts stellt sich daher bereits die Frage, ob dieser überhaupt vom Verbot des Art. 22 DSGVO erfasst ist. Gleiches ist für die abgelehnte Bargeldabhebung am Geldautomaten zu überprüfen. Da eine rechtliche Wirkung nicht gegeben ist (dem Betroffenen wird sein Anspruch nicht genommen, er wird lediglich nicht [sofort] erfüllt), hängt die Entscheidung von der Auslegung des Tatbestandsmerkmals „ähnlich erhebliche Beeinträchtigung“ ab.

548 Beispiele aus BeckOK DatenSR/*von Lewinski*, Art. 22 DSGVO Rn. 13.
549 *Abel*, ZD 2018, 304 (305); ebenso wohl *Hoeren/Niehoff*, RW 2018, 47 (65).
550 *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 22 DSGVO Rn. 23.

(1) Rechtliche Wirkung

Die Entscheidung muss eine rechtliche Wirkung entfalten, wobei es nach dem Wortlaut nicht darauf ankommt, ob diese Wirkung negativ, neutral oder positiv für den Betroffenen ist. Teilweise wird dieses Ergebnis in der Literatur so hingenommen,[551] überwiegend aber aufgrund der weiteren Formulierung „ähnlich erhebliche Beeinträchtigung" davon ausgegangen, dass der Gesetzgeber nur rechtlich nachteilige Entscheidungen erfassen wollte.[552]

Ein Argument dafür, dass die Rechtsfolge nicht nachteilig sein muss, ist der Vergleich mit dem Wortlaut des Art. 11 JI-RL[553], wo explizit von einer „nachteilige[n] Rechtfolge für die betroffene Person" gesprochen wird im Zusammenhang mit einer automatisierter Entscheidungsfindung im Einzelfall. Kritisiert wird jedoch gleichzeitig, dass der Gesetzgeber offensichtlich nur nachteilige Entscheidungen[554] im Blick hatte.

Andererseits sprechen neben bereits aufgeführten systematischen Argumenten auch teleologische dafür, automatisierte Einzelfallentscheidungen zugunsten des Betroffenen nicht vom Verbot des Art. 22 zu erfassen: Letztlich soll die Menschenwürde geschützt werden und der Betroffene davor geschützt werden, lediglich Objekt einer Computerberechnung zu sein. Dieses Schutzes bedarf der Betroffene aber gerade dann nicht, wenn

551 Sydow/*Helfrich*, Art. 22 DSGVO Rn. 48; Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 26; *Weichert*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, Art. 22 DSGVO Rn. 27.

552 *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 22 DSGVO Rn. 25; *Veil*, in: Gierschmann et al., Kommentar Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 69 ff.; so auch der Bundesrat in seiner Stellungnahme zu § 37 BDSG n.F., vgl. BT-Drs. 18/11325, S. 24; Plath/*Kamlah*, Art. 22 DSGVO 7e; *Piltz*, K&R 2016, 629 (636); *Paschke/Scheurer*, in: Gola/Heckmann, BDSG, § 37 BDSG Rn. 5; *Schantz*, D. V. Verbot automatisierter Einzelfallentscheidungen und Profiling, in: Schantz/Wolff, Das neue Datenschutzrecht, Rn. 737, 742; *Arning*, Kapitel 6: Umgang mit Betroffenen, in: Moos/Schefzig/Arning, Die neue Datenschutz-Grundverordnung, Rn. 355; BeckOK DatenSR/*von Lewinski*, Art. 22 DSGVO Rn. 33.

553 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2088/977/JI des Rates.

554 BeckOK DatenSR/*von Lewinski*, Art. 22 DSGVO Rn. 33.

er lediglich einen rechtlichen Vorteil erlangt.[555] Das von der Literatur teilweise aufgezeigte Problem, dass der Betroffene dann auch bei nur teilweise stattgebenden Entscheidungen keine Möglichkeit zur Intervention hätte,[556] ist rein fiktiv: Jede nur teilweise stattgebende Entscheidung hat auch gleichzeitig eine negative Wirkung, nämlich die Ablehnung des übrigen Begehrens und ist somit von Art. 22 DSGVO erfasst.[557] Nicht unter „rechtliche Wirkung" zu fassen sind grundsätzlich die Verweigerung eines Vertragsschlusses oder das Verwehren bestimmter Konditionen eines Vertrages, da diese aufgrund der Privatautonomie keine Rechtspositionen mangels eines Anspruchs verändern.[558]

Wenn beispielsweise ein Arbeitnehmer eine Gehaltserhöhung von monatlich 500 Euro beantragt, jedoch lediglich 100 Euro erhält, so hat er keine negative rechtliche Wirkung. Sein Antrag erlischt zwar nach § 150 Abs. 2 BGB, dies hat allerdings nur zur Folge, dass er nicht mehr nach § 145 BGB daran gebunden ist und hat somit eine rein vorteilhafte Wirkung für seinen Antrag. Gleiches gilt beispielsweise für die Ablehnung eines Kreditantrags.

Anders ist dies im öffentlichen Recht, wenn ein Verwaltungsakt der (berechtigten) Begehr nur teilweise entspricht. Der Verwaltungsakt ist – mit Ausnahme der Nichtigkeitsfälle – grundsätzlich wirksam (§ 43 Abs. 1 VwVfG) und muss vom Betroffenen zunächst angefochten werden, auch wenn er rechtswidrig ist.

Teilweise wird angeführt, dass etwas anderes bei der Verletzung von Diskriminierungsverboten oder in Fällen des Kontrahierungszwangs gelte.[559] Dies überzeugt nicht: Auch in diesen Fällen verschlechtert sich die Rechtsposition des Betroffenen nicht. Vielmehr verbessert sie sich sogar, indem er möglicherweise Schadensersatzansprüche (z.B. aus § 15 AGG bei einer Diskriminierung erwirbt). Das gleiche gilt, wenn ein Arbeitgeber gegen den arbeitsrechtlichen Gleichbehandlungsgrundsatz verstößt, indem er beispielsweise im Rahmen einer automatisierten Entscheidung

555 *Veil*, in: Gierschmann et al., Kommentar Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 71; *Paschke/Scheurer*, in: Gola/Heckmann, BDSG, § 37 BDSG Rn. 5.

556 Vgl. BeckOK DatenSR/*von Lewinski*, Art. 22 DSGVO Rn. 33.

557 So im Ergebnis auch *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 22; *Arning*, Kapitel 6: Umgang mit Betroffenen, in: Moos/Schefzig/Arning, Die neue Datenschutz-Grundverordnung, Rn. 355.

558 *Abel*, ZD 2018, 304 (306).

559 *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 22 DSGVO Rn. 34; *Martini/Nink*, NVwZ-Extra 2017, 1 (3).

einen Arbeitnehmer willkürlich aus einer Gratifikation ausschließt. Auch hier verändert sich die Rechtsposition durch die automatisierte Entscheidung nicht zum Negativen. Der Arbeitnehmer erwirbt hierdurch einen Anspruch gegen den Arbeitgeber auf Gleichbehandlung.[560] Dem steht selbstverständlich nicht entgegen, dass es sich in diesen Fällen um eine erhebliche Beeinträchtigung handeln kann, die ebenfalls vom Verbot erfasst ist.

Aufgrund seines einseitigen Leistungsbestimmungsrechts nach § 315 BGB hat die Ausübung des Direktionsrechts durch einen Arbeitgeber eine rechtliche Wirkung; leistet der Beschäftigte bei berechtigter Weisung keine Folge, stellt dies eine Pflichtverletzung dar.[561]

(2) Ähnlich erhebliche Beeinträchtigung

Wie bereits angedeutet, sind auch automatisierte Entscheidungen, die erhebliche Beeinträchtigungen beim Betroffenen hervorrufen, wie beispielsweise im Falle der Ablehnung eines Online-Kreditantrages oder im Rahmen eines Online-Bewerbungsverfahrens, vom Verbot erfasst.[562] Es muss demnach eine nachhaltige Störung der „wirtschaftlichen oder persönlichen Entfaltung" vorliegen.[563] Grundlage der Bewertung sind bei objektiver Betrachtung die Umstände des Einzelfalls,[564] da Entscheidungen – je nach Betroffenem und seiner subjektiven Lage – sehr unterschiedliche Wirkungen haben können.[565] So kann beispielsweise die Ablehnung eines Online-Kreditantrages für eine Person überhaupt keine negative Auswirkung haben, wenn diese Person sehr vermögend ist und den Kreditantrag lediglich als „Selbstversuch" gestellt hat, während die andere Person das „Kreditgeld" dringend benötigt, um finanziellen Verpflichtungen nachkommen zu können. Hierbei kommt es nicht auf das subjektive Empfin-

560 Allgemein zum arbeitsrechtlichen Gleichbehandlungsgrundsatz, ErfK/*Preis*, § 611a BGB Rn. 574 ff.

561 WHWS/*Broy/Heinson*, B. II. Die automatisierte Einzelfallentscheidung im Beschäftigungsverhältnis, Rn. 29.

562 Siehe hierzu auch Erwägungsgrund 71.

563 *Abel*, ZD 2018, 304 (306); Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 27; *Arning*, Kapitel 6: Umgang mit Betroffenen, in: Moos/Schefzig/Arning, Die neue Datenschutz-Grundverordnung, Rn. 356; zustimmend Sydow/*Helfrich*, Art. 22 DSGVO Rn. 51.

564 Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 28.

565 Sydow/*Helfrich*, Art. 22 DSGVO Rn. 51.

den des Empfängers an, sondern auf eine objektive Betrachtung aus der Sichtweise eines „Durchschnittsmenschen".[566]

Aus dem Zusatz *erhebliche* (Beeinträchtigung) ergibt sich, dass die Störung über eine reine Belästigung hinausgehen muss.[567] In aller Regel stellt die Nichtbegründung eines Vertragsverhältnisses eine solche erhebliche Benachteiligung dar.[568] Gleiches muss dann auch für eine teilweise Ablehnung eines Antrags (z.B. Kreditsumme nur 10.000 Euro statt 100.000 Euro) oder Annahme zu verschlechterten Konditionen (17 % statt 7 % Kreditzins) gelten. Dasselbe gilt selbstverständlich auch für Diskriminierungen, in Fällen des Kontrahierungszwangs oder bei Verstößen gegen den arbeitsrechtlichen Gleichbehandlungsgrundsatz. Zwar erwirbt der Betroffene hierdurch einen „rechtlichen Vorteil" in Form eines Anspruchs, andererseits ist er zunächst durch die Entscheidung beeinträchtigt, indem ihm eine zustehende Rechtsposition oder Gratifikation nicht gewährt wird. Gerade bei Streitigkeiten mit dem Arbeitgeber können starke negative Emotionen zur Folge haben, die deutlich über eine reine Belästigung hinausgehen. Mitunter muss sich der Betroffene mit dem Verarbeiter vor Gericht zunächst um seine Rechtsposition streiten. Da die Kosten eines Rechtsbeistands im ersten Rechtszug eines arbeitsgerichtlichen Verfahrens nach § 12a Abs. 1 S. 1 ArbGG nicht erstattet werden, entstehen mitunter sogar finanzielle Nachteile.

d) Ausnahmen

Das Verbot automatisierter Einzelfallentscheidungen enthält drei Ausnahmen: (a) Erforderlichkeit für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen, (b) Zulässigkeit aufgrund von Rechtsvorschriften der EU oder der Mitgliedstaaten, denen der Verantwortliche unterliegt oder (c) ausdrückliche Einwilligung des Betroffenen in diese Form der Entscheidung.

---

566 *Veil*, in: Gierschmann et al., Kommentar Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 66, 68.

567 *Arning*, Kapitel 6: Umgang mit Betroffenen, in: Moos/Schefzig/Arning, Die neue Datenschutz-Grundverordnung, Rn. 356; *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 22 DSGVO Rn. 35.

568 So auch *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 22 DSGVO Rn. 36; einschränkend BeckOK DatenSR/*von Lewinski*, Art. 22 DSGVO Rn. 39.

Bei jeder Ausnahme wird vorausgesetzt, dass angemessene Maßnahmen zur Wahrung der Rechte und berechtigten Interessen der betroffenen Person getroffen werden: Für die Ausnahme aus lit. b ergibt sich das aus der Ausnahmevorschrift selbst, während für die Ausnahmen der lit. a und c sich dies aus Abs. 3 ergibt. Bei Letzteren konkretisiert die Norm weiter, dass der Betroffene mindestens das Recht auf Erwirkung eines Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts sowie auf Anfechtung der Entscheidung haben muss.

Eine Rückausnahme besteht nach Art. 22 Abs. 4 DSGVO grundsätzlich für besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO wie beispielsweise rassische Herkunft, Gewerkschaftszugehörigkeit, sexuelle Orientierung oder Gesundheitsdaten; diese Daten dürfen nicht Grundlage automatisierter Einzelfallentscheidungen sein.

Art. 70 Abs. 1 S. 2 lit. f DSGVO sieht vor, dass der Europäische Datenschutzausschuss (EDSA) Leitlinien, Empfehlungen und bewährte Verfahren zur näheren Bestimmung der Kriterien und Bedingungen für die auf *Profiling* beruhenden Entscheidungen gemäß Art. 22 Abs. 2 DSGVO vorsieht.[569]

aa) Erforderlichkeit

Das Kriterium der Erforderlichkeit für den Vertragsschluss bzw. die -erfüllung ist wohl der umstrittenste Ausnahmetatbestand von Art. 22 Abs. 2 DSGVO. Hintergrund ist, dass die Vorschrift in den Ratsverhandlungen zwischenzeitlich eine deutlich weitere Formulierung hatte. So sollte es danach schon zulässig sein, wenn die Entscheidung „im Rahmen des Abschlusses oder der Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen vorgenommen" würde.[570] Diese Formulierung ähnelt jener des § 6a Abs. 2 Nr. 1 BDSG, wonach das Verbot nicht galt, wenn „*die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wur-*

569 *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 22 DSGVO Rn. 38 verweist in seiner Kommentierung darauf, dass der EDSA Leitlinien, Empfehlungen und bewährte Verfahren für zulässige *Entscheidungen* nach Abs. 2 zur Verfügung stellen soll und übersieht hierbei, dass der EDSA nur für auf *Profiling* basierende Entscheidungen beauftragt wurde.

570 Vgl. *Veil*, in: Gierschmann et al., Kommentar Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 77.

de“, wobei hier das Merkmal der positiven Entscheidung für den Betroffenen die maßgebliche Einschränkung traf.

Die Ausnahme in Art. 22 Abs. 2 lit. a DSGVO ist somit deutlich restriktiver als die (deutsche) Vorgängernorm. Da die Norm ausdrücklich den Vertragsschluss miteinbezieht, erfasst sie auch automatisierte Entscheidungen, die in Vorbereitung eines Vertrages erfolgen.[571]

Härting schließt daraus, dass die automatisierte Einzelfallentscheidung deshalb objektiv erforderlich sein müsse.[572] Nicht ausreichend sei, wenn es sinnvoll, nützlich oder gar aus praktischer Sicht unerlässlich sei. Aus diesem Grund falle ein Kredit-Scoring nicht unter diese Ausnahme.[573]

Diese Sichtweise überzeugt nicht, denn nach dieser Auffassung hätte die Ausnahme keinen vorstellbaren Anwendungsbereich mehr: In jedem Bereich ist es möglich, einen menschlichen Entscheider einzuschalten, sodass eine automatisierte Einzelfallentscheidung niemals objektiv erforderlich wäre.[574] Überzeugender ist daher eine teleologische Interpretation des Ausnahmetatbestandes,[575] wo berücksichtigt wird, welches Risiko beim Verarbeiter durch die Entscheidung abgedeckt werden soll bzw. welche Vorteile auch für den Betroffenen hierdurch entstehen könnten. Hieraus ergibt sich, dass ein unmittelbarer sachlicher Zusammenhang zwischen der automatisierten Einzelfallentscheidung und dem konkreten Vertragszweck bestehen muss[576] und diese Form der Entscheidung ein geeignetes Mittel zur Erreichung dieses Zwecks ist, ohne dass mildere, gleich wirksame Mittel zur Verfügung stehen.[577] Die Frage ist daher, ob die Entscheidung über den Vertragsschluss oder im Rahmen der Vertragserfüllung auch ohne automatisierte Entscheidungsfindung *genauso gut* (also mit derselben Berücksichtigung und Bewertung aller entscheidungsrelevanten Interessen) hätte

571 *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 22 DSGVO Rn. 39.
572 So im Ergebnis auch *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 22 DSGVO Rn. 43.
573 *Härting*, DSGVO, Rn. 621; ebenso Sydow/*Helfrich*, Art. 22 DSGVO S. 56.
574 So auch *Veil*, in: Gierschmann et al., Kommentar Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 77.
575 *Veil*, in: Gierschmann et al., Kommentar Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 78.
576 Plath/*Kamlah*, Art. 22 DSGVO Rn. 8; *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 22 DSGVO Rn. 30. stellen auf einen unmittelbaren Zusammenhang mit der „Entscheidungs- und Kalkulationsgrundlage“ für ein konkretes Rechtsgeschäft ab.
577 *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 22 DSGVO Rn. 42.

getroffen werden können.[578] Mithin ist eine Wertung[579] vorzunehmen, wobei ein objektiver Maßstab anzulegen ist. Es ist die Frage aufzuwerfen, ob keine datenschutzrechtlich weniger einschneidenden Mittel zur Verfügung stehen.[580]

Von der Ausnahme zur Regel würde die Regelung werden, wenn es auf den subjektiven Maßstab des Verantwortlichen ankäme, denn dieser sieht die automatisierte Entscheidungsfindung in aller Regel als notwendig an, wenn er sie einsetzt.[581]

Weichert vertritt, dass in Fällen, in denen das Vertragsverhältnis von einer komplexen Auswertung eines größeren und für Menschen nicht mehr überschaubaren Datenumfangs („*Big Data*") abhängig gemacht wird, eine Erforderlichkeit nach Art. 22 Abs. 2 lit. a DSGVO angenommen werden kann.[582] Unter Berücksichtigung des Umstands, dass ein menschlicher Entscheider auf Basis der Datengrundlage inhaltlich entscheiden muss, damit es sich um keine automatisierte Einzelfallentscheidung handelt, ist diese Auffassung nachvollziehbar, aber keinesfalls überzeugend.

Diese Auffassung führt den Schutzzweck der Norm völlig ad absurdum. Hiernach würde gelten: Je mehr Daten herangezogen werden, desto eher ist eine automatisierte Entscheidung zulässig. Einerseits steht dem Vertragspartner grundsätzlich offen, welche Daten er als Grundlage für die Entscheidung benötigt und somit als erforderlich erachtet (unter Berücksichtigung der Persönlichkeitsrechte des Betroffenen; im Arbeitsverhältnis unterm Topos „Fragerecht des Arbeitgebers" diskutiert), anderseits läuft diese Auffassung auch dem Grundsatz der Datenminimierung zuwider.

Allerdings lässt sich aus den Gedanken von *Weichert* ein überzeugender Ansatz für die Konkretisierung des Erforderlichkeitsbegriffs herleiten: Nicht wenn das Vertragsverhältnis von einer enormen Datenmenge *abhängig* gemacht wird, sondern der Verantwortliche im Rahmen des Vertragsverhältnisses die Bearbeitung einer enormen Datenmenge zu bewältigen hat, kann eine automatisierte Entscheidung erforderlich sein. Dies trifft insbesondere dann zu, wenn – wie im Falle einer enormen Anzahl an Bewerbungen – der Verarbeiter keine ausreichende personelle Kapazität

578 *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 22 DSGVO Rn. 42.
579 *Blum/Kainer*, PERSONALquarterly 2019, 22 (24); so wohl auch Plath/*Kamlah*, Art. 22 DSGVO Rn. 8.
580 Vgl. *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 22 DSGVO Rn. 42.
581 Für diese Sichtweise wohl Ehmann/Selmayr/*Hladjk*, Art. 22 DSGVO.
582 *Weichert*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, Art. 22 DSGVO Rn. 43.

hat, die Vielzahl zwingend notwendig zu verarbeitenden Daten zu verarbeiten.[583] Der Unterschied zur Auffassung von *Weichert* ist, dass nicht dem Verarbeiter die Entscheidung über die Frage der Notwendigkeit einer automatisierten Verarbeitung durch Erhöhung der benötigten Datenmenge obliegt. Ausschlaggebend ist, ob es dem Verarbeiter zumutbar ist, die Datenflut ohne Zuhilfenahme einer automatisierten Entscheidung zu bewältigen und hierbei die Interessen der Betroffenen hinreichend zu berücksichtigen. Das ist etwa dann nicht der Fall, wenn zur Verminderung einer Bewerberflut nur noch jede zweite, fünfte oder zehnte Bewerbung gesichtet würde.

Die Automatisierung eines Entscheidungsvorgangs ist dann solange und soweit zulässig, bis dem Verantwortlichen die Bearbeitung durch menschliche Entscheider wieder zumutbar ist. Ab diesem Zeitpunkt ist die automatisierte Einzelfallentscheidung bei einer objektiven, wertenden Betrachtung nicht mehr erforderlich und es stehen datenschutzrechtlich weniger einschneidende Maßnahmen zur Verfügung.

Im Hintergrund steht also eine Verhältnismäßigkeitsprüfung, verbunden mit einer Interessenabwägung,[584] wobei insbesondere im Arbeitsverhältnis dem Interesse des Betroffenen, keiner automatischen Einzelfallentscheidung zu unterliegen, aufgrund des intensiveren Eingriffs ein sehr hohes Gewicht beizumessen ist.

bb) Unionale bzw. nationale Öffnungsklausel

Ein weiterer Ausnahmetatbestand vom Verbot der automatisierten Einzelfallentscheidung ist die Öffnungsklausel des Art. 22 Abs. 2 lit. b DSGVO, wonach solche Entscheidungen zulässig sind, wenn diese nach dem Recht der Union oder der Mitgliedstaaten zulässig sind. Anders als bei Art. 88 DSGVO für den nationalen Beschäftigtendatenschutz handelt es sich hierbei um eine echte Öffnungsklausel, die nicht lediglich Spezifizierungen zulässt. Zu beachten ist, dass die Öffnungsklausel sich lediglich auf automatisierte Einzelfallentscheidungen bezieht und nicht auf das Profiling,

583 In diese Richtung auch *Götz*, Big Data im Personalmanagement, S. 167, wenngleich er am Ende der Vorschrift „keine relevanten Verbotsausnahmen für People-Analytics im Personalwesen" zuschreibt.

584 So bereits *Blum/Kainer*, PERSONALquarterly 2019, 22 (24); ebenso WHWS/*Broy/Heinson*, B. II. Die automatisierte Einzelfallentscheidung im Beschäftigungsverhältnis, Rn. 37.

d.h. die Mitgliedsstaaten können im nationalen Recht keine eigenständigen Regelungen zur Profilbildung auf Basis von Art. 22 Abs. 2 lit. b DSGVO schaffen, wie dies der deutsche Gesetzgeber in § 28b BDSG a.F. (nunmehr § 31 BDSG[585]) getan hatte.[586] Nicht überzeugend ist die Ansicht, die Mitgliedsstaaten das Scoring auf Basis von Abs. 2 lit. b mit dem Argument erlaubt, dass Art. 22 den Vorgang der Datenanalyse und Nutzung des Ergebnisses rechtlich einheitlich bewerte.[587] Diese Auffassung übersieht, dass Art. 22 lediglich eine Verfahrensregelung ist und keine Verarbeitungsregelung. Die Zulässigkeit von Scoring-Vorschriften ist am allgemeinen Maßstab der Beurteilung der Rechtmäßigkeit (Art. 6 DSGVO bzw. § 26 Abs. 1 BDSG für Beschäftigungszwecke) zu messen.[588] Auf Art. 22 Abs. 2 lit. b DSGVO werden derzeit im deutschen Recht § 35a VwVfG für automatisierte Verwaltungsakte, § 31a SGB X im Sozialverfahren sowie § 155 Abs. 4 AO für die automatisierte Steuerfestsetzung gestützt, ebenso wie § 37 BDSG für automatisierte Entscheidungen im Rahmen eines Versicherungsvertrags.[589]

Nach Erwägungsgrund 41 der DSGVO bedarf es keines nationalen formellen Gesetzes; ausreichend ist eine demokratisch legitimierte Rechtsvorschrift.[590] Aus diesem Grund stellt die Betriebsvereinbarung keine nationale Öffnungsklausel im Sinne dieser Vorschrift dar. Dennoch dürfen aufgrund von Art. 88 DSVO spezifische Vorschriften für automatisierte Einzelfallentscheidungen geschaffen werden, sofern sie den klar erkennbaren Grundsatz, den Menschen nicht zum Objekt einer maschinellen Entscheidung werden zu lassen, berücksichtigen.[591]

Erforderlich ist, dass die Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie berechtigten Interessen der Betroffenen enthalten. Welche Maßnahmen das sind, ist nicht gesondert

---

585 Zur Vereinbarkeit von § 31 BDSG mit dem Unionsrecht siehe **E. § 1 III. 2. c) bb) (1)**.

586 Plath/*Kamlah*, Art. 22 DSGVO Rn. 9

587 *Weichert*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, Art. 22 DSGVO Rn. 41; wohl auch *Taeger*, ZRP 2016, 72 (74 f.).

588 In diese Richtung *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 110.

589 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 31 f.; *Abel*, ZD 2018, 304.

590 *Weichert*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, Art. 22 DSGVO Rn. 37; Sydow/*Helfrich*, Art. 22 DSGVO Rn. 60.

591 *Walter*, 8.4 Automatisierte Entscheidungsfindung (Art. 22 DSGVO), in: Kaulartz/Ammann/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, Rn. 20.

angegeben. Eine Orientierungshilfe bieten jedoch Art. 22 Abs. 3 DSGVO sowie die Art. 7 ff. EU-GRC.[592]

cc) Ausdrückliche Einwilligung

Anders als im alten Datenschutzrecht unter der Geltung von Art. 15 DS-RL ist es nunmehr explizit möglich, in automatisierte Entscheidungen einzuwilligen.[593] Der Zusatz „ausdrücklich" bedeutet, dass sich die Einwilligung nicht lediglich auf die Datenverarbeitung an sich, sondern explizit auf die besondere Verarbeitung in Form der automatisierten Entscheidung beziehen muss.[594]

Die allgemeinen Anforderungen an eine wirksame Einwilligung (Art. 4 Nr. 11, Art. 7 DSGVO)[595] gelten selbstverständlich auch für die Einwilligung im Rahmen des Art. 22 DSGVO.[596]

Helfrich weist darauf hin, dass im Zusammenhang mit Profiling und vergleichbaren Technologien der Informiertheit des Betroffenen eine besondere Rolle zukomme, sodass der Verantwortliche diesen in einer solchen Weise zu informieren hat, dieser die Tragweite seiner Entscheidung erkennen und abwägen kann.[597] Dies ist jedoch keine Besonderheit der Einwilligung im Rahmen von Art. 22 DSGVO, sondern gilt für jede datenschutzrechtliche Einwilligung (nach Art. 6 Abs. 1 lit. a, Art. 7 DSGVO).

e) Schutzmaßnahmen, Art. 22 Abs. 3 DSGVO

In den (Ausnahme-)Fällen der Zulässigkeit der automatisierten Einzelfallentscheidung aufgrund Erforderlichkeit und ausdrücklicher Einwilligung hat der Verantwortliche angemessene Maßnahmen zu treffen, um die Rechte und Freiheiten sowie berechtigten Interessen der betroffenen Personen zu wahren. Hierzu gehört mindestens das Recht auf Erwirkung

592 Vgl. Auernhammer (5. Aufl. 2017)/*Herbst*, Art. 22 DSGVO Rn. 16.
593 Ehmann/Selmayr/*Hladjk*, Art. 22 DSGVO Rn. 13.
594 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 40; Auernhammer (5. Aufl. 2017)/*Herbst*, Art. 22 DSGVO Rn. 17.
595 Siehe zur Einwilligung allgemein bereits D.§ 1III.2.a)
596 Auernhammer (5. Aufl. 2017)/*Herbst*, Art. 22 DSGVO Rn. 17; dagegen wohl *Neufeld/Glugla*, MuT 2019, 40 (41): Einwilligung in automatisierte Entscheidung bei einem Bewebungsverfahrens zulässig.
597 Sydow/*Helfrich*, Art. 22 DSGVO Rn. 67.

des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung (Art. 22 Abs. 3 S. 2 DSGVO). Ziel ist, einen Grundrechtsschutz durch Verfahren herzustellen.[598] Ein solches Recht auf Eingreifen eines Verantwortlichen besteht in jedem Fall als subjektives Recht und nicht nur in besonders begründeten Einzelfällen, da sonst die Gefahr bestünde, dass der Mensch zum bloßen Objekt einer Computerentscheidung degradiert würde.[599]

Erwägungsgrund 71 („Profiling"[600]) konkretisiert näher, dass neben den bereits genannten Rechten und Freiheiten der Betroffene auch einen Anspruch auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung haben soll (S. 4). Ebenso sollen geeignete mathematische oder statistische Verfahren für das Profiling verwendet werden sowie technische und organisatorische Maßnahmen getroffen werden, mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird (Erwägungsgrund 71 S. 6).

Der zugrundeliegende Algorithmus muss im Rahmen dieser Schutzmaßnahmen jedoch nicht gegenüber dem Betroffenen offengelegt werden; hier stehen schutzwürdige Geheimhaltungsinteressen der Verarbeiter entgegen.[601] Zudem werden die wenigsten Betroffenen mit dem offengelegten Programmcode effektiv ihre Rechte wahrnehmen können, da das Verständnis für die Programmiersprache fehlen wird.[602]

598 Näher hierzu *Martini/Nink*, NVwZ-Extra 2017, 1 (3 f.).

599 A.A. *von Lewinski/Barros Fritz/Biermeier*, Bevorstehende und künftige Regelungen des Einssatzes von Alogrithmen im HR-Bereich, <*algorithmwatch.org/de/rechtsgutachten-von-lewinski/*>, S. 38: Nur bei berechtigten Gründen, da ansonsten das Regel-Ausnahmeverhältnis zwischen Absatz 2 und 3 verkehrt würde.

600 Inoffizielle Beschreibung des Erwägungsgrundes.

601 So auch *von Lewinski/Barros Fritz/Biermeier*, Bevorstehende und künftige Regelungen des Einssatzes von Alogrithmen im HR-Bereich, <*algorithmwatch.org/de/rechtsgutachten-von-lewinski/*>, S. 28.

602 Ähnlich Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 36.

4. Art. 35 DSGVO: Pflicht zur Datenschutzfolgenabschätzung (DPIA[603]) bei Profiling

Statt einer generellen Meldepflicht für Datenverarbeitungen (wie sie das alte Datenschutzrecht vorsah, vgl. Art. 18 DS-RL) schreibt die DSGVO für Datenverarbeitungen, die für den Betroffenen *ein besonders hohes Risiko* für die Rechte und Freiheiten natürlicher Personen zur Folge bergen, eine Datenschutz-Folgenabschätzung vor (Art. 35 DSGVO).[604] Art. 35 Abs. 1 DSGVO sieht eine solche insbesondere für den Fall der Verwendung neuer Technologien vor. Diese Form der Risikoanalyse wird im angelsächsischen Rechtskreis bereits seit über 20 Jahren betrieben.[605]

Kernzweck ist die Bewertung des Risikos für die Betroffenen und somit der Schutz personenbezogener Daten. Daneben hilft das DPIA – sinnvoll genutzt – den Entwicklern Risiken früh im Sinne von „Datenschutz durch Technikgestaltung" (Art. 25 DSGVO) zu erkennen sowie Transparenz herzustellen.[606] In die Risikoabwertung dürfen nicht nur Datenschutzrisiken einfließen. Es sind alle Rechte der Grundrechtecharta relevant, wie sich bereits aus dem offenen Wortlaut von Art. 35 Abs. 1 DSGVO entnehmen lässt.[607]

Die DSGVO beschreibt nicht explizit, wann von einem hohen Risiko für die Rechte und Freiheiten für die Betroffenen auszugehen ist. Lediglich in Absatz 3 der Norm werden Fälle genannt, in denen ein DPIA „insbesondere" erforderlich sein soll, also nach Auffassung des Gesetzgebers ein besonders hohes Risiko vorliegt. Nach Art. 35 Abs. 3 lit. a ist beispielsweise eine Folgenabschätzung erforderlich, wenn eine *systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen* (also ein Profiling im Sinne des Art. 4 Nr. 4 DSGVO durchgeführt wird und als Entscheidungsgrundlage dienen soll).

Zu beachten ist hier die unterschiedliche Formulierung im Vergleich zum Verbot der automatisierten Einzelfallentscheidung; anders als Art. 22

---

603 DPIA = Data Protection Impact Assesment; im Deutschland ist auch die Abkürzung „DSFA" geläufig.
604 *Schantz*, NJW 2016, 1841 (1846).
605 Unter dem Namen „Privacy Impact Assessment", vgl. *Friedewald/Schiering/Martin*, DuD 2019, 473.
606 *Friedewald/Schiering/Martin*, DuD 2019, 473 f. m.w.N.
607 So auch *Friedewald/Schiering/Martin*, DuD 2019, 473 (474).

fordert Art. 35 DSGVO gerade keine ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung, sondern lediglich die Gründung der Entscheidung auf eine solche bzw. das Dienen als Grundlage.

Da die Datenschutzfolgenabschätzung keine Auswirkungen auf die rechtliche Zulässigkeit der hier untersuchten Maßnahmen hat, wird auf die Spezialliteratur zu Art. 35 DSGVO[608] sowie das Working Paper 248[609] der *Artikel-29-Datenschutzgruppe* verwiesen.

§ 2 *Betriebsverfassungsrecht*

Das Betriebsverfassungsrecht setzt dem Einsatz moderner Technologien im Bereich Human Ressources weitere Grenzen. In Betrieben mit in der Regel mindestens fünf ständigen wahlberechtigten Arbeitnehmern sollen Betriebsräte gewählt werden, vgl. § 1 Abs. 1 BetrVG. Der Einsatz der hier dargestellten Technologien wird vor allem in größeren Unternehmen stattfinden, da es sich für kleinere Betriebe oftmals nicht lohnt, Profiling-Systeme einzusetzen („*man kennt sich*“) oder diese Technologien schlichtweg zu teuer sind, respektive kein entsprechendes Kosten-/Nutzenverhältnis erzielen.

Im Bereich des Datenschutzes kann eine Betriebsvereinbarung zwar legitimierend wirken,[610] nichtsdestotrotz ist hierfür ein Konsens mit dem Betriebsrat erforderlich. Auch wenn keine Betriebsvereinbarung vorliegt, sind bestimmte (zwingende) Mitbestimmungsrechte zu beachten. Relevant sind insbesondere die Rechte aus den §§ 87 Abs. 1, 94 f. BetrVG[611] sowie die §§ 75 Abs. 2, 92 Abs. 1 und 111 BetrVG, auf die im Folgenden genauer eingegangen wird.

I. Anwendbarkeit des BetrVG

In Unternehmen, in denen Betriebsräte bestehen, regelt das BetrVG die Rechte dieser Interessensvertretung. Anders als das Datenschutzrecht ist

608 So beispielsweise *Bitkom e.V.*, Risk Assessment & Datenschutz-Folgenabschätzung.

609 *Artikel-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 "wahrscheinlich ein hohes Risiko mit sich bringt" (WP 248).

610 Siehe bereits **D. § 1 V. 1**.

611 So bereits *Blum/Kainer*, PERSONALquarterly 2019, 22 (25).

das Betriebsverfassungsrecht grundsätzlich betriebsbezogen. Der Begriff des Betriebs wird vom Gesetz nicht definiert, sondern als bekannt vorausgesetzt. Die Rechtsprechung und überwiegende Literatur definieren den Begriff des Betriebs als „*organisatorische Einheit, innerhalb der ein Unternehmer allein oder in Gemeinschaft mit seinen Mitarbeitern mit Hilfe von sächlichen und immateriellen Mitteln bestimmte arbeitstechnische Zwecke fortgesetzt verfolgt*".[612] Das Betriebsverfassungsgesetz kennt allerdings auch betriebsübergreifende Strukturen wie den Gesamtbetriebsrat (§§ 47 ff. BetrVG) und den Konzernbetriebsrat (§§ 54 ff. BetrVG). Angelegenheiten, die nicht nur einen Betrieb, sondern mehrere Betriebe innerhalb eines Unternehmens betreffen, fallen in die Zuständigkeit des Gesamtbetriebsrats, sofern sie nicht durch die einzelnen Betriebsräte innerhalb ihrer Betriebe geregelt werden können (§ 50 BetrVG). Dies gilt analog für den Konzernbetriebsrat bei Konzernangelegenheiten (§ 58 BetrVG).

Für die Einführung neuer Arbeitsmethoden im Personalwesen sowie den Einsatz neuartiger Tools auf alle Arbeitnehmer ist in aller Regel davon auszugehen, dass die höchste übergreifende Struktur zuständig ist. Dies ist dem Umstand geschuldet, dass Personalarbeit regelmäßig auf der Unternehmensebene und nicht der Betriebsebene angesiedelt ist. Bei Konzernen hingegen ist vielfach die gesamte HR-Abteilung in ein eigenes Unternehmen ausgegliedert, in Form eines „Service-Centers". Von dort aus läuft die zentrale Personalplanung, während auf Unternehmens- und Betriebsebene nur noch Vorgaben der Konzernleitung durchgeführt werden.

Zu beachten ist, dass der Arbeitnehmerbegriff des BetrVG ein Spezialbegriff ist, der nicht mit dem sonstigen arbeitsrechtlichen Arbeitnehmerbegriff übereinstimmt; er geht zwar vom allgemeinen Begriff aus, ist aber sowohl enger (z.B. enge Familienangehörige des Arbeitgebers sind weitgehend ausgenommen), andererseits auch weiter (z.B. im Rahmen der Arbeitnehmerüberlassung oder bei Heimarbeitern).[613]

Wesentlich hierbei ist die Ausnahme für leitende Angestellte nach § 5 Abs. 3 BetrVG. Diese sind zwar ebenfalls als Arbeitnehmer im Sinne des BetrVG zu qualifizieren, dennoch gilt das Betriebsverfassungsrecht nicht für diese Gruppe.[614] Leitende Angestellte sind, vereinfacht dargestellt, solche Personen, die unter eigener Verantwortung typische Unternehmer-

612 Statt aller Richardi/*Richardi/Maschmann*, § 1 BetrVG Rn. 17 m.w.N. zur Rechtsprechung und Literatur.

613 ErfK/*Koch*, § 5 BetrVG Rn. 2.

614 Zur Erfassung der leitenden Angestellen vom betriebsverfassungsrechtlichen Arbeitnehmerbegriff, siehe BT-Drs. IV/1786, S. 36.

funktionen mit einem erheblichen eigenen Entscheidungsspielraum wahrnehmen.[615] Ihnen kommt „ein besonderes persönliches Vertrauen des Arbeitgebers“[616] zugutekommt. Kriterien zur Beurteilung, ob jemand leitender Angestellter ist, finden sich in § 5 Abs. 3 und 4 BetrVG.

Betriebsvereinbarungen entfalten für leitende Angestellte keine normative Wirkung.[617] Ihnen stehen nach §§ 30 ff. SprAuG eigene Mitwirkungsrechte zu, die allerdings bei weitem nicht so umfassend sind, wie jene des Betriebsrats.[618] Berührt eine Betriebsvereinbarung die rechtlichen Interessen der leitenden Angestellten, so muss nach § 2 Abs. 1 S. 2 SprAuG der Sprecherausschuss rechtzeitig angehört werden.[619]

Verwechselt werden darf der Begriff ebenfalls nicht mit dem des Beschäftigten im Sinne des Datenschutzrechts[620], sodass bei der Prüfung, ob Betriebsverfassungsrecht Anwendung findet, genau differenziert werden muss.

II. Mitbestimmungsrechte des Betriebsrats

1. Mitbestimmungsrechte aus § 87 Abs. 1 BetrVG

Zentraler Mitbestimmungstatbestand im Betriebsverfassungsrecht ist § 87 BetrVG, der die Mitbestimmungsrechte des Betriebsrats in sozialen Angelegenheiten regelt. Diese Norm zählt eine Reihe an Tatbeständen auf, bei denen ein vorhandener Betriebsrat (sofern dies nicht bereits durch Gesetz oder Tarifvertrag geregelt wurde) zwingend mitzubestimmen hat. Kommt keine Einigung zwischen Betriebsrat und Arbeitgeber zustande, so entscheidet nach § 87 Abs. 2 BetrVG die Einigungsstelle, deren Spruch für Betriebsrat und Arbeitgeber bindend ist. Werden die Mitbestimmungsrechte aus Absatz 1 verletzt, so hat der Betriebsrat nicht nur einen Unterlassungsanspruch; nach der herrschenden Theorie der Wirksamkeitsvoraussetzung

615 *Kania*, Stichwort "Leitende Angestellte", in: Küttner, Personalbuch 2020, Rn. 1 m.w.N.

616 Dieser Begriff wurde in der Vorgängerfassung der Norm verwendet, hat sich jedoch als zu unbestimmt herausgestellt, weshalb das BetrVG 1972 konkrete Kriterien aufgestellt hat, um eine eindeutigere Abgrenzung zu ermöglichen, vgl. hierzu BT-Drs. IV/1786, S. 36.

617 MHdB-ArbR/*Arnold*, § 316 Die Betriebsvereinbarung, Rn. 31.

618 *Koch*, Sprecherausschüsse, in: Schaub/Koch, Arbeitsrecht von A-Z.

619 Vgl. Richardi/*Richardi*, § 77 BetrVG Rn. 45.

620 Hierauf wird weiter unten bei **E. § 1 III. 1. c) bb)** näher eingegangen.

sind auch einseitige, den Arbeitnehmer belastende, Maßnahmen des Arbeitgebers unwirksam.[621] Ein generelles, datenschutzrechtliches Beweisverwertungsverbot aufgrund eines Verstoßes gegen das Mitbestimmungsrecht ergibt sich dennoch nicht; für ein Beweisverwertungsverbot muss die Verwertung der Informationen zu einem (erneuten) nicht zu rechtfertigenden Eingriff in materielle Grundrechtspositionen (insbesondere in das Persönlichkeitsrecht[622]) führen, der durch die „reine" Verletzung eines Mitbestimmungstatbestands bei der Erhebung noch nicht gegeben ist.[623]

Die erzielte Einigung wird in der Regel in einer Betriebsvereinbarung festgehalten, die nach § 77 Abs. 1 BetrVG vom Arbeitgeber zu vollziehen ist.

Im Folgenden werden die für die eingangs dargestellten Technologien und Einsatzszenarien relevanten Mitbestimmungstatbestände aufsteigend erläutert[624]:

a) § 87 Abs. 1 Nr. 1 BetrVG: Mitbestimmung bei Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb

§ 87 Abs. 1 Nr. 1 BetrVG erfasst die gesamte „Gestaltung des Zusammenlebens und Zusammenwirkens der Arbeitnehmer im Betrieb". Nicht erforderlich ist, dass verbindliche Normen für das Verhalten im Betrieb geschaffen werden. Es ist ausreichend, dass durch eine Maßnahme des Arbeitgebers das Verhalten des Arbeitnehmers in Bezug auf die betriebliche Ordnung beeinflusst bzw. berührt wird.[625] Mitbestimmungspflichtig ist daher nicht nur die *Schaffung* von Verhaltensregelungen, sondern auch

621 Statt aller ErfK/*Kania*, § 87 BetrVG Rn. 136, 138; BeckOK ArbR/*Werner*, § 87 BetrVG Rn. 1 m.w.N. zur st. Rspr.; kritisch insbesondere Richardi/*Richardi*, § 87 BetrVG Rn. 104 ff.

622 *Lunk*, NZA 2009, 457 (459).

623 BAG, Urt. v. 20.10.2016 – 2 AZR 395/15, NZA 2017, 443 (447) Rn. 36; ausführlich Urt. v. 13.12.2007 – 2 AZR 537/06, NZA 2008, 1008 (1010) Rn. 26 ff.; ErfK/*Kania*, § 87 BetrVG Rn. 137; aA BeckOK ArbR/*Werner*, § 87 BetrVG Rn. 4.

624 Spezifisch zur Flexibilisierung der Arbeit (die in dieser Arbeit nicht gesondert betrachtet wird) und der Mitbestimmung nach §§ 87 Abs. 1 Nr. 2 und 3 BetrVG äußern sich *von Lewinski/Barros Fritz/Biermeier*, Bevorstehende und künftige Regelungen des Einssatzes von Alogrithmen im HR-Bereich, <*algorithmwatch.org/de/rechtsgutachten-von-lewinski/*>, S. 30 ff.

625 BAG, Beschl. v. 24.03.1981 – 1 ABR 32/78, NJW 1982, 404 = AP BetrVG 1972 § 87 Arbeitssicherheit Nr. 2.

deren *Vollzug*.[626] Das Mitbestimmungsrecht beruht auf der Tatsache, dass die Arbeitnehmer ihre vertraglich geschuldete Leistung innerhalb einer Arbeitsorganisation erbringen müssen, die vom Arbeitgeber vorgegeben ist und dabei einem Weisungsrecht unterliegen.[627] Der Betriebsbegriff ist daher in diesem Rahmen nicht räumlich, sondern funktional zu verstehen, sodass beispielsweise auch Regelungen zum Verhalten von Mitarbeitern im Außendienst erfasst sind.[628]

Zu unterscheiden ist innerhalb des Tatbestands zwischen Regelungen, die das Ordnungsverhalten und solchen, die das Arbeitsverhalten betreffen. Letztere sind unter diesem Tatbestand nicht mitbestimmungspflichtig.[629] Regelungen zum Arbeitsverhalten weisen keinen Bezug zur betrieblichen Ordnung auf, sondern beziehen sich auf die arbeitsvertragliche Leistungsverpflichtung wie beispielsweise Arbeitsanweisungen, in denen im Rahmen des Direktionsrechts näher bestimmt wird, welche Arbeiten wie ausgeführt werden.[630] Sie konkretisieren daher die Arbeitspflicht als Hauptleistungspflicht des zwischen dem Arbeitgeber und dem Arbeitnehmer geschlossenen Vertrags.

Nicht unter den Mitbestimmungstatbestand fällt ferner die Ausübung individualrechtlicher Befugnisse (Versetzung, Abmahnung, Kündigung etc.), beispielsweise als Reaktion auf ein Fehlverhalten des Arbeitnehmers, auch wenn diese aus einem Verstoß gegen die betriebliche Ordnung folgt.[631]

Bei der Kontrolle der Arbeitnehmer ist zu differenzieren: Maßnahmen, die nur zur Kontrolle und ggf. Steuerung des Arbeitsverhaltens dienen, unterfallen nicht der Mitbestimmung nach § 87 Abs. 1 Nr. 1 BetrVG (Anm.: Sie können aber von Nr. 6 erfasst werden, dazu sogleich). Wird mit der Überwachung auch eine Verhaltenssteuerung im Betrieb bezweckt, so ist der Tatbestand erfüllt.[632]

---

626 Richardi/*Richardi*, § 87 BetrVG Rn. 176.
627 *Fitting*, § 87 Nr. 1 Rn. 63.
628 BAG, Beschl. v. 22.08.2017 – 1 ABR 52/14, NZA 2018, 50 (53) = BAGE 160, 41 Rn. 25; Beschl. v. 27.01.2004 – 1 ABR 7/03, NZA 2004, 556 (557) = BAGE 109, 235 unter II. 1. a) bb) der Gründe.
629 St. Rspr.; vgl. statt vieler BAG, Beschl. v. 22.08.2017 – 1 ABR 52/14, NZA 2018, 50 (52) = BAGE 160, 41 Rn. 24 m.w.N.
630 BAG, Beschl. v. 21.01.1997 – 1 ABR 53/96, AP BetrVG 1972 § 87 Ordnung des Betriebes Nr. 27 unter B. I. 1. der Gründe.
631 BAG, Beschl. v. 17.10.1989 – 1 ABR 100/88, BAGE 63, 169 - juris Rn. 39 f.
632 BeckOK ArbR/*Werner*, § 87 BetrVG Rn. 29.

Im Rahmen von *People Analytics* gibt es unzählige Maßnahmen, die vom Mitbestimmungsrecht des § 87 Abs. 1 Nr. 1 BetrVG erfasst werden, weil nicht primär das Arbeitsverhalten kontrolliert werden soll. So bleibt beispielsweise die Durchführung der Arbeit auch ohne das Tragen von Wearables, die beispielsweise zum Gesundheitsschutz eingesetzt werden, möglich. Aus diesem Grund fällt die Anordnung zum Tragen solcher unter dieses Mitbestimmungsrecht.[633] Auch der Einsatz von Dashboards für Arbeitnehmer, um den persönlichen Alltag zu optimieren,[634] bezweckt eine Verhaltenssteuerung und ist somit vom Mitbestimmungsrecht erfasst.

§ 87 Abs. 1 Nr. 1 BetrVG soll (neben § 87 Abs. 1 Nr. 6 BetrVG, dazu sogleich) ebenfalls, die Persönlichkeitsrechte der Arbeitnehmer bei einseitigen Maßnahmen schützen.[635]

Freilich reicht die Regelungsbefugnis der Betriebspartner nur so weit, wie der Arbeitgeber dem Arbeitnehmer das Verhalten im Rahmen seines Direktionsrechts vorschreiben kann. Es ist somit nicht möglich, in einer Betriebsvereinbarung die Überwachung des Privatlebens der Arbeitnehmer über das betriebliche Smartphone zu regeln.[636]

b) § 87 Abs. 1 Nr. 6 BetrVG: Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen

Nach dem Wortlaut des § 87 Abs. 1 Nr. 6 BetrVG hat der Betriebsrat ein Mitbestimmungsrecht bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.

Dieser Mitbestimmungstatbestand bezweckt primär den Schutz der Persönlichkeitsrechte der Arbeitnehmer vor Eingriffen durch den Arbeitgeber

633 Zu beachten sind hier die Parallelen zu einer vorgegebenen Kleiderordnung, vgl. BAG, Beschl. v. 08.08.1989 – 1 ABR 65/88, AP BetrVG 1972 § 87 Ordnung des Betriebes Nr. 15 unter B. I. 2. der Gründe.

634 Hierzu **E. § 3 I.**

635 BAG, Beschl. v. 17.01.2012 – 1 ABR 45/10, NZA 2012, 687 (689) Rn. 26 m.N.

636 BAG, Beschl. v. 27.01.2004 – 1 ABR 7/03, NZA 2004, 556 (557) = BAGE 109, 235 unter II. 1. a) bb) der Gründe.

mittels technischer Einrichtungen,[637] da hierdurch besondere und vielfältige Gefahren geschaffen werden.[638]

Da dieses Mitbestimmungsrecht vor allem bei der Digitalisierung der Arbeit in den hier dargestellten Formen eine Rolle spielt, dennoch aber keine neuen mitbestimmungsrechtlichen Problemlagen erzeugt werden[639], erfolgt im Folgenden eine vertiefte Auseinandersetzung mit den Einzelheiten von § 87 Abs. 1 Nr. 6 BetrVG.

aa) Definitionen: Technische Einrichtung / Überwachung

Technische Einrichtungen sind „*Anlagen oder Geräte […], die, unter Verwendung nicht menschlicher, sondern anderweit erzeugter Energie, mit den Mitteln der Technik, insbesondere der Elektronik, eine selbstständige Leistung erbringen.*“[640] Kern des Mitbestimmungstatbestandes ist also die Erweiterung der Überwachung über das individuelle Wahrnehmungsvermögen einer kontrollierenden Person hinaus.[641] Hieraus resultiert ein deutlich höheres Gefahrenpotential für die Persönlichkeitsrechte, da somit unabhängig, dauernd und unterunterbrochen Daten im Rahmen einer Überwachung gesammelt werden können, sogar in einer Form, die für den betroffenen Arbeitnehmer nicht wahrnehmbar ist.[642]

Unter Überwachung wird ein Vorgang verstanden, bei welchem Informationen über das überwachende Objekt gesammelt, verarbeitet oder ausgewertet werden (in Form eines Soll-Ist-Vergleichs). Hierdurch soll entschieden werden können, ob und ggf. wie auf eine festgestellte Abwei-

637 ErfK/*Kania*, § 87 BetrVG Rn. 48; GK-BetrVG/*Wiese/Gutzeit*, § 87 Nr. 6 BetrVG Rn. 510: kollektivrechtliche Ergänzung des individualrechtlichen Persönlichkeitsschutzes; DKW/*Klebe*, § 87 Nr. 6 BetrVG Rn. 166.

638 BAG, Beschl. v. 11.03.1986 – 1 ABR 12/84, AP BetrVG 1972 § 87 Überwachung Nr. 14; GK-BetrVG/*Wiese/Gutzeit*, § 87 Nr. 6 BetrVG Rn. 511.

639 GK-BetrVG/*Wiese/Gutzeit*, § 87 Nr. 6 BetrVG Rn. 507: „*Die Mitbestimmung [hängt] nicht von diffusen Entwicklungen im Arbeitsleben ab, sondern [knüpft] gegenständlich an technische Überwachungseinrichtungen an*“; hierzu auch DKW/*Klebe*, § 87 Nr. 6 BetrVG Rn. 156a.

640 BVerwG, Beschl. v. 31.08.1988 – 6 P 35.85, AP BPersVG § 75 Nr. 25 zur Definition der "technischen Einrichtung" im Sinne des wortgleichen § 75 Abs. 3 Nr. 17 BPersVG.

641 Richardi/*Richardi/Maschmann*, § 87 BetrVG Rn. 496.

642 Richardi/*Richardi/Maschmann*, § 87 BetrVG Rn. 496.

chung reagiert werden soll. Jeder einzelne Teilvorgang an sich ist bereits eine Überwachung.[643]

Ziel des Mitbestimmungstatbestandes ist es folglich, *„Arbeitnehmer vor Beeinträchtigungen ihres Persönlichkeitsrechts durch den Einsatz technischer Überwachungseinrichtungen zu bewahren, die nicht durch schutzwerte Belange des Arbeitgebers gerechtfertigt und unverhältnismäßig sind*"[644], m.a.W. zu verhindern, dass der Arbeitnehmer zum bloßen Überwachungsobjekt wird.[645] Hierbei stellt das Bundesarbeitsgericht unter anderem auf die Ausführungen der höchsten Richter aus Karlsruhe zum Volkszählungsgesetz[646] ab. Zu beachten sei jedoch, dass das Mitbestimmungsrecht nicht auf den Schutz vor Gefahren der modernen Datenverarbeitung schlechthin abziele, sondern dem Umstand Rechnung trage, dass der individual- und datenschutzrechtliche Schutz nicht ausreiche und daher durch einen kollektiven Schutz ergänzt werden müsse. Bei der technischen Auswertung drohe ein Kontextverlust der Daten ohne Möglichkeit einer wirksamen Gegenkontrolle, was zu einem erheblichen Informationsdruck für den Arbeitnehmer führe, seine Abhängigkeit steigere und ihn zum Informationsobjekt mache.[647]

Erforderlich ist daher, dass das Verhaltens- und Leistungsdatum einzelnen Arbeitnehmern zugeordnet werden kann, da ansonsten keine Überwachung vorliegt;[648] ausreichend ist auch eine Gruppe von Arbeitnehmern, sofern diese für eine bestimmte Leistung oder Verhalten gemeinschaftlich verantwortlich ist.[649] Letzteres gilt aber nur insoweit, als (mittelbar) Rückschlüsse auf die einzelnen Arbeitnehmer gezogen werden können.[650] Inso-

643 BAG, Beschl. v. 14.09.1984 – 1 ABR 23/82, NZA 1985, 28 (29 f.) m.w.N.

644 BAG, Beschl. v. 13.12.2016 – 1 ABR 7/15, NZA 2017, 657 (659) = BAGE 157, 220 = AP BetrVG 1972 § 87 Nr. 47 Rn. 21.

645 St. Rspr.; vgl. BAG, Beschl. v. 13.12.2016 – 1 ABR 7/15, NZA 2017, 657 (659) = BAGE 157, 220 = AP BetrVG 1972 § 87 Nr. 47 Rn. 21; Beschl. v. 29.06.2004 – 1 ABR 21/03, NZA 2004, 1278 (1281) = BAGE 111, 173 = AP BetrVG § 87 1972 Überwachung Nr. 41 (m. Anm. Ehmann); Beschl. v. 18.02.1986 – 1 ABR 21/84, BAGE 51, 143 - juris Rn. 27.

646 BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1 – Volkszählungsurteil.

647 So beispielsweise in BAG, Beschl. v. 14.09.1984 – 1 ABR 23/82, NZA 1985, 28 (30).

648 BAG, Beschl. v. 14.09.1984 – 1 ABR 23/82, NZA 1985, 28 (29).

649 BAG, Beschl. v. 18.02.1986 – 1 ABR 21/84, BAGE 51, 143 - juris Rn. 23.

650 GK-BetrVG/*Wiese/Gutzeit*, § 87 Nr. 6 BetrVG Rn. 573 f.

fern lässt sich hier eine Parallele zum datenschutzrechtlichen Personenbezug finden.[651]

Beispiele für technische Überwachungseinrichtungen sind: Zeitstempler[652], die automatische Erfassung von Telefongesprächen mittels EDV-Anlagen[653], Fahrtenschreiber[654], aber auch Software, die aufzeichnet[655] (bspw. Office Software, da für jede Datei die Bearbeitungszeit und Bearbeitungsdauer gespeichert wird und eingesehen werden kann sowie Browser, die den Verlauf und Cookies speichern[656]), Mobiltelefone[657], Personalabrechnungs- und Informationssysteme[658].

Besonders die zitierte Entscheidung zum letzten Beispiel ist interessant, da das System im Fall des BAG Aussagen über das Verhalten und die Leistung des Arbeitnehmers erarbeitete, ohne die dieser Aussage zugrunde liegenden Daten selbst auszuweisen. So wurden im System nicht die einzelnen geschriebenen Zeilen erfasst, jedoch die Gesamtzeilenanzahl pro Arbeitnehmer über einen bestimmten Zeitraum. Eine Überwachung liegt daher bereits vor, wenn nicht jeder einzelne Arbeitsvorgang gespeichert wird, sondern eine Zusammenfassung aller Arbeitsvorgänge beispielsweise am Ende eines Arbeitstages erzeugt wird. Ausreichend ist ebenfalls, wenn diese bereits in einer aufgearbeiteten Form angezeigt werden (z.B. wie im Fall durch eine Anzeige der vom jeweiligen Sachbearbeiter verfassten Zeilen im System anstatt der Anzeige der einzeln verfassten Zeilen). Für das Vorliegen einer mitbestimmungspflichten Überwachung ist es sogar nicht einmal relevant, dass die Aufzeichnung an sich noch keine sachgerechte Beurteilung der Leistung des Arbeitnehmers erlaubt.[659]

---

651 *Götz*, Big Data im Personalmanagement, S. 189.

652 LAG Düsseldorf, Beschl. v. 21.11.1978 – 19 TaBV 39/78, DB 1979, 459.

653 BAG, Beschl. v. 27.05.1986 – 1 ABR 48/84, AP BetrVG 1972 § 87 Überwachung Nr. 15 = NZA 1986, 643.

654 BAG, Beschl. v. 10.07.1979 – 1 ABR 50/78, AP BetrVG 1972 § 87 Überwachung Nr. 3.

655 Spezifisch zum Keylogger: BAG, Urt. v. 27.07.2017 – 2 AZR 681/16, NZA 2017, 1327 = BAGE 159, 389 = CR 2018, 27.

656 ErfK/*Kania*, § 87 BetrVG Rn. 62.

657 Insbes. aufgrund der Möglichkeit, Einzelgesprächsnachweise vom Provider anzufordern (so bereits *Wedde*, CR 1995, 41 (45), bei Smartphones aber insbesondere auch durch die im Gerät verbauten Sensoren und dadurch deutlich weitreichenderen Überwachungsmöglichkeiten.

658 „PAISY", vgl. BAG, Beschl. v. 23.04.1985 – 1 ABR 2/82, AP BetrVG 1972 § 87 Überwachung Nr. 12.

659 BAG, Beschl. v. 23.04.1985 – 1 ABR 2/82, AP BetrVG 1972 § 87 Überwachung Nr. 12.

Bei Big Data-Anwendungen besteht daher immer dann ein Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG, wenn bezogen auf einzelne Arbeitnehmer oder Gruppen von Arbeitnehmer, die für eine Leistung gemeinsam verantwortlich sind, Aussagen getroffen werden oder Daten aggregiert dargestellt werden.

Zu beachten ist, dass dieses Mitbestimmungsrecht auch dann besteht, wenn die Datenverarbeitung nicht beim Arbeitgeber, sondern einem Dritten erfolgt.[660]

bb) Reichweite des Mitbestimmungsrechts: Überwachungseignung ausreichend

Eine technische Einrichtung ist dann zur Überwachung von Verhalten und Leistung der Arbeitnehmer bestimmt, wenn sie „aufgrund vorhandener Programme Verhaltens- und Leistungsdaten ermittelt und aufzeichnet, die bestimmten Arbeitnehmern zugeordnet werden können, unabhängig davon, zu welchem Zweck diese Daten erfasst werden.[661]

Früher wurde in diesem Zusammenhang teilweise vertreten, dass es auf die subjektive Zielsetzung ankomme, die der Arbeitgeber mit der technischen Kontrolleinrichtung verfolge, da ansonsten der gesetzliche Tatbestand verlassen und das Mitbestimmungsrecht grenzenlos ausgeweitet würde.[662] Hierfür spräche auch der Wortlaut der Norm, der von einer Bestimmung zur Überwachung spricht. Bereits kurz nach Inkrafttreten des BetrVG 1972 hatte sich das BAG mit dieser Streitfrage zu beschäftigen und dabei festgestellt, dass eine objektive Eignung zur Überwachung ausreichend ist:[663]

In dem vom BAG behandelten Fall ging es um die Inbetriebnahme von sog. Produktographen (Nutzungsschreiber). Der Betriebsrat sah ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG, da diese Produktographen objektiv dazu geeignet seien, die Leistungen der Arbeitnehmer zu

---

660 BAG, Beschl. v. 27.01.2004 – 1 ABR 7/03, NZA 2004, 556 (558) = BAGE 109, 235; MHdB-ArbR/*Salamon*, § 325 Mitbestimmung bei der technischen Überwachung, Rn. 11.

661 BAG, Beschl. v. 18.02.1986 – 1 ABR 21/84, BAGE 51, 143 - juris Rn. 19.

662 Vgl. *Ehmann*, EzA § 87 BetrVG 1972 Bildschirmarbeitsplatz Nr. 1; *Stadler*, BB 1972, 800.

663 BAG, Beschl. v. 09.09.1975 – 1 ABR 20/74, AP BetrVG 1972 § 87 Überwachung Nr. 2, seitdem st. Rspr. und h.L., vgl. statt aller BeckOK ArbR/*Werner*, § 87 BetrVG Rn. 92 m.w.N.

überwachen. Der Arbeitgeber wandte sich hiergegen mit dem Argument, dass er nicht beabsichtige, die Maschinenarbeiter zu überwachen, sondern lediglich wissen wolle, wie die Maschinen tatsächlich genutzt würden.

Die Erfurter Richter untersuchten in ihrem Beschluss lehrbuchartig die Vorschrift anhand der juristischen Auslegungsmethoden. Dabei stellten sie auf die Begründung zum Regierungsentwurf des BetrVG 1972[664] ab, die den Eingriff in den persönlichen Bereich der Arbeitnehmer in den Mittelpunkt stellt. Hieraus ergebe sich, dass es auf die objektive Eignung und Verwendungsmöglichkeit der Einrichtung ankomme und nicht auf die subjektive Zielrichtung des Arbeitgebers. Schutzziel sei, Eingriffe in den Persönlichkeitsbereich der Arbeitnehmer durch Verwendung anonymer technischer Kontrolleinrichtungen nur bei gleichberechtigter Mitbestimmung des Betriebsrats zuzulassen. Nach § 75 Abs. 2 BetrVG verpflichteten sich Arbeitgeber und Betriebsrat gemeinsam zur Wahrung und Förderung der Persönlichkeitsrechte der Arbeitnehmer. Dies sei auch bei der Auslegung von § 87 Abs. 1 Nr. 6 BetrVG zu beachten. Es bestehe kein Unterschied, ob eine Überwachung das erklärte Ziel der Einrichtung sei oder lediglich ein Nebeneffekt und ob die Daten ausgewertet würden oder nicht. Denn eine Überwachung beginne nicht erst mit der Auswertung der Daten.

Beim Abstellen auf eine subjektive Überwachungsabsicht gäbe es ferner ein weiteres Problem: Mitbestimmungsrechte des Betriebsrats wären allein von (regelmäßig) nicht feststellbaren subjektiven Elementen auf Seiten des Arbeitgebers abhängig.[665] Aus diesem Grund ist heute allgemeine Auffassung, dass eine Überwachungseignung ausreicht.[666]

Weiterhin umstritten ist jedoch, ob die bloße Möglichkeit zur Überwachung (aufgrund der Rechen- und Speicherkapazität / Eignung der Einrichtung) ausreicht, oder die Einrichtung auch so eigesetzt werden muss, dass tatsächlich Beschäftigtendaten erfasst werden, die zur Kontrolle ihrer Leistung oder ihres Verhaltens verwendet werden könnten.[667]

---

664 BT-Drs. IV/1786, S. 48 f.

665 BAG, Beschl. v. 06.12.1983 – 1 ABR 43/81, BAGE 44, 285 (Rn. 166) = AP BetrVG 1972 Überwachung Nr. 7 (zit. n. juris).

666 Vgl statt vieler GK-BetrVG/*Wiese/Gutzeit*, § 87 Nr. 6 BetrVG Rn. 532; DKW/*Klebe*, § 87 Nr. 6 BetrVG Rn. 186 jeweils m.w.N.

667 Bloße Möglichkeit der Überwachung ausreichend: *Däubler*, Gläserne Belegschaften, Rn. § 14 Rn. 756; wohl auch BVerwG, Beschl. v. 02.02.1990 – 6 PB 11.89, BeckRS 1990, 30937999; Beschl. v. 27.11.1991 – 6 P 7.90, BeckRS 1991, 30937826 = NVwZ-RR 1993, 153 (ausreichend ist die Möglichkeit, dass ein Überwachungsprogramm nachinstalliert wird) ; dagegen: Richardi/*Richar-*

In seiner Entscheidung zur Auslegung des § 76 Abs. 3 Nr. 17 BPersVG[668] hat das Bundesverwaltungsgericht den Schutzzweck der Norm in den Vordergrund gestellt:[669] Das Mitbestimmungsrecht soll dazu dienen, dass die Beeinträchtigungen und Gefahren für den Schutz der Persönlichkeit auf das erforderliche Maß beschränkt bleiben. Der Überwachungsdruck für den Mitarbeiter entstehe bereits dann, wenn die Anlage „*ohne weiteres, d.h. ohne unüberwindliche Hindernisse, mit einem solchen [Überwachungs-]Programm versehen werden kann*." Dies sei dann der Fall, wenn sich dieses „*beim Hersteller der Anlage oder sonst ohne außergewöhnliche Schwierigkeiten und ohne unverhältnismäßigen Aufwand*" beschaffen ließe. In diesem Falle müsse der Arbeitnehmer immer damit rechnen, verdeckt überwacht zu werden, was ihn in der Entfaltung seiner Persönlichkeit einschränken würde. Nur wenn es einer technischen Änderung der Anlage bedürfe, scheide ein Mitbestimmungsrecht aus.

Nicht nachvollziehbar ist die Begründung des Bundesverwaltungsgerichts allerdings, wenn sie unterstellt, dass ein Benutzer einer technischen Anlage immer mit einer (heimlichen) Überwachung rechnen müsse. Zunächst wird sich ein Arbeitnehmer, wenn keine Anhaltspunkte bestehen, einerseits davon ausgehen, dass sich der Arbeitgeber rechtmäßig verhalten wird, andererseits lässt das Urteil eine Begründung für die selbst statuierte Ausnahme vermissen: Weshalb kommt es darauf an, ob die Softwareeinfach besorgt werden kann oder die Anlage zuvor technisch verändert werden muss? Folgte man der Begründung zum überzeugten Überwachungsdruck, müssten alle Anlagen erfasst sein, auch jene, die erst noch technisch geändert werden müssen oder bei denen der Arbeitgeber nur unter Schwierigkeiten die Überwachungssoftware beschaffen kann. Ein durchschnittlicher Arbeitnehmer kann nicht erkennen, ob die Anlage technisch geändert wurde oder Beschaffung von Überwachungssoftware schwierig ist.

Das Bundesarbeitsgericht ist der Auffassung, dass die Funktions- und Arbeitsweise von solchen Programmen nicht verheimlicht werden könne, weil den Arbeitnehmern die Anwendung erklärt und erläutert werden müsse und diese Erläuterungen auch dem Betriebsrat zugänglich seien. Im

---

di/Maschmann, § 87 BetrVG Rn. 513; MHdB-ArbR/*Salamon*, § 325 Mitbestimmung bei der technischen Überwachung, Rn. 34 ff.; DKW/*Klebe*, § 87 Nr. 6 BetrVG Rn. 186; BAG, Beschl. v. 06.12.1983 – 1 ABR 43/81, BAGE 44, 285 = AP BetrVG 1972 Überwachung Nr. 7 - juris Rn. 163 ff.

668 Diese Norm entspricht dem § 87 Abs. 1 Nr. 6 BetrVG.

669 BVerwG, Beschl. v. 27.11.1991 – 6 P 7.90, BeckRS 1991, 30937826 = NVwZ-RR 1993, 153.

Übrigen könne der Betriebsrat nach § 80 Abs. 2 BetrVG eine rechtzeitige und umfassende Unterrichtung über das jeweilige Programm und dessen Arbeitsweise verlangen, wozu auch die Auskunft gehöre, welche Verhaltens- und Leistungsdaten aufgezeichnet werden. Bei mangelnder Sachkunde kann ein Sachverständiger nach § 80 Abs. 3 BetrVG hinzugezogen werden. Daher bestünden ausreichend Möglichkeiten für den Betriebsrat, sich genügend Kenntnisse zu verschaffen, um die Voraussetzungen für ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG zu prüfen.[670]

Letztlich muss der Arbeitgeber – wenn der Betriebsrat ein Mitbestimmungsrecht geltend macht –zumindest darlegen, warum ein etwaiges Mitbestimmungsrecht nach seiner Auffassung nicht besteht. Damit erhalten der Betriebsrat und über ihn mittelbar die Arbeitnehmer den Überblick über die Einrichtung. Ein Überwachungsdruck aufgrund Ungewissheit lässt sich daher auch ohne Ausweitung des Tatbestands vermeiden.

Voraussetzung für die Entstehung eines Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 6 BetrVG ist daher, dass die Anlage tatsächlich personenbezogene Daten erfasst oder erzeugt, unabhängig von der konkreten Nutzungsweise der Daten. Ohne eine Erfassung von Daten über Beschäftigte besteht auch kein Mitbestimmungsrecht des Betriebsrats, denn dann ist die technische Einrichtung nicht für die Überwachung geeignet.[671]

cc) Zeitpunkt der Mitbestimmung: Einführung und Anwendung der technischen Einrichtung

Das Mitbestimmungsrecht setzt bereits früh – nämlich in der Planungsphase einer solchen technischen Einrichtung – an. Als „Einführung" wird die Entscheidung, ob, für welchen Zeitraum und mit welcher Zweckbestimmung und Wirkungsweise eine solche Kontrolleinrichtung betrieben werden soll, verstanden. Es handelt sich somit um das Vorfeld der zweiten Tatbestandsalternative „Anwendung". Hierbei werden alle vorbereitenden Maßnahmen vom Mitbestimmungsrecht erfasst.[672]

---

670 BAG, Beschl. v. 06.12.1983 – 1 ABR 43/81, BAGE 44, 285 (Rn. 172) = AP BetrVG 1972 Überwachung Nr. 7(zit. n. juris).

671 So auch BAG, Beschl. v. 06.12.1983 – 1 ABR 43/81, BAGE 44, 285 (Rn. 169, insbes. Rn. 177) = AP BetrVG 1972 Überwachung Nr. 7 (zit. n. juris); so auch die h.M., vgl. statt vieler GK-BetrVG/*Wiese/Gutzeit*, § 87 Nr. 6 BetrVG Rn. 535 m.w.N.

672 *Bachner*, DB 2006, 2518 m.w.N.

Der Betriebsrat hat also sowohl beim „Ob" der Überwachungseinrichtung als auch beim „Wie" in Bezug auf die Abwicklung und Anwendung der technischen Überwachungseinrichtung mitzubestimmen.[673]

Ein Initiativrecht bezüglich der Einführung einer technischen Überwachungseinrichtung hat der Betriebsrat hingegen nicht.[674] Dies ergibt sich aus dem – bereits dargestellten – Sinn und Zweck der Vorschrift, dem Schutz der Arbeitnehmer vor Eingriffen in das Persönlichkeitsrecht. Im Kern beinhaltet das Recht eine Abwehrfunktion gegenüber der Einführung solcher Einrichtungen. Dieser Kernfunktion würde es widersprechen, wenn man dem Betriebsrat mit dieser Vorschrift dazu verhelfen würde, eine solche Überwachungseinrichtung über das Mitbestimmungsrecht in Form eines Initiativrechts gerade einzuführen. Aus demselben Grund hat der Betriebsrat auch kein Mitbestimmungsrecht bei der Abschaffung von Überwachungseinrichtungen durch den Arbeitgeber.[675] Über § 87 Abs. 1 Nr. 6 BetrVG kann der Betriebsrat jedoch initiativ die Abschaffung einer Überwachungseinrichtung verlangen – dies ergibt sich ebenfalls aus dem Telos der Norm.[676]

dd) Form der Mitbestimmung

Grundsätzlich reicht eine formlose Betriebsabsprache zur Wahrung von Mitbestimmungsrechten aus. In aller Regel wird in diesem Zusammenhang jedoch eine Betriebsvereinbarung abgeschlossen – dies erfolgt aber nicht aus betriebsverfassungsrechtlichen, sondern aus datenschutzrechtlichen Gründen: Nach § 26 Abs. 4 BDSG kann eine Betriebsvereinbarung legitimierende Wirkung für die Datenverarbeitung haben,[677] nicht ausreichend wäre mangels normativer Wirkung eine bloße Regelungsabrede.

673 Richardi/*Richardi/Maschmann*, § 87 BetrVG Rn. 525.

674 BAG, Beschl. v. 28.11.1989 – 1 ABR 97/88, NZA 1990, 406; GK-BetrVG/*Wiese/Gutzeit*, § 87 Nr. 6 BetrVG Rn. 597 Der Betriebsrat hat allerdings ein Initiativrecht zur Änderung bestehender Kontrolleinrichtungen, vgl. *Fitting*, § 87 Nr. 6 Rn. 251.

675 Ausführlich BAG, Beschl. v. 28.11.1989 – 1 ABR 97/88, NZA 1990, 406 (407 f.).

676 So auch Richardi/*Richardi/Maschmann*, § 87 BetrVG Rn. 527, 531 m.w.N.

677 Siehe hierzu die Ausführungen unter **D. § 1 V. 1.**

ee) Grenzen des Mitbestimmungsrechts

Eine Grenze erfährt das Mitbestimmungsrecht dort, wo durch die Mitbestimmung des Betriebsrats, respektive durch eine Betriebsvereinbarung in unzulässiger Weise in das Persönlichkeitsrecht des Arbeitnehmers eingegriffen wird. Einerseits verstößt eine etwaige Betriebsvereinbarung hierdurch bereits gegen die Vorgaben des Art. 88 Abs. 2 DSGVO bzw. § 26 Abs. 4 S. 2 BDSG, sofern sie diesbezügliche Erlaubnistatbestände zur Datenverarbeitung enthält. Andererseits ist diese auch aus betriebsverfassungsrechtlichen Gründen rechtswidrig. Nach § 75 Abs. 2 BetrVG haben Arbeitgeber und Betriebsrat die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und fördern. Diese Verpflichtung ist eine Konkretisierung und gesetzliche Bestätigung, dass das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1, Art. 1 Abs. 1 GG auch im Betrieb gilt.[678]

Auch im Rahmen der Mitbestimmung sind daher nur verhältnismäßige Eingriffe in das allgemeine Persönlichkeitsrecht gestattet, wobei eine Gesamtabwägung der Umstände und Interessen beider Seiten stattzufinden hat. Auch wenn im Grundsatz das Datenschutzrecht hier bereits (enge) Vorgaben macht und die Verhältnismäßigkeit konkretisiert, spielt noch ein weiterer Faktor eine wichtige Rolle: Die Kollektivität der Maßnahme bzw. Eingriffe. Auch wenn der Eingriff für den einzelnen Arbeitnehmer nur eine geringfügige Einschränkung seines Persönlichkeitsrechts darstellt, daher verhältnismäßig (und somit datenschutzrechtlich zulässig) ist, kann aufgrund der Anzahl der betroffenen Arbeitnehmer kollektivrechtlich das geplante Vorhaben unzulässig sein.

Das BAG führt zur Gesamtabwägung aus: „*Für die Schwere des Eingriffs ist insbesondere von Bedeutung, wie viele Personen intensiv den Beeinträchtigungen ausgesetzt sind. Das Gewicht der Beeinträchtigung hängt u.a. davon ab, ob die Betroffenen als Personen anonym bleiben, welche Umstände und Inhalte der Kommunikation erfasst werden und welche Nachteile den Grundrechtsträgern aus der Überwachungsmaßnahme drohen oder von ihnen nicht ohne Grund befürchtet werden. Die Intensität der Beeinträchtigung hängt ferner maßgeblich von der Dauer und Art der Überwachungsmaßnahme ab. Von erheblicher Bedeutung ist, ob der Betroffene einen ihm zurechenbaren Anlass für die Datenerhebung geschaffen hat – etwa durch eine Rechtsverletzung – oder ob diese anlasslos*

678 BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (Rn. 1189) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54 Rn. 14 ff.; ferner Richardi/*Maschmann*, § 75 BetrVG Rn. 44 f.

erfolgt. Auch die ‚Persönlichkeitsrelevanz' der erfassten Informationen ist zu berücksichtigen."[679]

Die Schutzpflicht des § 75 Abs. 2 BetrVG statuiert somit eine Schranke für die Regelungsmacht der Betriebsparteien;[680] Abreden oder Vereinbarungen, die in unverhältnismäßiger Weise in das Persönlichkeitsrecht der Arbeitnehmer eingreifen, sind unzulässig und somit unwirksam.[681] Bei der Abwägung muss darauf geachtet werden, dass auf die „kollektiven Persönlichkeitsinteressen" und nicht lediglich auf einzelne Arbeitnehmer abgestellt wird, wobei die Verletzung des Persönlichkeitsrechts eines einzelnen Arbeitnehmers bereits zur Unwirksamkeit der Absprache führt, da diese gleichermaßen auch für ihn gelten würde.

c) § 87 Abs. 1 Nr. 10 und 11 BetrVG: Mitbestimmung bei Entlohnung und Entgelten

§ 87 Abs. 1 Nr. 10 und 11 BetrVG regeln die Mitbestimmung bei der Entlohnung sowie bei der Festsetzung von leistungsbezogenen Entgelten. Da bei beiden Mitbestimmungsrechten die Entlohnung der Arbeitnehmer im Mittelpunkt steht, werden diese für die Zwecke der vorliegenden Arbeit gemeinsam analysiert. Von Relevanz werden diese Mitbestimmungsrechte im Bereich der digitalen Arbeit insbesondere dann, wenn computergestützte Systeme dazu verwendet werden sollen, um die Entlohnung der Arbeitnehmer bestimmen bzw. beeinflussen, beispielsweise indem ein Teil der Vergütung variabel bezahlt wird und die genaue Höhe anhand von Kennzahlen aus IT-Systemen ermittelt wird.

Sinn und Zweck des Mitbestimmungsrechts aus § 87 Abs. 1 Nr. 10 BetrVG ist die Sicherstellung der Angemessenheit und Durchsichtigkeit des innerbetrieblichen Lohngefüges.[682] Ferner soll die Beteiligung des Be-

679 BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (Rn. 21) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54 m.w.N. aus der höchstrichterlichen Rechtsprechung.

680 BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205; BAG, Beschl. v. 15.04.2014 – 1 ABR 2/13 (B), NZA 2014, 551 = BAGE 148, 26 = AP BetrVG 1972 § 29 Nr. 9; BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54; aus der Literatur ErfK/*Kania*, § 87 BetrVG Rn. 9; *Fitting*, § 75 Rn. 142.

681 Richardi/*Richardi/Maschmann*, § 87 BetrVG Rn. 541.

682 St. Rspr.; vgl. statt aller BAG GS, Beschl. v. 03.12.1991 – GS 2/90, AP BetrVG 1972 § 87 Lohngestaltung Nr. 51.

triebsrats die Arbeitnehmerschaft vor einer einseitig an den Interessen des Unternehmens orientierten Lohngestaltung schützen. Das „Ob" der Leistungsgewährung obliegt jedoch dem Arbeitgeber.[683] Kurzum ist das Ziel daher die Herstellung von Lohngerechtigkeit.[684]

Ferner werden lediglich kollektive Entlohnungsfragen vom Mitbestimmungsrecht erfasst; die individuelle Lohngestaltung, die mit Rücksicht auf die besonderen Umstände des einzelnen Arbeitsverhältnisses getroffen wird, unterliegt nicht der Mitbestimmung.[685]

Sollen beispielsweise leistungsbezogene Entgelte auf Basis von Kennzahlen aus Big Data/IT-Systemen bezahlt werden, so muss eine Bezugsgröße und Bezugsbasis festgelegt werden, um hier einen Grundsatz und eine Entlohnungsstruktur aufzustellen. Diese können arbeits- oder erfolgsabhängig sein; bei der Festlegung solcher Strukturen und der dazu verwendbaren Kennzahlen und Gewichtungen hat der Betriebsrat mitzubestimmen.[686] Der Betriebsrat hat (nicht nur aufgrund § 75 Abs. 2 BetrVG) darüber zu wachen, dass diese Kennzahlen nachvollziehbar und transparent gebildet werden, um dem Telos der Norm gerecht sein Mitbestimmungsrecht ausüben zu können.

Ein Mitbestimmungsrecht bezüglich der Lohnhöhe bei leistungsbezogenen Entgelten statuiert § 87 Abs. 1 Nr. 11 BetrVG, indem es dem Betriebsrat erlaubt, bei Fragen über Bezugsgrößen einschließlich des Geldfaktors mitzubestimmen.[687] Gegenüber § 87 Abs. 1 Nr. 10 BetrVG handelt es sich hierbei um ein zusätzliches und erweitertes Mitspracherecht, welches darauf basiert, dass leistungsbezogene Entgelte, die zur Leistungssteigerung der Arbeitnehmer eingesetzt werden, diese besonders belasten. Einer solchen Leistungsvergütung ist immer auch eine Leistungsbewertung inhärent, welche nur schwer mit mathematischer Genauigkeit vorgenommen werden kann, sondern oftmals einen Beurteilungsspielraum enthält.[688]

---

683 BAG, Beschl. v. 29.02.2000 – 1 ABR 4/99, AP BetrVG 1972 § 87 Lohngestaltung Nr. 105 unter B. II. 1. b) bb) der Gründe.

684 Vgl. statt vieler GK-BetrVG/*Wiese/Gutzeit*, § 87 Nr. 10 BetrVG Rn. 834; Richardi/*Richardi*, § 87 BetrVG Rn. 752 jeweils m.w.N. aus der höchstrichterlichen Rechtsprechung.; hierbei spricht *Richardi* auch von „Verteilungsgerechtigkeit" in Abgrenzung zur „Austauschgerechtigkeit".

685 BAG, Beschl. v. 29.02.2000 – 1 ABR 4/99, AP BetrVG 1972 § 87 Lohngestaltung Nr. 105 unter B. II. 1. b) bb) der Gründe.

686 Vgl. Richardi/*Richardi*, § 87 BetrVG Rn. 777.

687 ErfK/*Kania*, § 87 BetrVG Rn. 117.

688 BAG, Beschl. v. 29.03.1977 – 1 ABR 123/74, AP BetrVG 1972 § 87 Provision Nr. 1unter IV. 3. b) der Gründe.

Provisionen hingegen, die nicht lediglich leistungsbestimmt, sondern oftmals noch an anderen Kenngrößen wie Unternehmenserfolg festgemacht werden, unterliegen nicht dem Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 11 BetrVG.[689]

Hier setzen „intelligente Systeme" bzw. evidenzbasierte Systeme an, deren Ziel es ist, mathematisch berechnete und somit spezifischere Aussagen zu gewissen Kenngrößen auszugeben. Allerdings ist zu beachten, dass diese Systeme derzeit auf Heuristik basieren und daher ebenfalls nur Annäherungswerte darstellen, die fehlerbehaftet sein können. Aus diesem Grund wäre es in diesem Zusammenhang – trotz einer wahrscheinlich höheren Präzision der Bestimmung der Kenngrößen – nicht geboten, das Mitbestimmungsrecht teleologisch für solche leistungsbezogenen Entgelte zu reduzieren.

2. Mitbestimmungsrecht aus § 94 BetrVG: Personalfragebögen, Beurteilungsgrundsätze

Nach § 94 Abs. 1 BetrVG bedürfen Personalfragebögen der Zustimmung des Betriebsrats; dieses Mitbestimmungsrecht wird in Abs. 2 für die Aufstellung allgemeiner Beurteilungsgrundsätze erweitert. Es handelt sich hierbei um ein echtes Mitbestimmungsrecht.[690]

a) Personalfragebögen

Als Fragebogen wird eine formularmäßige Zusammenfassung von Fragen, die gewisse personenbezogene Daten betreffen, verstanden, die dem Arbeitgeber ein Bild von der Person und deren Qualifikation verschaffen sollen. Personalfragebögen sind ein Mittel der Personalplanung. Bei solchen besteht allerdings immer die Gefahr, dass unzulässige Fragen gestellt werden, die das Persönlichkeitsrecht der betroffenen Bewerber verletzen könnten. Hier setzt § 94 BetrVG an, der durch die Mitbestimmung des Betriebsrats sicherstellen soll, dass der Arbeitgeber nur solche Fragen stellt,

689 So bereits *Stadler*, BB 1972, 800 (801).
690 BeckOK ArbR/*Mauer*, § 94 BetrVG Vor Rn. 1.

für die ein berechtigtes Auskunftsbedürfnis besteht.[691] Solche Fragenbögen werden in der Regel sowohl bei der Einstellung als auch bei der Aufgabenübertragung von Arbeitgebern eingesetzt. Bei ersteren hat der Betriebsrat somit ein Mitbestimmungsrecht zum Schutz von Personen, die noch nicht zur wählenden Belegschaft angehören.[692]

Aus dem Telos der Norm ergibt sich, dass auch persönliche Angaben in Arbeitsverträgen von diesem Mitbestimmungsrecht erfasst sind, da ansonsten eine Umgehungsgefahr bestehen würde.[693]

Der Betriebsrat kann nicht nur den Inhalt des Fragebogens mitbestimmen, sondern auch über die Einführung eines Fragebogens selbst.[694] Er hat jedoch kein Initiativrecht bezüglich der Einführung; § 94 BetrVG statuiert lediglich ein Zustimmungserfordernis.[695]

Umstritten ist, ob sich das Mitbestimmungsrecht auch auf die Festlegung, wofür die gewonnen Informationen verwendet[696] bzw. in welchem Zusammenhang sie eingesetzt werden dürfen sowie auf die Verwaltung der Information (Speicherfristen, Zugriffe etc.)[697] erstreckt. Teilweise wird dies mit dem Argument abgelehnt, dass sich die Grenzen der Verarbeitung aus der arbeitsvertraglichen Fürsorgepflicht und den gesetzlichen Datenschutzbestimmungen[698] ergeben, sodass hier keine erzwingbare Mitbestimmung besteht. Im Hinblick auf die Verwaltung der Informationen wird vertreten, dass das Persönlichkeitsrecht des Arbeitnehmers nicht berührt sei.[699] Wird der Sinn des Mitbestimmungsrechts, nämlich die Wahrung der Persönlichkeitsrechte der Arbeitnehmerschaft, zugrunde gelegt, so wird schnell klar, dass sich das Mitbestimmungsrecht auch auf den Ver-

---

691 BAG, Beschl. v. 21.09.1993 – 1 ABR 28/93, AP BetrVG 1972 § 94 Nr. 4 unter B. II. 1. a) der Gründe; siehe auch die Regierungsbegründung zu § 94 BetrVG, BT-Drs. IV/1786, S. 50.

692 Vgl. § 5 Abs. 1 BetrVG, wonach Bewerber nicht zum Arbeitnehmerbegriff im Sinne des BetrVG gehören; siehe auch GK-BetrVG/*Raab*, § 94 BetrVG Rn. 2.

693 Im Ergebnis ebenfalls GK-BetrVG/*Raab*, § 94 BetrVG Rn. 3.

694 *Fitting*, § 94 Rn. 9; GK-BetrVG/*Raab*, § 94 BetrVG Rn. 6; *Lützeler/Kopp*, ArbRAktuell 2015, 491 (493); einschränkend MHdB-ArbR/*Oberthür*, § 335 Zustimmung zu Personalfragebögen, Rn. 7: Mitbestimmungsrecht nur hinsichtlich konkreter Fragebögen, nicht über die Frage selbst, ob ein Arbeitgeber Personalfragebögen nutzen möchte; ebenso Richardi/*Thüsing*, § 94 BetrVG Rn. 38.

695 DKW/*Klebe*, § 94 BetrVG Rn. 2 m.w.N. aus der Rechtsprechung.

696 So *Fitting*, § 94 Rn. 9;DKW/*Klebe*, § 94 BetrVG Rn. 7; BeckOK ArbR/*Mauer*, § 94 BetrVG Rn. 3.

697 So DKW/*Klebe*, § 94 BetrVG Rn. 7.

698 MHdB-ArbR/*Oberthür*, § 335 Zustimmung zu Personalfragebögen, Rn. 7 argumentiert hier mit der engen Zweckbindung des § 26 BDSG.

699 GK-BetrVG/*Raab*, § 94 BetrVG Rn. 24 m.w.N.

wendungszweck sowie die Randbedingungen der Informationsverwaltung beziehen müssen. Bereits das geltende Datenschutzrecht zeigt deutlich, wie wichtig die Zweckbestimmung (Art. 5 Abs. 1 lit. b DSGVO) sowie die Rahmenbedingungen der Datenverarbeitung (Art. 5 Abs. 1 lit. a, c, d, e, f DSGVO) für die Wahrung der Persönlichkeitsrechte der Betroffenen sind. Das Argument, dass das Persönlichkeitsrecht bei der „Verwaltung" nicht berührt sei, läuft somit ins Leere. Gerade bei unsachgemäßer Speicherung der Daten (z.B. ohne ausreichenden Zugriffsschutz bzw. Verschlüsselung) besteht ein immenses Risiko, dass personenbezogene Daten durch Unbefugte erlangt werden können.

Dies wäre beispielsweise der Fall, wenn vertrauliche Personaldaten für alle zugänglich auf dem Unternehmenslaufwerk gespeichert würden oder durch einen Datenleck aufgrund unzureichender Absicherung gegenüber Zugriffen aus dem Internet veröffentlicht würden.

Hierdurch würde das Persönlichkeitsrecht der (betroffenen) Arbeitnehmer durch mangelnde Schutzvorkehrungen seitens des Arbeitgebers verletzt werden. Gerade hiervon will das Mitbestimmungsrecht des § 94 BetrVG schützen.[700] Es ist zwar zutreffend, dass sich die Grenzen der Verarbeitung (zumeist) aus den engen Grenzen des Datenschutzrechts ergeben; der Betriebsrat hat jedoch im Hinblick auf § 75 Abs. 2 BetrVG eine Überwachungspflicht. Dieser kann er nur sachgemäß nachkommen, wenn er auch ein rechtliches Werkzeug hat, um sicherzustellen, dass die ggf. für bestimmte Zwecke zulässigerweise erhobenen Daten nicht anderweitig in unzulässiger Weise weiterverwendet werden (z.B. indem der Arbeitgeber vom Bewerber eine [meist unwirksame] Einwilligung einholt und seine Verarbeitung auf dieser Basis rechtfertigt). Die Arbeitnehmer werden aufgrund der Befürchtung von Nachteilen in den seltensten Fällen ihren Rechten nachgehen.

Werden allgemeine (Einstellungs-)Fragebögen – auch in digitaler Form –genutzt, um mittels moderner Personalsoftware „Scores" oder Profile zu erstellen, so ist der Betriebsrat darüber genau aufzuklären, damit er sein Mitbestimmungsrecht ordnungsgemäß ausüben kann.[701] Selbiges gilt für Fragebögen im laufenden Beschäftigungsverhältnis, beispielsweise wenn

700 So auch DKW/*Klebe*, § 94 BetrVG Rn. 7.

701 Dies gilt allgemein: Sobald formalisiert personenbezogene Daten abgefragt werden wird das Mitbestimmungsrecht des § 95 BetrVG ausgelöst. Auf die Form (analog oder digital) kommt es aufgrund des Sinn und Zwecks der Norm nicht an, vgl. *Lützeler/Kopp*, ArbRAktuell 2015, 491 (493); *Raif/Swidersky*, GWR 2017, 351 (352); *Fitting*, § 94 Rn. 8 m.w.N.

die Arbeitnehmer bei der PC-Anmeldung kurze Fragen zum heutigen Gemütszustand o.ä. bekommen; auch hier werden personenbezogene Daten des einzelnen Arbeitnehmers systematisiert erfasst.[702] Wenn nur Verhaltens- und Leistungsdaten erfasst werden, unterliegen die Fragebögen nicht § 94 BetrVG, sondern § 87 Abs. 1 Nr. 6 BetrVG.[703]

b) Allgemeine Beurteilungsgrundsätze

Wesentlich relevanter für die vorliegende Arbeit ist jedoch die zweite Alternative, die ein Mitbestimmungsrecht für die Aufstellung allgemeiner Beurteilungsgrundsätze statuiert. Solche sind im Rahmen digitaler Personalbewertung (z.B. in Form von Profiling oder Scoring) die Grundlage jeder Berechnung. Ohne festlegte Kriterien kann keine (objektive) Berechnung und Bewertung erfolgen. So begründete bereits die Regierung das Mitbestimmungsrecht in ihrem Entwurf damit, dass gerade in diesem Bereich eine „Objektivierung erstrebenswert" ist.[704] Ein weiterer wesentlicher Faktor, der diesem Mitbestimmungsrecht innewohnt, ist, dass die internen Entwicklungs- und Berufschancen durch die Bewertung der Leistung wesentlich beeinflusst werden.[705]

Unter Beurteilungsgrundsätzen werden allgemeine Richtlinien verstanden, nach denen Leistung und Verhalten der Arbeitnehmer bewertet werden.[706] Sie sollen eine Bewertung des Verhaltens oder der Leistung von Arbeitnehmern objektivieren und vereinheitlichen, um somit eine Vergleichbarkeit herzustellen.[707] Ebenfalls können hierdurch Personalentwicklungs- und -fördermaßnahmen transparenter und nachvollziehbarer eingesetzt werden.[708]

Die Richtlinien müssen nicht verbindlich sein, sondern es reicht aus, wenn bestimmte Kriterien als Orientierungshilfe für die Bewertung von

---

702 MHdB-ArbR/*Oberthür*, § 335 Zustimmung zu Personalfragebögen, Rn. 5.
703 Richardi/*Thüsing*, § 94 BetrVG Rn. 10; MHdB-ArbR/*Oberthür*, § 335 Zustimmung zu Personalfragebögen, Rn. 5.
704 BT-Drs. IV/1786, S. 50.
705 GK-BetrVG/*Raab*, § 94 BetrVG Rn. 4.
706 DKW/*Klebe*, § 94 BetrVG Rn. 32.
707 BAG, Beschl. v. 17.03.2015 – 1 ABR 48/13, NZA 2015, 885 (887) Rn. 25; Beschl. v. 14.01.2014 – 1 ABR 49/12, NZA-RR 2014, 356 Rn. 20 mit Verweis auf die Gesetzesbegründung, BT-Drs. VI/1786, S. 50; Beschl. v. 23.10.1984 – 1 ABR 2/83, NZA 1985, 224 (227) = BAGE 47, 96 unter B. II. 5. b).
708 DKW/*Klebe*, § 94 BetrVG Rn. 34.

Arbeitnehmern festgelegt werden, wie beispielsweise Aufgabenbeschreibungen für die jeweilige Stelle als Teil des Beurteilungsverfahrens.[709]

Bei § 94 Abs. 2 BetrVG handelt es sich wie bei Abs. 1 um ein Zustimmungserfordernis, d.h. der Betriebsrat kann nicht die Aufstellung von allgemeinen Beurteilungsgrundsätzen vom Arbeitgeber verlangen.[710] Analog zum Mitbestimmungsrecht bei Fragebögen hat der der Betriebsrat auch bei der Einführung allgemeiner Beurteilungsgrundsätze mitzubestimmen,[711] ebenso in welchem Rahmen diese angewandt werden. Wie in § 94 Abs. 1 BetrVG spielt auch hier die Zweckbestimmung eine entscheidende Rolle für die Relevanz einzelner Beurteilungsmerkmale; nur bei begründetem Bedürfnis für die Arbeitsaufgabe dürfen die Kriterien zur Beurteilung herangezogen werden.[712] Das Mitbestimmungsrecht erstreckt sich auch auf die Ausgestaltung des Beurteilungsverfahrens.[713]

Im Bereich des Profiling und Scoring ist es zwingend erforderlich, dass eine Bewertungsmatrix erstellt wird. Werden Mitarbeiter bewertet, so handelt es sich um mitbestimmungspflichtige Beurteilungsgrundsätze.[714] Bewerbungsmanagementsysteme, die Bewerbungen automatisch auswerten, fallen somit ebenfalls unter diesen Tatbestand.[715] Das Mitbestimmungsrecht erstreckt sich ferner darauf, ob die Bewertung vollautomatisch erfolgt oder eine Person dazwischengeschaltet wird.[716] Letzteres kann aufgrund Art. 22 DSGVO aus datenschutzrechtlicher Hinsicht zwingend sein.[717]

Nicht von der Mitbestimmung erfasst ist allerdings die Anwendung der Beurteilungsgrundsätze im Einzelfall.[718]

---

709 Vgl. BAG, Beschl. v. 14.01.2014 – 1 ABR 49/12, NZA-RR 2014, 356 (357) Rn. 21; Voraussetzung ist allerdings, dass diese als Funktionsbeschreibung Grundalge des Beurteilungsverfahrens werden, vgl. Richardi/*Thüsing*, § 94 BetrVG Rn. 59.

710 BAG, Beschl. v. 23.03.2010 – 1 ABR 81/08, NZA 2011, 811 (812 f.) Rn. 20.

711 Dagegen MHdB-ArbR/*Oberthür*, § 336 Zustimmung zu allgemeinen Beurteilungsgrundsätzen, Rn. 6.

712 Vgl. DKW/*Klebe*, § 94 BetrVG Rn. 36. Dies entspricht im Übrigen in datenschutzrechtlicher Hinsicht auch dem Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c) DSGVO.

713 BAG, Beschl. v. 17.03.2015 – 1 ABR 48/13, NZA 2015, 885 Os. 2; MHdB-ArbR/*Oberthür*, § 336 Zustimmung zu allgemeinen Beurteilungsgrundsätzen, Rn. 3.

714 So auch DKW/*Klebe*, § 94 BetrVG Rn. 38, 40.

715 Richardi/*Thüsing*, § 94 BetrVG Rn. 58.

716 Richardi/*Thüsing*, § 94 BetrVG Rn. 62.

717 Siehe hierzu **D. § 1 V. 3**.

718 Allg. M., vgl. statt aller MHdB-ArbR/*Oberthür*, § 336 Zustimmung zu allgemeinen Beurteilungsgrundsätzen, Rn. 5 m.w.N.

Wird im Rahmen der Bewerberauswahl ein Algorithmus eingesetzt, der die Bewerber nach bestimmten Kriterien (aus)sortiert, besteht auch ein Mitbestimmungsrecht nach § 95 BetrVG, da eine Auswahlrichtlinie zugrunde liegt (dazu sogleich).[719] Nicht der Mitbestimmung unterliegt hingegen die Aussortierung des konkreten Bewerbers, da dies eine (personelle) Einzelmaßnahme darstellt. Letzteres ist ein Anwendungsfall von § 99 Abs. 1 BetrVG.[720]

3. Mitbestimmungsrecht aus § 95 BetrVG: Auswahlrichtlinien

Nach § 95 Abs. 1 BetrVG bedürfen Richtlinien über die personelle Auswahl bei Einstellungen, Versetzungen, Umgruppierungen und Kündigungen (sog. *Auswahlrichtlinien*) der Zustimmung des Betriebsrats. In Betrieben mit mehr als 500 Arbeitnehmern kann der Betriebsrat nach Abs. 2 die Aufstellung von Richtlinien über die bei den genannten Maßnahmen zu beachtenden fachlichen und persönlichen Voraussetzungen und sozialen Gesichtspunkte verlangen. Das Mitbestimmungsrecht bezieht sich sowohl auf die inhaltliche Ausgestaltung als auch die Frage der Einführung und Anwendung überhaupt.[721]

Unter einer Auswahlrichtlinie im Sinne der Vorschrift werden Grundsätze verstanden, die zu berücksichtigen sind, „*wenn bei beabsichtigten personellen Einzelmaßnahmen, für die mehrere Arbeitnehmer oder Bewerber in Betracht kommen, zu entscheiden ist, welchen gegenüber sie vorgenommen werden*“[722]. Dem Arbeitgeber muss jedoch auch mit solchen Richtlinien ein gewisser Beurteilungsspielraum verbleiben, da ansonsten nicht mehr von einer „Richtlinie“ gesprochen werden kann.[723] Je differenzierter jedoch die Auswahlkriterien der Richtlinie sind, desto mehr darf der Ermessens-

719 *Göpfert/Dußmann*, NZA-Beilage 2016, 41 (45); *Lützeler/Kopp*, ArbRAktuell 2015, 491 (493); *Fitting*, § 95 Rn. 11.

720 Auf § 99 BetrVG wird – da es sich hier um ein Mitbestimmungsrecht bei personellen Einzelmaßnahmen handelt – im Rahmen dieser Arbeit nicht näher eingegangen.

721 MHdB-ArbR/*Oberthür*, § 337 Mitbestimmung bei Auswahlrichtlinien, Rn. 20.

722 St. Rspr; vgl. statt vieler BAG, Beschl. v. 26.07.2005 – 1 ABR 29/04, NZA 2005, 1372; Beschl. v. 10.12.2002 – 1 ABR 27/01, BeckRS 2002, 41197 = BAGE 104, 187 unter B. III. 3. a) m.w.N.

723 BAG, Beschl. v. 27.10.1992 – 1 ABR 4/92, NZA 1993, 607 (610) m.w.N.: So handelt es sich beispielsweise auch bei einem Punktesystem noch um eine Auswahlrichtlinie, sofern dem Arbeitgeber ein Entscheidungsspielraum verbleibt. Unerheblich ist dabei, dass es Fälle geben kann, in denen das Auswahlermessen

spielraum des Arbeitgebers eingegrenzt werden. Undifferenzierte Kriterien führen öfters zu falschen Ergebnissen, die im Einzelfall noch vom Arbeitgeber korrigierbar sein müssen. Ansonsten wären die Ergebnisse solcher Auswahlrichtlinien nicht mehr sachgerecht.[724] Aus diesem Grund müssen die Kriterien auch angemessen gewichtet werden.[725]

Sinn und Zweck ist es, die jeweilige Personalentscheidung zu versachlichen und somit für den Betroffenen durchschaubarer zu machen.[726] Für den Arbeitnehmer soll transparent sein, weshalb er und nicht ein anderer von einer Maßnahme betroffen ist.[727] Die Mitbestimmung des Betriebsrats hieran wird damit begründet, dass dieser im Sinne der Arbeitsnehmer Einfluss nehmen kann unter welchen fachlichen und persönlichen Voraussetzungen solche Einzelmaßnahmen erfolgen sollen. Es besteht ein legitimes Interesse der Arbeitnehmerschaft, dass die Kriterien billig und angemessen sind.[728]

Hieraus resultiert die in Abs. 2 nochmals verdeutlichte (allgemeine) Voraussetzung, dass Kriterien der Auswahlrichtlinien die für die jeweilige personelle Auswahl maßgeblichen fachlichen, persönlichen oder sozialen Gesichtspunkte sein müssen.[729]

Auswahlrichtlinien dürften nicht mit Stellenbeschreibungen oder Anforderungsprofilen verwechselt werden. Diese unterliegen nicht der Mitbestimmung, da sie stellenbezogenen sind und sich nicht auf einzelne Arbeitnehmer beziehen; bezüglich solcher besteht lediglich eine Unterrichtungspflicht nach § 92 Abs. 1 BetrVG.[730] Das Anforderungsprofil ist der Personalauswahl vorgelagert. Entspricht ein Arbeitnehmer nicht den Anforderungen, so kommt er bereits überhaupt nicht für diese Stelle in

---

durch das Punktesystem bereits soweit beschränkt ist, dass der Arbeitgeber im konkreten Einzelfall kein Ermessen mehr hat.

724 BAG, Beschl. v. 27.10.1992 – 1 ABR 4/92, NZA 1993, 607 (613).

725 MHdB-ArbR/*Oberthür*, § 337 Mitbestimmung bei Auswahlrichtlinien, Rn. 14.

726 BT-Drs. IV/1786, S. 50.

727 BAG, Beschl. v. 26.07.2005 – 1 ABR 29/04, NZA 2005, 1372 (1373); Beschl. v. 10.12.2002 – 1 ABR 27/01, BeckRS 2002, 41197 = BAGE 104, 187 unter B. III. 3. a) m.w.N. aus der Rspr.

728 BAG, Beschl. v. 27.10.1992 – 1 ABR 4/92, NZA 1993, 607 (611).

729 Insofern gelten die Kriterien auch für Betriebe mit weniger als 500 AN; vgl. BAG, Beschl. v. 26.07.2005 – 1 ABR 29/04, NZA 2005, 1372 (1373) m.N.; einschränkend noch auf Vorschläge des Betriebsrats Beschl. v. 10.12.2002 – 1 ABR 27/01, BeckRS 2002, 41197 = BAGE 104, 187 unter B. III. 3. a); aus der Literatur *Fitting*, § 95 Rn. 18.

730 MHdB-ArbR/*Oberthür*, § 337 Mitbestimmung bei Auswahlrichtlinien, Rn. 9 m.w.N.

Betracht und werden in einer eventuellen Auswahlentscheidung nicht berücksichtigt; er unterliegt also gar keiner Auswahl.[731]

Werden mit Hilfe von Personalmanagement-Software-Tools daher Vorschläge für bestimmte Stellen erstellt, Bewerber sortiert, Vorschläge für Versetzungen oder Umgruppierungen erstellt oder gar eine „Abschussliste" generiert, so arbeitet im Hintergrund ein definierter Algorithmus. Dieser muss zuvor von einem Programmierer oder dem Arbeitgeber mit entsprechenden Daten gefüttert worden sein, in dessen Rahmen auch festgelegt worden sein muss, welche Daten überhaupt als Grundlage für das Tool herangezogen werden und welche Gewichtung die jeweiligen Daten haben. Letzteres kann mitunter variieren, wenn KI bzw. neuronale Netze eingesetzt werden, die sich selbst optimieren.[732] Jedenfalls besteht sowohl bei der Einführung als auch bei der Anwendung ein Mitbestimmungsrecht des Betriebsrats.[733] Nicht nur aufgrund § 75 Abs. 2 BetrVG hat der Betriebsrat – insbesondere bei selbstoptimierenden Systemen – darüber zu wachen, dass die Gewichtung der Kriterien weiterhin sachgerecht und für den Arbeitnehmer nachvollziehbar bleibt. Dies kann aufgrund der Intransparenz komplexer neuronaler Netze zur Quadratur des Kreises führen. Arbeitgeber sind allerdings bereits aus datenschutzrechtlichen Gründen dazu verpflichtet, solche Systeme transparent zu halten.[734] Zu beachten ist ferner, dass ein solches System im Rahmen des Lernprozesses nicht neue, nicht stellenrelevante Merkmale, als Grundlage der Bewertung heranzieht oder gar schafft. Hier müssen die Kriterien des § 95 Abs. 2 BetrVG beachtet werden. Der Anwendungsbereich künstlicher Intelligenz im Auswahlverfahren ist daher sowohl aus datenschutzrechtlicher als auch betriebsverfassungsrechtlicher Sicht aufgrund der Transparenz-Probleme zum jetzigen Zeitpunkt noch als gering einzustufen.

4. Unterrichtungs- und Beratungspflicht bei Maßnahmen der Personalplanung, § 92 Abs. 1 BetrVG

§ 92 Abs. 1 BetrVG bestimmt, dass der Arbeitgeber den Betriebsrat über die Personalplanung anhand von Unterlagen rechtzeitig und umfassend

731 GK-BetrVG/*Raab*, § 95 BetrVG Rn. 38 m.w.N.
732 Siehe hierzu **C. § 2 II. 2.**
733 *Lützeler/Kopp*, ArbRAktuell 2015, 491 (493); *Göpfert/Dußmann*, NZA-Beilage 2016, 41 (45); *Fitting*, § 95 Rn. 11.
734 Vgl. Art. 5 Abs. 1 lit. a DSGVO.

zu unterrichten hat. Diese Unterrichtung umfasst insbesondere den gegenwärtigen und künftigen Personalbedarf, die sich daraus ergebenden personellen Maßnahmen einschließlich der geplanten Beschäftigung von Personen, die nicht in einem Arbeitsverhältnis stehen, sowie Maßnahmen der Berufsbildung. S. 2 statuiert eine Beratungspflicht, wonach der Arbeitgeber mit dem Betriebsrat über Art und Umfang der erforderlichen Maßnahmen und über die Vermeidung von Härten zu beraten hat. Das Beratungsrecht ist enger als das Informationsrecht, wie sich bereits aus dem einschränkenden Wortlaut des S. 2 ergibt. Nur im Hinblick auf die mit der Planung verbundenen personellen Maßnahmen muss der Arbeitgeber mit dem Betriebsrat beraten.[735]

Im Mittelpunkt der hiesigen Betrachtung steht das Tatbestandmerkmal der Personalplanung, welchem aufgrund der umfassenden Reichweite eine besondere Bedeutung zukommt und daher auch für die Einführung von People Analytics-Maßnahmen einschlägig sein könnte. Im Rahmen der Personalplanung kann der Betriebsrat nach § 92 Abs. 2 BetrVG dem Arbeitgeber Vorschläge für die Einführung und Durchführung machen.

Die bereits untersuchten Mitbestimmungsrechte in §§ 94, 95 BetrVG betreffen Maßnahmen, die aus der Personalplanung resultieren oder für diese erforderlich sind, der Planung im zeitlichen Verlauf also nachgelagert sind.

Wie eingangs dargestellt setzen Arbeitgeber in diesem Bereich immer häufiger Software-Tools ein, um dem konkreten Personalbedarf, die Fluktuationsquote, die Qualifizierung von Arbeitnehmern etc. zu berechnen. Auch Netzwerkgraphen, die darstellen sollen, welche Arbeitnehmer mit welchen besonders häufig kommunizieren, können zur Personalplanung genutzt werden.

Die Personalplanung umschließt also Faktoren des innerbetrieblichen sowie des außerbetrieblichen Arbeitsmarktes sowie alle dazugehörigen Maßnahmen.[736] Der Begriff wird vom Gesetz selbst nicht definiert. Nach der Gesetzesbegründung soll § 92 BetrVG sicherstellen, dass der Betriebsrat rechtzeitig über die betriebliche personelle Lage sowie deren Entwicklung informiert wird und hierzu auch umfassende Unterlagen erhält. Zur Vermeidung von Härten soll der Betriebsrat mit dem Arbeitgeber daher frühzeitig beraten.[737] In der Rechtsprechung bestand die Notwendigkeit einer Definition: Hiernach ist die Personalplanung jede Planung, die sich

735 BAG, Beschl. v. 06.11.1990 – 1 ABR 60/89, NZA 1991, 358 (362) unter 3. a).
736 *Fitting*, § 92 Rn. 6 ff.
737 BT-Drs. IV/1786, S. 50.

auf den gegenwärtigen und künftigen Personalbedarf in quantitativer und qualitativer Hinsicht, auf dessen Deckung im weiteren Sinne und auf den abstrakten Einsatz der personellen Kapazität bezieht. Umfasst wird die Personalbedarfsplanung, die Personalbeschaffungsplanung, die Planung des Personaleinsatzes sowie der -entwicklung.[738]

Entschließt sich ein Arbeitgeber beispielsweise dazu, People Analytics für ein evidenzbasiertes Personalmanagement einzusetzen, hat er den Betriebsrat rechtzeitig darüber zu unterrichten. „Rechtzeitig" ist eine Unterrichtung dann, wenn sie so frühzeitig erfolgt, dass der Betriebsrat noch Einfluss auf die Planung nehmen kann.[739] Eine Beratungspflicht besteht hingegen nach § 92 S. 2 BetrVG erst dann, wenn sich aus der Planung konkrete personelle Maßnahmen ergeben.[740]

Dies wird bei der Einführung von People Analytics dann der Fall sein, wenn diese Analysen auch Grundlage für Personalentscheidungen werden sollen, sei es im Rahmen von personellen Einzelmaßnahmen in Form von Zielvereinbarungen, Versetzungen, Einstellungen, Kündigungen usw. oder auch von abteilungs- oder unternehmensübergreifenden Maßnahmen. Beispiele für Letztere könnten sein, dass durch die Analyse ein Personalmangel oder -überschuss festgestellt wird oder sonstige Faktoren, die der Unternehmer aus dem Weg räumen möchte (z.B. hohe Krankheitsraten durch mangelnde Sicherheitsschulungen, unkoordinierter Einsatz von Personal im Außendienst).

5. Unterrichtungs- und Beratungspflicht bei der Planung von technischen Anlagen, § 90 BetrVG

§ 90 Abs. 1 Nr. 2 BetrVG verpflichtet den Arbeitgeber, bei der Planung technischer Anlagen den Betriebsrat rechtzeitig zu unterrichten. Gemäß § 90 Abs. 2 BetrVG hat der Arbeitgeber mit dem Betriebsrat die vorgesehenen Maßnahmen und ihre Auswirkungen auf die Arbeitnehmer, insbesondere auf die Art ihrer Arbeit sowie die sich daraus resultierenden Anforderungen an die Arbeitnehmer so rechtzeitig zu beraten, dass Vorschläge

738 St. Rspr.; vgl. statt vieler BAG, Beschl. v. 23.03.2010 – 1 ABR 81/08, NZA 2011, 811 (813) Rn. 23; Beschl. v. 06.11.1990 – 1 ABR 60/89, NZA 1991, 358 (359 f.) m.w.N. aus der Kommentarliteratur.

739 ErfK/*Kania*, § 92 BetrVG Rn. 8.

740 BAG, Beschl. v. 06.11.1990 – 1 ABR 60/89, NZA 1991, 358 (362) unter 3. a).

und Bedenken des Betriebsrats bei der Planung berücksichtigt werden können.

Unter den Begriff technische Anlage fallen alle technischen Geräte und Maschinen, die unmittelbar oder mittelbar dem Arbeitsablauf dienen, von Bedeutung für die Arbeitsumgebung sein oder sich sonst auf die Arbeitsplatzgestaltung auswirken könnten.[741] Hierunter fallen auch EDV-Anlagen oder die Umstellung einer Personalabrechnung vom Offline- auf den Online-Betrieb[742], aber auch der Anschluss von Arbeitsplätzen an das Internet oder die Umstellung auf Cloud-Computing.[743] Ein Personalinformationssystem oder eine People Analytics-Software ist daher eine technische Anlage i.S.v. § 90 Abs. 1 Nr. 2 BetrVG.[744]

Ein Beratungsrecht nach § 90 Abs. 1 Nr. 3 BetrVG besteht darüber hinaus, wenn bspw. im Bereich des Personalmanagements neue IT-Systeme eingeführt werden oder bestehende umfassend modifiziert werden.[745]

Der Informationsanspruch umfasst auch Informationen zum Aufbau und zur Funktions- und Wirkungsweise dieser IT-Systeme, so mitunter auch die eingesetzten Algorithmen bzw. deren grundlegende Logik und „Lernstrukturen".[746]

6. Unterrichtungs- und Beratungspflicht bei Betriebsänderungen nach § 111 BetrVG

Bei größeren Maßnahmen im Bereich des Personalwesens kommt auch eine Unterrichtungs- und Beratungspflicht nach § 111 BetrVG in Betracht. Dies ist dann der Fall, wenn es sich um ein Unternehmen mit in der Regel mehr als 20 wahlberechtigten Arbeitnehmern handelt und es sich um eine

741 Richardi/*Annuß*, § 90 BetrVG Rn. 10.
742 Beispiele aus BeckOK ArbR/*Werner*, § 90 BetrVG Rn. 3 m.w.N.
743 *Wedde*, Automatisierung im Personalmanagement - arbeitsrechtliche Aspekte und Beschäftigtendatenschutz, <*algorithmwatch.org/de/gutachten-arbeitsrecht-datenschutz-wedde/*>, S. 23.
744 So für das Personalinformationssystem *Kreitner/Weil/Schlegel*, Stichwort "Personalinformationssystem", in: Küttner, Personalbuch 2020, Rn. 7.
745 *Wedde*, Automatisierung im Personalmanagement - arbeitsrechtliche Aspekte und Beschäftigtendatenschutz, <*algorithmwatch.org/de/gutachten-arbeitsrecht-datenschutz-wedde/*>, S. 23.
746 *Wedde*, Automatisierung im Personalmanagement - arbeitsrechtliche Aspekte und Beschäftigtendatenschutz, <*algorithmwatch.org/de/gutachten-arbeitsrecht-datenschutz-wedde/*>, S. 25.

Betriebsänderung handelt, die wesentliche Nachteile für die Belegschaft oder erhebliche Teile der Belegschaft zur Folge haben können.

Was unter einer Betriebsänderung zu verstehen ist, ist in § 111 S. 3 BetrVG abschließend[747] aufgezählt. Im Kern muss es sich hierbei um eine wesentliche Änderung der Gestaltung des Betriebs handeln.[748] Bei der Einführung eines evidenzbasierten Managements bzw. moderner Personalmanagement-Maßnahmen wie People Analytics, kommen die Nrn. 4 und 5 in Betracht. § 111 S. 3 Nr. 4 BetrVG statuiert, dass unter einer Betriebsänderung *grundlegende Änderungen der Betriebsorganisation, des Betriebszwecks oder der Betriebsanlagen* zu verstehen sind, während Nr. 5 – etwa gleich unspezifisch – die *Einführung grundlegend neuer Arbeitsmethoden und Fertigungsverfahren* als Betriebsänderung definiert.

a) Der Tatbestand des § 111 S. 3 Nr. 4 BetrVG

So wurde in der früheren Rechtsprechung die Umstellung des Rechnungswesens unter Einsatz von Datensichtgeräten als grundlegende Änderung der Betriebsanlagen angesehen, wenn diese im Vergleich zu den Anlagen des gesamten Betriebs von erheblicher Bedeutung sind.[749] In der sog. *Datensichtgeräte*-Entscheidung des BAG[750] hatten sich die Erfurter Richter damit auseinanderzusetzen, ob bei der Einführung neuer Technologien der Tatbestand des § 111 BetrVG ausgelöst werden kann. Im entschiedenen Fall sollte die bis dahin elektronisch geführte Buchhaltung derart modernisiert werden, dass die Buchungsdaten der Betriebe in Deutschland nicht mehr postalisch übermittelt, sondern über ein Satellitensystem direkt nach Houston (USA) übermittelt werden. Hierzu sollten im Betrieb in Deutschland 70 neue Datensichtgeräte installiert werden, die per Satellit an den Zentralrechner in den Vereinigten Staaten angeschlossen sind. Vom Betriebsrat wurde vorgetragen, dass durch diese Rationalisierung Arbeitsplätze entfallen oder in ihrer Werthaltigkeit gemindert würden. Es sei mit Versetzungen und einer gravierenden Änderung der Arbeitsbedingungen für etwa 125 bis 150 Mitarbeiter zu rechnen. Im Mittelpunkt der

747 Str.; vgl. statt vieler Richardi/*Annuß*, § 111 BetrVG Rn. 41 m.w.N.
748 Richardi/*Annuß*, § 111 BetrVG Rn. 40.
749 BAG, Beschl. v. 26.10.1982 – 1 ABR 11/81, BAGE 41, 92 = SAE 1984, 275 m. Anm. Buchner – Datensichtgeräte.
750 BAG, Beschl. v. 26.10.1982 – 1 ABR 11/81, BAGE 41, 92 = SAE 1984, 275 m. Anm. Buchner – Datensichtgeräte.

Entscheidung stand der Umstand, dass etwa 75 Mitarbeiter zuvor nicht mit EDV-Geräten gearbeitet hatten, sondern lediglich Formulare von Hand EDV-gerecht ausgefüllt haben. Hierdurch waren mehr als 5 % und somit ein „erheblicher Teil" der Belegschaft betroffen. Es müsse jedoch – so das BAG – überprüft werden, ob es sich hierdurch schon um eine „grundlegende Änderung" von Betriebsanlagen handle; hier komme es auf den Grad der technischen Änderung an.

Da bei der Einführung von neuen Technologien in der Datenverarbeitung (z.B. durch moderne HR-Tools oder Big-Data-People-Analytics-Verfahren gerade keine Anlagen geändert werden, sondern lediglich die Software auf dem Server nach einem anderen Prinzip die Daten auswertet und hierdurch die betroffenen Arbeitnehmer ggf. eine andere Eingabemaske und andere Auswertungsmöglichkeiten zu Gesicht bekommen, handelt es sich noch nicht um eine Betriebsänderung im Sinne von § 111 S. 3 Nr. 4 BetrVG.[751] Eine Änderung der Betriebsanlagen findet nicht statt. Vielmehr ist dies mit einer Aktualisierung der Benutzersoftware zu vergleichen, die eben – wie oft bei Aktualisierungen – schlicht neue Funktionen beinhaltet und eine verbesserte Produktivität hierdurch verspricht.[752]

b) Einführung grundlegend neuer Arbeitsmethoden (§ 111 S. 3 Nr. 5 BetrVG)?

Die Einführung moderner Auswertungstechnologien im HR-Bereich könnte allerdings dazu führen, dass das Personalmanagement aufgrund der neu vorliegenden Daten nunmehr evidenzbasiert erfolgt. Die „klassische HR-Arbeit" wandelt sich zu einer rein datenbasierten Arbeit wandelt, mit der Folge, dass auch neue Anforderungen an die Stellen in diesem Bereich gestellt werden. Statt Personalsachbearbeiter werden Data Scientists eingestellt, die Muster in den Daten erkennen bzw. die eingesetzte Software optimieren sollen. Hierbei könnte an eine Betriebsänderung durch

751 Vgl. aber *Wedde*, Automatisierung im Personalmanagement - arbeitsrechtliche Aspekte und Beschäftigtendatenschutz, <*algorithmwatch.org/de/gutachten-arbeitsrecht-datenschutz-wedde/*>, S. 26: Im Einzelfall kann es als eine Betriebsänderung angesehen werden.

752 Vgl. zur Ersatzbeschaffung von Maschinen Richardi/*Annuß*, § 111 BetrVG Rn. 50; siehe zur tiefgreifenden Änderung oder Einführung neuer EDV-Software aber *Fitting*, § 111 Rn. 95.

die Einführung grundlegend neuer Arbeitsmethoden nach § 111 S. 3 Nr. 5 BetrVG gedacht werden.[753]

Die Tatbestände der Nrn. 4 und 5 überschneiden sich wesentlich. Der Unterschied ist im Objekt der Veränderung zu sehen: Während in Nr. 4 die Arbeitsmittel im Vordergrund stehen, sind es bei Nr. 5 die Arbeitnehmer bzw. der Einsatz der menschlichen Arbeitskraft.[754]

Unter dem Begriff Arbeitsmethode ist die „jeweilige Art, eine Arbeit systematisch abzuwickeln"[755] zu verstehen, wobei hierunter die Strukturierung des Arbeitsablaufs des einzelnen Arbeitnehmers und der Einsatz technischer Hilfsmittel darunterfallen, kurzum wie die Arbeit zur Erfüllung der gestellten Arbeitsaufgabe geleistet werden muss.[756]

Fraglich ist, wann es sich um „grundlegend neue" Arbeitsmethoden handelt. Für die Bestimmung des Begriffs müssen im Zweifel das Ausmaß der nachteiligen Auswirkungen der Änderungen herangezogen werden.[757] Es ist also eine qualitative Bewertung erforderlich, wobei die Zahl der von ihr betroffenen Arbeitnehmer sowie das Gewicht der Auswirkungen auf die Beschäftigten maßgebliche Bewertungskriterien sind.[758]

Für die hier behandelten Beispiele der Einführung von modernen Tools im Bereich HR wie Netzwerk-Graphen, Big-Data-Auswertungen von Personaldaten oder People Analytics kann keine pauschale Aussage getroffen werden, da es auf den einzelnen Betrieb ankommt. Hochtechnisierte Betriebe, die bereits teilweise solche Tools nutzen und lediglich neue Tools einsetzen, um die Funktionalitäten zu erweitern, werden keine grundlegenden Veränderungen der Arbeitsmethoden wahrnehmen. Handelt es sich aber um einen Betrieb mit einem sehr klassischen HR-Management (beispielsweise, wo Personalakten noch handgeführt werden), so kann die Einführung von People Analytics oder Big-Data-Auswertungsverfahren durchaus zu grundlegend neuen Arbeitsmethoden führen – je nach Größe der Personalabteilung. In diesem Fall würden neue Anforderungen an die vorhandenen Stellen gestellt sowie das Berufsbild des HR-Verantwortli-

753 So auch *Wedde*, Automatisierung im Personalmanagement - arbeitsrechtliche Aspekte und Beschäftigtendatenschutz, <*algorithmwatch.org/de/gutachten-arbeitsrecht-datenschutz-wedde/*>, S. 26.

754 *Fitting*, § 111 Rn. 97 m.N.

755 BAG, Beschl. v. 22.03.2016 – 1 ABR 12/14, NZA 2016, 894 (896) Rn. 19.

756 BAG, Beschl. v. 22.03.2016 – 1 ABR 12/14, NZA 2016, 894 (896) Rn. 19.

757 *Buchner*, ZfA 1988, 449 (455); BAG, Beschl. v. 22.03.2016 – 1 ABR 12/14, NZA 2016, 894 Rn. 21.

758 BAG, Beschl. v. 22.03.2016 – 1 ABR 12/14, NZA 2016, 894 Rn. 21; *Fitting*, § 111 Rn. 101.

chen verändert. Es bedürfte u.U. Schulungen in den Bereichen IT sowie Datenauswertung. Da es sicherlich im Betrieb Beschäftigte gibt, die Probleme mit hochtechnisierter Software haben, könnte es für diese gewichtige Auswirkungen bis hin zur Kündigung haben.

Aus diesem Grund müssen Unternehmen, die solche Technologien einsetzen möchten, vorab die Personalstruktur der Personalabteilung unter die Lupe nehmen sowie die vorhandene IT-Landschaft mit der künftigen vergleichen, um bewerten zu können, inwiefern die Unterrichtungs- und Beratungspflicht des § 111 BetrVG ausgelöst wird. Durch die grundlegend andere Herangehensweise bei Big-Data-Applikationen sowie viele Erkenntnisse, die bei sehr klassischem HR-Management nicht gewonnen werden können, ist eine Betriebsänderung alles andere als abwegig, insbesondere in Unternehmen mit Fokus auf Human Ressource Management.

III. Verpflichtung zum Schutz und zur Förderung des Persönlichkeitsrechts der Arbeitnehmer aus § 75 Abs. 2 BetrVG

→ *siehe bereits* D. § 2 II. 1. b) ee) „*Grenzen des Mitbestimmungsrechts*“

IV. Allgemeine Unterrichtungspflicht / Auskunftsbegehren des Betriebsrats, § 80 Abs. 2 BetrVG

Nach § 80 Abs. 2 BetrVG hat der Betriebsrat gegen den Arbeitgeber den Anspruch, rechtzeitig und umfassend unterrichtet zu werden, damit er seine Aufgaben ordnungsgemäß durchführen kann. Hierzu sind dem Betriebsrat auch auf Verlangen jederzeit die zur Durchführung seiner Aufgaben erforderlichen Unterlagen zur Verfügung zu stellen (§ 80 Abs. 2 S. 2 BetrVG). Nach § 80 Abs. 3 BetrVG darf der Betriebsrat – wenn erforderlich – nach näherer Vereinbarung mit dem Arbeitgeber Sachverständige hinzuziehen. Die Kosten hierfür hat nach § 40 Abs. 1 BetrVG der Arbeitgeber zu tragen.

Im Bereich des Datenschutzes hat der Betriebsrat nicht nur nach § 75 Abs. 2 BetrVG, sondern auch nach § 80 Abs. 1 Nr. 1 BetrVG zu überwachen, dass der Arbeitgeber die geltenden Datenschutzgesetze einhält. Hierbei sind dem Betriebsrat nach § 80 Abs. 2 BetrVG die notwendigen Unterlagen zur Verfügung zu stellen, damit er seine Aufgabe ordnungsgemäß durchführen kann. Datenschutzrechtlich kann dies insofern problematisch sein, dass die Weitergabe personenbezogener Arbeitnehmerdaten nicht be-

reits durch § 80 Abs. 2 S. 2 Hs. 2 BetrVG spezialgesetzlich geregelt ist, sondern an der allgemeinen Befugnisnorm des § 26 Abs. 1 BDSG zu messen ist. Die Lösung dieses Problems ergibt sich aber bereits aus § 26 Abs. 1 S. 1 a.E. BDSG, wonach die Verarbeitung personenbezogener Beschäftigtendaten zulässig ist, wenn dies zur Ausübung der Pflichten der Interessensvertretung der Beschäftigten erforderlich ist.[759]

Der Arbeitgeber kann die Herausgabe von Unterlagen und Informationen auch nicht mit dem Argument des Betriebs- oder Geschäftsgeheimnisses verweigern. Nach § 79 BetrVG haben bei solchen Informationen die Mitglieder und Ersatzmitglieder des Betriebsrats die Pflicht, solche Informationen nicht zu offenbaren oder zu verwerten.[760]

V. Zwischenergebnis

Wie sich aus der Untersuchung zeigt, hat der Betriebsrat umfassende Mitbestimmungsrechte bei der Einführung neuer HR-Technologien; insbesondere bestehen vielerorts Initiativrechte. Arbeitgeber sind hingegen gehalten, bereits frühzeitig mit dem Betriebsrat über geplante Maßnahmen im Personalbereich zu verhandeln (§ 92 und ggf. § 111 BetrVG). Etwaige Betriebsvereinbarungen können hierbei legitimierende Wirkung für die Datenverarbeitung haben (§ 26 Abs. 4 BDSG), wobei die Grenzen des Art. 88 Abs. 2 sowie des § 75 Abs. 2 BetrVG zu beachten sind. In § 26 Abs. 6 BDSG wird nochmals vom Gesetzgeber klargestellt, dass die datenschutzrechtlichen Bestimmungen die des BetrVG nicht verdrängen. Da die Akzeptanz von People-Analytics-Maßnahmen – wie Untersuchungen zeigen[761] – bei der erfolgreichen Umsetzung eine große Rolle spielt, ist es daher nicht nur aus rechtlicher Sicht geboten, den Betriebsrat (und ggf. die gesamte Belegschaft) schon früh „ins Boot zu holen". Gelingt es dem Arbeitgeber durch offene Kommunikation, seine Beschäftigten zu überzeugen, dass *People Analytics* nicht nur zur Kostenreduzierung, sondern auch zum Vorteil der Beschäftigten eingesetzt werden, so ist es möglich, eine Win-Win-Situation zu schaffen.[762] Die Arbeitnehmer können hierbei

759 BT-Drs. 18/11325, S. 97.

760 BeckOK ArbR/*Werner*, § 80 BetrVG Rn. 50 Insofern ist auch der Betriebsrat dem Datenschutz – ob nun als Teil der verantwortlichen Stelle oder als eigenständige verantwortliche Stelle – ebenfalls verpflichtet. Hierzu ErfK/*Kania*, § 80 BetrVG Rn. 22 m.w.N.

761 Beispielsweise *Bodie et al.*, Colorado Law Review 2017, 961 (1036 f.).

762 Ähnlich *Bodie et al.*, Colorado Law Review 2017, 961 (1037).

den notwendigen Input zur Verbesserung der Analysen geben, wodurch frühzeitig reliable Auswertungen erzeugt werden und zur Verbesserung der Arbeitssituation und somit auch der Effizienz der Arbeit beitragen können.

§ 3 Telekommunikationsrecht / Medienrecht

I. Fernmeldegeheimnis, § 88 Abs. 2 TKG

Als weiterer rechtlicher Themenkomplex spielt das Telekommunikationsrecht eine wichtige Rolle bei der Einführung und Umsetzung der eingangs skizzierten Personalmanagement-Tools. Viele Tools – wie beispielsweise die Netzwerkgraphen – basieren darauf, dass die betriebliche Kommunikation ausgewertet wird, um – im Beispiel des Netzwerkgraphen – Rückschlüsse auf besonders wichtige Kommunikationsknoten im Unternehmen geben zu können. Aber auch für die eingangs erwähnten und später untersuchten Dashboards wird das Kommunikationsverhalten ausgewertet, um beispielsweise dem Arbeitnehmer anzeigen zu können, wieviel Zeit er pro Tag mit dem Beantworten von E-Mails verbringt oder welchen Personen er häufig nicht antwortet usw.

Schranken setzen könnte § 88 TKG, welches das Fernmeldegeheimnis im einfachgesetzlichen Recht statuiert: Nach § 88 Abs. 1 unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war, dem Fernmeldegeheimnis. Jegliche Kommunikationslösungen wie Telefonie, Bereitstellung von Internet oder E-Mail-Dienste unterliegen dem Gesetz, da hier die Kommunikation der Teilnehmer und somit der Übermittlungsvorgang im Vordergrund steht.[763] Jeder Diensteanbieter ist nach § 88 Abs. 2 zur Wahrung des Geheimnisses verpflichtet, welches auch nach dem Ende der Tätigkeit fortbesteht.

1. Grundlagen / rein dienstliche Nutzung

Es ist umstritten, ob ein Arbeitgeber als Diensteanbieter im Sinne des TKG anzusehen ist.[764] Der Begriff des Diensteanbieters ist in § 3 Nr. 6

763 *Klein*, CR 2016, 606 (607).
764 Überblick bei *Wybitul*, ZD 2011, 69.

TKG definiert. Hiernach ist Diensteanbieter jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt (lit. a) oder an der Erbringung solcher Dienste mitwirkt (lit. b). Einhellige Meinung ist, dass der Arbeitgeber kein Diensteanbieter ist, wenn er lediglich die dienstliche Nutzung von Internet, E-Mail und Telefonie erlaubt und die Privatnutzung hingegen verbietet.[765] Argumentiert wird damit, dass es sich nicht um ein Angebot für Dritte im Sinne von § 3 Nr. 10 TKG handelt.[766] Nach § 3 Nr. 10 TKG ist das „geschäftsmäßige Erbringen von Telekommunikationsdiensten" (wie in § 3 Nr. 6 TKG verlangt) das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht. Für den Fall, dass der Arbeitgeber den Anschluss nicht (auch) für die private Nutzung bereitstellt, bietet er das Internet daher nicht für Dritte an.[767]

Zu beachten ist, dass die Nutzung privater Endgeräte für dienstliche Zwecke immer mehr zunimmt (sog. *Bring Your Own Device*, kurz: *BYOD*), weshalb eine exakte Trennung zwischen dienstlicher und privater Nutzung kaum noch möglich ist. Dies gilt auch dann, wenn beispielsweise auf dem Diensttelefon neben dienstlichen Anwendungen auch private Messengerdienste oder Apps für soziale Medien installiert sind[768] oder private Mobiltelefone über WLAN des Arbeitgebers sich mit dem Internet verbinden dürfen. In diesen Fällen nutzen Arbeitnehmer für private Zwecke die Telekommunikationsdienste des Arbeitgebers.

765 *Faas*, 70.2 Einführung und Nutzung von Informationstechnologie im Arbeitsverhältnis, in: Taeger/Pohle, Computerrechts-Handbuch, Rn. 32; ArbG Frankfurt/M, Urt. v. 14.07.2004 – 9 Ca 10256/03, MMR 2004, 829; *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder*, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Diensten am Arbeitsplatz, S. 5 f.; einen guten Überblick über den Meinungsstand ist bei *Wybitul*, ZD 2011, 69 zu finden.

766 ArbG Frankfurt/M, Urt. v. 14.07.2004 – 9 Ca 10256/03, MMR 2004, 829 (830).

767 *Ernst*, NZA 2002, 585 (587); *Löwisch*, DB 2009, 2782; *Thüsing*, § 3. Zum System des Beschäftigtendatenschutzes, in: Thüsing, Beschäftigtendatenschutz und Compliance, Rn. 64 f.

768 Vgl. hierzu *Lensdorf/Born*, CR 2013, 30.

2. Private Nutzung der Telekommunikationsdienste des Arbeitgebers erlaubt

a) Meinungsstand

Gestattet der Arbeitgeber den Arbeitnehmern die Privatnutzung seiner Dienste (Internet oder E-Mail), so nimmt die insbesondere die ältere Literauffassung eine Anwendbarkeit des TKG an, mit der Folge, dass das in § 88 TKG statuierte Fernmeldegeheimnis Anwendung findet.[769] Zwischen dem Arbeitgeber und Arbeitnehmern entstehe im Hinblick auf die Privatnutzung ein gesondertes TK-Nutzungsverhältnis, wodurch der Arbeitnehmer als Dritter im Sinne des TKG qualifiziert werde.[770] Hierfür spreche die Gesetzeshistorie, da in der Regierungsbegründung auch Nebenstellenanlagen in Hotels und Krankenhäusern genannt wurden.[771]

Die Gegenauffassung (insbesondere die aktuellere Rechtsprechung) spricht sich gegen eine Anwendbarkeit des TKG auf Arbeitgeber aus. Argumentiert wird hierbei mit § 3 Nr. 24 TKG, wonach Telekommunikationsdienste nur solche Dienste sind, die „*in der Regel gegen Entgelt*" erbracht werden.[772] Zudem widerspreche auch der in § 1 TKG statuierte Gesetzeszweck, „*den Wettbewerb im Bereich der Telekommunikation und leistungsfähige Telekommunikationsinfrastrukturen zu fördern und flächendeckend*

769 *Ernst*, NZA 2002, 585 (587); *Mengel*, BB 2004, 2014 (2017); so auch die Bundesregierung, *Bundesministerium des Innern*, Hintergrundpapier zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, <*rsw.beck.de/docs/librariesprovider5/rsw-dokumente/Hintergrundpapier*>, S. 6; *Vietmeyer/Byers*, MMR 2010, 807 (808); *Kremer/Meyer-van Raay*, ITRB 2010, 133 f.; einen guten Überblick über die Vertreter dieser Auffassung gibt *Thüsing*, § 3. Zum System des Beschäftigtendatenschutzes, in: Thüsing, Beschäftigtendatenschutz und Compliance, Rn. 75 ff.; zum Meinungsstand siehe ferner *Faas*, 70.2 Einführung und Nutzung von Informationstechnologie im Arbeitsverhältnis, in: Taeger/Pohle, Computerrechts-Handbuch, Rn. 37.

770 *Vietmeyer/Byers*, MMR 2010, 807 (808); *Kremer/Meyer-van Raay*, ITRB 2010, 133 (134).

771 So u.a. *Braun*, in: Geppert/Schütz, Beck'scher TKG-Kommentar, § 91 TKG Rn. 12 m.w.N.

772 *Löwisch*, DB 2009, 2782; LAG Niedersachsen, Urt. v. 31.05.2010 – 12 Sa 875/09, MMR 2010, 639 (640) ohne nähere Begründung; im Hinblick auf die Anwendbarkeit des TKG bei Gestattung der privaten Nutzung des dienstlichen E-Mail-Accounts, vgl. LAG Berlin-Brandenburg, Urt. v. 16.02.2011 – 4 Sa 2132/10, ZD 2011, 43 (44); zum Widerspruch des Wortlauts von § 3 Nr. 6, 10 und 24: *Thüsing*, § 3. Zum System des Beschäftigtendatenschutzes, in: Thüsing, Beschäftigtendatenschutz und Compliance, Rn. 82.

angemessene und ausreichende Dienstleistungen zu gewährleisten" gegen eine Anwendbarkeit des TKG im Arbeitsverhältnis.[773]

Thüsing hat sich im Detail mit dieser Frage beschäftigt und differenziert zwischen der Duldung der Privatnutzung und der ausdrücklichen Gestattung: Im Falle der Duldung hätte eine solche nur dann rechtliche Relevanz, wenn dies zu einer Änderung des Arbeitsvertrags hin zu einer Gestattung führen würde, ansonsten sei es schlicht vertragswidriges Verhalten. Lediglich das Entstehen einer betrieblichen Übung könnte hieran etwas ändern; eine solche entstünde jedoch nicht bei einer ausdrücklich entgegenstehenden Weisung des Arbeitgebers.[774]

Allerdings kritisiert *Thüsing* auch bei erlaubter Privatnutzung die ältere Auffassung: Mit der überwiegenden Rechtsprechung[775] spricht er sich gegen eine Anwendbarkeit des TKG aus.[776] Arbeitgeber erbrächten ihre Dienste nicht zielgerichtet für Dritte nach außen, sondern in erster Linie diese für die Beschäftigen, damit sie ihren arbeitsvertraglichen Pflichten nachkommen können.[777] § 3 Nr. 10 TKG setze voraus, dass „*das Angebot von Telekommunikation an außerhalb der Sphäre des Diensteanbieters stehende Dritte gerichtet*"[778] werde,[779] worunter Arbeitnehmer nicht zählen. Arbeitsinterne Beziehungen soll das TKG gerade nicht regeln.[780]

---

773 *Löwisch*, DB 2009, 2782.

774 *Thüsing*, § 3. Zum System des Beschäftigtendatenschutzes, in: Thüsing, Beschäftigtendatenschutz und Compliance, Rn. 66 ff.

775 LAG Berlin-Brandenburg, Urt. v. 16.02.2011 – 4 Sa 2132/10, ZD 2011, 43; LAG Niedersachsen, Urt. v. 31.05.2010 – 12 Sa 875/09, MMR 2010, 639; unklar OLG Karlsruhe, Beschl. v. 10.01.2005 – 1 Ws 152/04, MMR 2005, 178; VGH Kassel, Beschl. v. 19.05.2009 – 6 A 2672/08.Z, NJW 2009, 2470; LG Krefeld, Urt. v. 07.02.2018 – 7 O 198/17, Rn. 60 (zit. n. juris); LAG Berlin-Brandenburg, Urt. v. 14.01.2016 – 5 Sa 657/15, Rn. 116 (zit. n. juris); VG Karlsruhe, Urt. v. 27.05.2013 – 2 K 3249/12, CR 2013, 428 Rn. 65 (zit. n. juris), bestätigt durch VGH Baden-Württemberg, Urt. v. 30.07.2014 – 1 S 1352/13, Rn. 79 (zit. n. juris).

776 *Thüsing*, § 3. Zum System des Beschäftigtendatenschutzes, in: Thüsing, Beschäftigtendatenschutz und Compliance, Rn. 80 ff.

777 So auch LG Krefeld, Urt. v. 07.02.2018 – 7 O 198/17, Rn. 60 (zit n. juris).

778 LAG Berlin-Brandenburg, Urt. v. 14.01.2016 – 5 Sa 657/15, Rn. 116 (zit. n. juris).

779 Vgl. auch *Schütz*, in: Geppert/Schütz, Beck'scher TKG-Kommentar, § 3 TKG Rn. 33, der jedoch darauf hinweist, dass dies bereits bei einem Telekommunikationsdienst für geschlossene Benutzergruppen erfüllt sei.

780 Siehe VG Karlsruhe, Urt. v. 27.05.2013 – 2 K 3249/12, CR 2013, 428 Rn. 65 (zit. n. juris), bestätigt durch VGH Baden-Württemberg, Urt. v. 30.07.2014 – 1 S 1352/13, Rn. 79 (zit. n. juris).

Wie *Thüsing* überzeugend dargestellt hat, würde man § 3 Nr. 24 TKG überdehnen, wenn man den Arbeitgeber regelmäßig als Anbieter ansehen würde. Diese Norm erfordert nämlich, dass die Diensteanbieter in der Regel gegen Entgelt anbieten, was bei Arbeitgebern, die ihren Arbeitnehmern die Nutzung der betrieblichen Infrastruktur zur privaten Nutzung anbieten (beispielsweise durch Erlaubnis, private E-Mails über den dienstlichen Account zu versenden oder das private Mobiltelefon im firmeneigenen WLAN einzuloggen – so auch in aller Regel bei BYOD-Regelungen) gerade nicht der Fall ist. Entgeltlichkeit müsse die Regel darstellen, nicht Unentgeltlichkeit.[781]

Auch die rechtlichen Aufbewahrungspflichten (z.B. aus dem HGB und der AO) sprechen dafür, den Arbeitgeber nicht dem Fernmeldegeheimnis aus § 88 TKG im Rahmen der erlaubten Privatnutzung des dienstlichen E-Mail-Accounts zu unterwerfen. Durch § 88 TKG wäre es dem Arbeitgeber verwehrt, seinen Pflichten nachzukommen, wenn er nicht auf die entsprechenden Postfächer zugreifen kann.[782]

b) Stellungnahme / Lösungsansatz

Die bisherigen Ausführungen zu diesem Thema lassen jedoch einen wichtigen Aspekt vermissen: Die Unterscheidung nach den technischen Gegebenheiten.

aa) Nutzung des dienstlichen E-Mail-Postfachs für private Zwecke

Im Bereich der Privatnutzung des dienstlichen E-Mail-Postfachs ist der Arbeitgeber grundsätzlich kein Diensteanbieter im Sinne des TKG; jedenfalls unterliegen die dienstlichen E-Mails nicht dem Schutz des § 88 TKG. Hierfür sprechen insbesondere teleologische Argumente sowie die Zielsetzung des Gesetzes. Es handelt sich beim TKG um ein wettbewerbsrechtliches Gesetz, welches den fairen Wettbewerb auf dem Gebiet der Telekommunikationsdienste sicherstellen soll. Arbeitgeber, die ihren Arbeitnehmern die Privatnutzung des dienstlichen Postfachs gestatten, befinden sich nicht

781 *Thüsing*, § 3. Zum System des Beschäftigtendatenschutzes, in: Thüsing, Beschäftigtendatenschutz und Compliance, Rn. 82.

782 *Thüsing*, § 3. Zum System des Beschäftigtendatenschutzes, in: Thüsing, Beschäftigtendatenschutz und Compliance, Rn. 88 f.

im Wettbewerb zu anderen Telekommunikationsanbietern. Ferner lässt das bereits aufgeführte Argument der gesetzlichen Nachweispflichten kein anderes Ergebnis zu. Würde man dem Arbeitgeber verwehren, auf dienstliche Postfächer zugreifen, wenn er die Privatnutzung erlaubt, könnte er diesen Pflichten nicht mehr nachkommen. Überzeugend ist auch das Argument, dass ein solcher Dienst durch den Arbeitgeber in aller Regel nicht gegen Entgelt erbracht wird. Entgegen *Thüsing* schwächt der Wortlaut von § 3 Nr. 10 TKG das Verlangen nach üblicher Entgeltlichkeit nicht ab, denn § 3 Nr. 10 TKG schreibt lediglich fest, dass keine Gewinnerzielungsabsicht gefordert ist; Entgelt kann mitunter auch verlangt werden, ohne dass eine Gewinnerzielungsabsicht vorliegt, wenn hierbei nur die dadurch entstehenden Aufwendungen ersetzt werden sollen.

Zudem muss der Arbeitgeber – insbesondere beim Straftatverdacht – die Möglichkeit besitzen, dienstliche Postfächer auf eventuelle Anhaltspunkte zu untersuchen. Dies kann – wie das noch im Entwurf befindliche Gesetz zur Bekämpfung der Unternehmenskriminalität (kurz: Verbandssanktionengesetz – VerSanG)[783] zeigt – nicht nur für repressive Maßnahmen gegen den Arbeitgeber relevant sein, sondern auch um eigene Geldbußen zu verringern: Nach § 18 Abs. 1 Nr. 4 VerSanG-E kann das Gericht die Verbandssanktion mindern, wenn der Verband oder der von ihm beauftragte Dritte nach Abschluss der verbandsinternen Untersuchung das Ergebnis der verbandsinternen Untersuchung einschließlich aller für die verbandsinternen Untersuchung wesentlichen Dokumente, auf denen das Ergebnis beruht, sowie des Abschlussberichts zur Verfügung stellen. Nach der Begründung zählen hierzu auch Dokumente, die zur Entlastung einzelner Mitarbeiter beitragen können.[784]

Wenn man bedenkt, dass inzwischen nahezu der komplette verkörperte Gedankenaustausch innerhalb Unternehmen über E-Mail oder Chats erfolgt, ist dies von wesentlicher Bedeutung. Ohne einen Zugriff auf das Postfach könnte das Unternehmen weder gewisse Mitarbeiter entlasten noch die Verbandsstrafe senken, da ein Zugriff sogar strafrechtlich durch § 206 StGB sanktioniert wäre. Der Zugriff auf die wesentlichen Dokumente, die das Gesetz zur Senkung der Strafe verlangt, verbliebe also verwehrt.

Mit einem technischen Argument lässt sich eine differenzierende Lösung finden: Inzwischen ist es bei den meisten E-Mail-Clients möglich,

783 Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz vom 15.08.2019.

784 Vgl. Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz vom 15.08.2019, S. 100.

gewisse E-Mails als „privat“ zu kennzeichnen. Bei einer Untersuchung des Postfachs oder dem Zugriff durch den Arbeitgeber bestünde daher die Möglichkeit einer Filterung von als „privat“ gekennzeichneten Nachrichten, um den bezweckten Schutz des Fernmeldegeheimnisses, den privaten Bereich des Arbeitnehmers, zu erfüllen.[785] Weist ein Arbeitgeber den Arbeitnehmer darauf hin und nutzt dieser die Möglichkeit der Kennzeichnung nicht, so lässt sich dies als Verzicht auf den Schutz der Privatsphäre für die konkreten Nachrichten zu werten. Bei einer grundrechtlichen Abwägung der dahinterstehenden kollidierenden Grundrechte würde sich dies jedenfalls zugunsten des Arbeitgebers auswirken. Selbst wenn man also das TKG auf Arbeitgeber anwendet, unterliegen dienstliche (und nicht gekennzeichnete private) E-Mails nicht dem Schutz des § 88 TKG.

bb) Nutzung des Internetzugangs des Arbeitgebers für private Zwecke

Bei der Nutzung des Internetzugangs des Arbeitgebers für private Zwecke, z.B. dem Zugang zum Internet durch private Mobiltelefone ist richtigerweise – wie beim Zugriff auf das dienstliche E-Mail-Postfach möglich – eine Unterscheidung nach den technischen Gegebenheiten zu treffen:

(1) Getrennte Netzwerke bzw. gesondertes Netzwerk

Stellt der Arbeitgeber den Arbeitnehmern ein eigenes Netzwerk zur Privatnutzung bereit (z.B. mit der SSID[786]„WiFi-Privatnutzung“), so liegt es nahe, ihn als Diensteanbieter im Sinne des TKG einzustufen. Solche „Hotspot-Dienste“ werden zwar immer öfters von Unternehmen für ihre Kunden kostenlos erbracht, in aller Regel erfolgen diese – zumindest in Deutschland – allerdings noch gegen Entgelt. Hier greift auch der Schutzzweck des Gesetzes wieder verstärkt ein, denn der Arbeitgeber tritt als Hotspot-Betreiber in Wettbewerb mit Mobilfunkanbietern. Nutzen Arbeitnehmer das betriebliche, für die Mitarbeiter bereitgestellte, kostenlose

785 Ablehnend *Däubler*, Gläserne Belegschaften, Rn. 340, mit dem nicht-überzeugenden Argument, dass dann der Arbeitgeber auf alle Fälle die äußeren Daten auch der privaten Mails zur Kenntnis bekäme, ohne darauf einzugehen, dass auch hier softwareseitig eine Ausblendung solcher Daten möglich ist.

786 SSID = Service Set Identifier, bezeichnet die für den Endnutzer sichtbare Kennung eines drahtlosen Netzwerks.

WLAN für ihre Mobiltelefone, so sind geringere Datentarife beim Telefontarifanbieter erforderlich, da der größte Datenverkehr untertags über die Internetleitung des Arbeitgebers läuft. Zudem ist steht der Arbeitnehmer seinem Arbeitgeber tatsächlich als „Dritter" gegenüber, denn im Rahmen dieser Nutzung ist es dem Arbeitgeber in der Regel gleichgültig, ob ein Arbeitnehmer das bereitgestellte Netzwerk nutzt oder ein Kunde (oder gar ein unbeteiligter Dritter, der sich mit einem beispielsweise offenen Netzwerk verbindet). Hier erwartet der Nutzer auch den Schutz seiner Verbindungsdaten sowie Kommunikationsinhalte durch das Fernmeldegeheimnis. Die Zielrichtung des Angebots ist eine völlig andere als bei der lediglich erlaubten Privatnutzung des dienstlichen E-Mail-Accounts, sodass in diesem Verhältnis der Arbeitgeber durchaus als Diensteanbieter agiert und den strengen Regelungen des TKG unterliegt.

(2) Betriebliches Netzwerk / einheitliches Netzwerk

Nutzen die Arbeitnehmer das für betriebliche Zwecke bereitgestellte Netzwerk *auch*, aber nicht primär, privat, indem beispielsweise im Rahmen einer BYOD-Regelung sich das Telefon bei Betreten des Firmengeländes mit dem für dienstliche Zwecke vorgesehene WLAN verbindet, so ist der Arbeitgeber kein Diensteanbieter im Sinne des TKG. Ziel der Bereitstellung dieser Dienste ist nicht vorwiegend die freie bzw. private Nutzung des betrieblichen Internetzugangs, sondern die Bereitstellung des Netzwerkzugangs für dienstliche Zwecke. So könnte beispielsweise das dienstliche Netzwerk genutzt werden, um die interne Telefonie auf dem Mobiltelefon bereitzustellen, sodass Arbeitnehmer auf dem Mobiltelefon auch unter der internen Durchwahl erreichbar sind, sobald das Gebäude betreten wird und sich das Telefon im Firmennetzwerk einbucht. Auch der Zugriff auf interne Anwendungen (wie beispielsweise Zeiterfassung oder das Intranet) könnte dann ohne die Nutzung von VPN-Clients erfolgen, wenn der Arbeitgeber diese aus Sicherheitsgründen nicht über öffentlich zugängliche Adressen bereitstellen möchte.

Die Lösung wäre hier auch nicht ein rein internes Netzwerk ohne Internetzugriff, denn viele Mobiltelefone schalten – zur Aufrechterhaltung der Internetverbindung – automatisch das WLAN aus, sobald kein Internetzugriff vorhanden ist, und verbinden sich über das Mobilfunknetz mit dem Internet. Eine Bereitstellung eines Internetzugangs über das drahtlose Netzwerk ist daher für die Funktionsfähigkeit der Dienste erforderlich. Die Folge ist, dass – insbesondere bei BYOD – auch privat genutzte

Anwendungen wie Messengerdienste sich automatisch mit dem Internet verbinden und daher das Netzwerk automatisch auch privat genutzt wird.

Der Arbeitnehmer hat jedoch grundsätzlich die Wahl: Möchte er den Schutz des TKG genießen, so deaktiviert er die privaten Anwendungen, trennt die Verbindung zum Firmennetzwerk oder verbindet sich – falls der Arbeitgeber parallel ein Mitarbeiternetzwerk zur privaten Nutzung bereitstellt – mit dem anderen Netzwerk. Da das Bereitstellen des dienstlichen Netzwerks rein dem Arbeitszweck dient, hierdurch – anders als im ersten Fall – keine Wettbewerbssituation entsteht und die Dienste in aller Regel nicht gegen Entgelt bereitgestellt werden, ist der Arbeitgeber kein Diensteanbieter im Sinne des TKG. Eine Anwendbarkeit des § 88 TKG scheidet somit aus.

cc) Nutzung des dienstlichen Telefons für private Zwecke

Analog muss dies auch für die Privatnutzung dienstlicher Telefonie gelten. Auch hier steht wie beim dienstlichen E-Mail-Account die dienstliche Nutzung im Vordergrund. Der Arbeitnehmer hat billigerweise damit zu rechnen, dass die Verbindungsdaten gespeichert und ausgewertet werden. In aller Regel wird die Privatnutzung dienstlicher Telefonie nicht mehr gegen Entgelt erbracht (mit Ausnahme von wenigen öffentlichen Einrichtungen), sofern keine exzessive Nutzung vorliegt. Durch getrennte Vorwahlen (z.B. die 0 für dienstliche Telefonate, die 9 für private Telefonate) ließe sich eine Trennung der dienstlichen von der privaten Telefonie erreichen, wodurch eine im Einzelfall getrennte Abrechnung und Verarbeitung der Daten ermöglicht wird.[787] Stellt der Arbeitgeber dem Arbeitnehmer die Möglichkeit der Privatnutzung in dieser Form bereit, so steht insbesondere bei der Bereitstellung einer eigenen Leitung für private Telefonie nicht die dienstliche, sondern die private Nutzung im Vordergrund. Dasselbe gilt auch für die dargestellten BYOD-Szenarien, wo der Arbeitnehmer über das Privattelefon die Möglichkeit hat, dienstliche Telefonate über das Firmennetzwerk zu führen. Wenn der Arbeitnehmer ein privates Telefonat führt, dann hat er die Möglichkeit, das Telefonat über die dem Fernmeldegeheimnis unterfallende private Telefonnummer zu führen.

Führt der Arbeitnehmer jedoch aufgrund der Erlaubnis private Telefonate über die dienstliche Rufnummer, so ist er nicht als „Dritter“ anzuse-

787 So auch *Däubler*, Gläserne Belegschaften, Rn. 340.

hen, da er insbesondere auch nach außen (gewollt) aus der Sphäre des Arbeitgebers kommend auftritt, indem die dienstliche Telefonnummer beim Empfänger angezeigt wird. Dienstliche Telefonie wird schließlich in erster Linie deshalb bereitgestellt, dass Arbeitnehmer ihre vertraglichen Pflichten erfüllen können.

3. Zwischenergebnis

Der bisherige Meinungsstand in der Rechtsprechung und Literatur lässt eine wichtige technische Unterscheidung vermissen. Zu pauschalisiert ist es, den Arbeitgeber generell als Diensteanbieter im Sinne des TKG einzustufen bzw. auszuschließen. Die Anwendbarkeit des Fernmeldegeheimnisses hängt davon ab, wie die angebotenen Dienste ausgestaltet sind. Es ist möglich, dass Arbeitgeber speziell für private Zwecke gekennzeichnete Infrastrukturen anbieten, wodurch Arbeitnehmer dem Arbeitgeber nicht mehr als in seiner Sphäre befindlich gegenüberstehen, sondern als „Dritte" im Sinne des TKG. Solche Dienste werden in aller Regel auch gegen Entgelt angeboten, sodass der Arbeitgeber als Anbieter grundsätzlich im Wettbewerb mit klassischen Telekommunikationsanbietern stehen. In solchen Situationen wird im Allgemeinen von den Arbeitnehmern die Anwendbarkeit des Fernmeldegeheimnisses erwartet.

Anders ist die Lage jedoch, wenn die Netze / Dienste vorwiegend dienstlichen Zwecken dienen; bei Letzteren scheidet eine Anwendbarkeit des TKG aus. Arbeitgeber können somit auf die Verbindungs- und Kommunikationsdaten zugreifen. Auf die Unterscheidung, ob der Zugriff während des Übermittlungsvorgangs erfolgt ist oder erst nach Abschluss der Übermittlung,[788] kommt es daher nicht an. Da der strafrechtliche Schutz durch § 206 StGB im Wesentlichen parallel zu § 88 TKG verläuft,[789] gelten die Ausführungen zum Fernmeldegeheimnis analog.

788 Keine Anwendbarkeit des Fernmeldegeheimnisses nach Abschluss der Übermittlung: VG Frankfurt/M., Urt. v. 06.11.2008 – 1 K 628/08.F (3), CR 2009, 125 (126); VGH Kassel, Beschl. v. 19.05.2009 – 6 A 2672/08.Z, NJW 2009, 2470 Kritisch zur Rechtsprechung und für eine Anwendbarkeit des Fernmeldegeheimnisses *Kremer/Meyer-van Raay*, ITRB 2010, 133 (135).

789 *Löwisch*, DB 2009, 2782 (2783).

II. Schutz der Kommunikation durch das TMG

Neben den Regelungen des TKG kann auch das TMG anwendbar sein, sofern sog. Mischdienste vorliegen, also nicht lediglich Signale übertragen werden, sondern auch Inhalte zur Verfügung gestellt werden.[790] Während das TKG vor allem die Nutzung von Verkehrs- und Standortdaten regelt, regelt das TMG die Nutzung von Bestands- und Nutzungsdaten.[791] Nach § 1 Abs. 1 S. 1 TMG gilt das Telemediengesetz für alle elektronischen Informations- und Kommunikationsdiensten, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 TKG, *die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen*, […] sind (Telemedien). Hierbei ist es nach § 1 Abs. 1 S. 2 gleichgültig, ob sie gegen Entgelt erbracht werden oder nicht.

So unterfällt beispielsweise die reine Internettelefonie (*Voice over IP – VoIP*) nicht dem TMG, da sich die Leistung darin erschöpft, Signale über Kommunikationsnetze zu übertragen.[792] Für das genannte Beispiel der Einwahl des mitarbeitereigenen Geräts in das Firmennetzwerk zur Nutzung der betrieblichen Telefonanlage ist das TMG somit nicht anwendbar. Dasselbe gilt für die Bereitstellung eines Internetzugangs, da auch hier lediglich Signale über Kommunikationsdienste übertragen werden.[793] Sobald ein Internetanbieter jedoch ein eigenes Portal zur Verfügung stellt, in welchem er Inhalte aussucht und aufbereitet, unterliegt er diesbezüglich dem TMG.[794] Das Anbieten des Internetzugangs durch Arbeitgeber, ohne ein eigenes Portal zu betreiben, unterliegt daher nicht den Regelungen des TMG. Etwas anderes würde nur gelten, wenn beispielsweise mit dem Internetzugang über den Hotspot zwingend die Nutzung eines bestimmten Portals zur Erlangung des Internetzugangs erforderlich wäre (sog. *Captive Portal*), in denen der Nutzer beispielsweise die Nutzungsbedingungen des Anbieters akzeptieren muss und gleichzeitig Inhalte bereitgestellt werden.

Als typisches Beispiel für einen Mischdienst nennt die Gesetzesbegründung die E-Mail-Übertragung, da zusätzlich noch eine inhaltliche Dienstleistung angeboten wird.[795] Hier bietet der Anbieter (Arbeitgeber) in aller Regel auch noch ein Portal in Gestalt eines Webmail-Clients, wo die

790 BeckOK InfoMedienR/*Martini*, § 1 TMG Rn. 11a.
791 *Jandt*, ZD 2018, 405 (406).
792 BeckOK InfoMedienR/*Martini*, § 1 TMG Rn. 12.
793 BeckOK InfoMedienR/*Martini*, § 1 TMG Rn. 13; anders noch die Gesetzesbegründung BT-Drs. 16/3078, S. 13.
794 *Ricke*, in: Spindler/Schuster, Recht der elektronischen Medien, § 1 TMG Rn. 7.
795 BT-Drs. 16/3078, S. 13.

Arbeitnehmer ihre E-Mails verfassen und empfangen können. Für diese Webmail-Portale wäre das TMG grundsätzlich anwendbar.[796]

Im Arbeitsverhältnis statuiert § 11 Abs. 1 TMG jedoch eine ausdrückliche Ausnahme für die datenschutzrechtlichen Vorschriften des vierten Abschnitts bei Diensten, die ausschließlich für berufliche oder dienstliche Zwecke genutzt werden. Sobald der Arbeitgeber allerdings die Privatnutzung der Dienste erlaubt, ist er Anbieter von Telemedien, sodass die weiteren Vorschriften des TMG, insbesondere § 15 Anwendung finden könnten.[797] Dies ergibt sich bereits aus einem Umkehrschluss aus § 11 Abs. 1 TMG.[798]

Nach § 15 Abs. 1 TMG ist es dem Arbeitgeber nur gestattet, personenbezogene Daten eines Nutzers zu erheben und zu verwenden, wenn dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Allerdings findet § 15 Abs. 1 TMG keine Anwendung bei Telemedien, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, § 11 Abs. 3 TMG.[799] Als Beispiele können hier insbesondere die E-Mail-Übertragung sowie der Internetzugang genannt werden,[800] sodass die Vorschriften des TMG für die vorliegende Untersuchung außer Betracht bleiben können. Etwaige Portale für das Intranet oder die Darstellung von Dashboards dienen hingegen nur betrieblichen Zwecken und werden nicht für private Zwecke zur Verfügung gestellt, sodass diese nach § 11 Abs. 1 TMG vom Telemediengerecht ausgenommen sind.

Unabhängig davon genießt die Datenschutzgrundverordnung nunmehr wohl Anwendungsvorrang für die Regelungen des vierten Abschnitts (§§ 11 – 15a) des TMG. Hintergrund ist, dass die Vorschriften des Abschnitts vorrangig eine Umsetzung der DS-RL darstellen und seit Geltung der DSGVO nicht auf der Grundlage von Öffnungsklauseln beibehalten werden dürfen, zumal diese nicht Umsetzung der ePrivacy-RL sind.[801]

---

796 *Klein*, CR 2016, 606 (607).

797 *Kömpf/Kunz*, NZA 2007, 1341 (1344 f.).

798 So auch *Panzer-Heemeier*, B. V. Betriebsvereinbarungen zur Nutzung technischer Einrichtungen, in: Oberthür/Seitz, Betriebsvereinbarungen, Rn. 74.

799 HdbIT-DSR/*Conrad/Hausen*, § 37 Arbeitsrechtliche Bezüge, Rn. 210 f.

800 *Müller-Broich*, in: Müller-Broich, Telemediengesetz, § 11 TMG Rn. 7.

801 *DSK*, Positionsbestimmung zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, <www.datenschutzkonferenz-online.de/media/ah/201804_ah_positionsbestimmung_tmg.pdf>, S. 2 Ziff. 3; jurisPK-Internetrecht/*Heckmann/Scheurer*, Kap. 9 Datenschutz, Rn. 64 f.; *Jandt*, ZD 2018, 405 (407).

§ 4 Zwischenergebnis

Auf moderne HR-Anwendungen im Bereich People Analytics sind eine Vielzahl rechtlicher Normen einschlägig. Zuvorderst müssen die Regelungen des Datenschutzrechts beachtet werden, deren Kernbereich, insbesondere im Bereich des Beschäftigtendatenschutzes, die Regelung solcher (Überwachungs-)Anwendungen sind. Effektive People Analytics benötigen eine immense Datengrundlage, welche neben der aktiven Erhebung bspw. durch Befragen der Arbeitnehmer insbesondere auch aus Sensor- und Logdaten erhoben wird. Durch die immer weitreichendere Digitalisierung des Arbeitsalltags fallen Unmengen an Daten an, die mit Hilfe von Big-Data-Technologien strukturiert und ausgewertet werden können. Im Fokus steht bei der rechtlichen Begrenzung zumeist der Schutz der Persönlichkeitsrechte der Arbeitnehmer. Arbeitnehmer dürfen grundsätzlich nicht dauerhaft überwacht werden. Jede Datenerhebung und -verarbeitung ist zweckgebunden und legitimationsbedürftig (Art. 5 Abs. 1 lit. a DSGVO). Als Rechtsgrundlage im Bereich des Beschäftigtendatenschutzes steht § 26 Abs. 1 BDSG im Mittelpunkt der Betrachtung. Er lässt eine Datenerhebung und -verarbeitung zu, wenn dies für die Zwecke des Beschäftigungsverhältnisses erforderlich ist. Im Rahmen der vorzunehmenden Erforderlichkeitsprüfung ist u.a. eine Bewertung der widerstreitenden Interessen, insbesondere des Interesses des Arbeitgebers an der Datenerhebung sowie das Interesse des Arbeitnehmers an der Geheimhaltung vorzunehmen. Die Einwilligung (Art. 7 DSGVO, § 26 Abs. 2 BDSG) ist zwar im Arbeitsverhältnis nicht grundsätzlich ausgeschlossen, für den Bereich der People Analytics ist jedoch genau zu überprüfen, ob diese freiwillig abgegeben wurde. Dies wird unter anderem auch davon abhängen, wofür die erhobenen Daten genutzt werden. § 26 Abs. 2 S. 2 BDSG gibt als Auslegungshilfe dem Anwender den Hinweis an die Hand, dass eine Freiwilligkeit insbesondere dann vorliegen kann, wenn gleichgelagerte Interessen verfolgt werden. Werden die Daten für Leistungsbeurteilungen und ggf. individualrechtliche Konsequenzen genutzt, so ist nicht davon auszugehen, dass Arbeitgeber und Arbeitnehmer gleichgelagerte Interessen verfolgen. Dienen die Analytics beispielsweise lediglich zur Selbstoptimierung oder dem Gesundheitsschutz, so kommt eine Einwilligung eher in Betracht.[802]

802 *Götz* hingegen empfiehlt für alle People Analytics die Einwilligungen der jeweils betroffenen Arbeitnehmer einzuholen, zeigt aber zugleich die Risken in den verschiedenen Situation auf, vgl. *Götz*, Big Data im Personalmanagement, S. 55 f.

Weiterhin ist das Verbot der automatisierten Einzelfallentscheidung aus Art. 22 DSGVO zu beachten, wonach algorithmisierte Entscheidungen ohne einen dazwischengeschalteten menschlichen Entscheider nur in besonderen Ausnahmefällen erlaubt sind, u.a. wenn es erforderlich ist. Die Erforderlichkeit einer automatisierten Entscheidung darf nicht nur anhand rein objektiver Kriterien verstanden werden. Auch hier ist grundsätzlich eine Wertung vorzunehmen.

Unabhängig davon, ob eine automatisierte Einzelfallentscheidung vorliegt, ist der Arbeitgeber, der ein Profiling seiner Arbeitnehmer vornimmt (was bei People Analytics die Regel ist), zur Erstellung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO verpflichtet, da grundsätzlich ein hohes Risiko für die (Daten der) Betroffenen besteht.

Doch nicht lediglich das Datenschutzrecht ist für diese Anwendungen von Relevanz, sondern auch das Betriebsverfassungsrecht. Der Betriebsrat hat nach §§ 87, 92, 94 f. sowie ggf. § 111 BetrVG weitreichende Mitbestimmungs- und Beratungsrechte. Nach § 75 Abs. 2 BetrVG wacht dieser zudem über die Persönlichkeitsrechte der im Betrieb beschäftigten Arbeitnehmer.

Nicht zuletzt aufgrund § 26 Abs. 4 BDSG ist es ohnehin geboten, den Betriebsrat frühzeitig über geplante Maßnahmen zu informieren und mit ihm zu verhandeln, um Rechtsunsicherheiten bei der Anwendung des § 26 Abs. 1 BDSG zu vermeiden und People-Analytics-Anwendungen mittels Betriebsvereinbarung zu regeln. Diese kann als Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten dienen, ohne dass eine weitere Erforderlichkeitsprüfung nach dem Schema des § 26 Abs. 1 BDSG vorgenommen werden muss. Die Betriebsparteien müssen bei der Verfassung einer solchen Vereinbarung allerdings die engen Vorgaben des Art. 88 Abs. 2 DSGVO beachten. Eine lückenlose Überwachung der Arbeitnehmer könnte demnach auch nicht durch eine Betriebsvereinbarung legitimiert werden.[803]

Ein weiterer, spezifischer Regelungskomplex, den es im Zusammenhang mit IT-Anwendungen zu beachten gilt, ist das Telekommunikations- und -medienrecht. Für die hier untersuchten Anwendungsbereiche im Bereich der People Analytics scheidet eine Anwendbarkeit jedoch aus. Der Arbeitgeber ist im dienstlichen Bereich gegenüber seinen Arbeitnehmern kein Diensteanbieter.

803 Eine solche Betriebsvereinbarung wäre auch nach § 75 Abs. 2 BetrVG rechtswidrig, vgl. BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205.

In der Praxis gilt es aber zu beachten, dass dies noch nicht höchstrichterlich entschieden wurde. Zwar sind die überwiegende (vor allem jüngere) Rechtsprechung und Literatur nunmehr auch der Auffassung, dass eine Anwendbarkeit des TKG auf Arbeitgeber ausscheidet, dennoch sollte die weitere Rechtsentwicklung genau betrachtet werden. Insbesondere die Datenschutzbehörden sind derzeit (noch?) der Auffassung, dass bei erlaubter oder geduldeter Privatnutzung des dienstlichen E-Mail-Accounts oder der vom Arbeitgeber bereitgestellten Internetverbindung das Fernmeldegeheimnis Anwendung findet.[804]

Während es beim Internetzugang möglich ist – insbesondere bei BYOD –, den Datenverkehr sauber zu trennen (z.B. indem auch auf dem betrieblichen PC ein eigener Browser mit anderen Einstellungen für das private Surfen installiert wird), ist die Möglichkeit der Kennzeichnung im E-Mail-Postfach offensichtlich bei den Datenschutzbehörden noch unbekannt. Aus diesem Grund ist es nach derzeitiger Rechtslage für die Praxis zu empfehlen, die private Nutzung des dienstlichen E-Mail-Dienstes zu untersagen. Andernfalls könnte dies mitunter sogar aufgrund § 206 StGB strafrechtliche Sanktionen zur Folge haben.

804 „*Ist die private Nutzung des Internets erlaubt […], wird der Arbeitgeber hinsichtlich der privaten Nutzung zum Diensteanbieter im Sinne des TKG und unterliegt den Datenschutzbestimmungen des TMG.*“, vgl. *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder*, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Diensten am Arbeitsplatz, S. 7. „*Ist die private E-Mail-Nutzung erlaubt […], ist der Arbeitgeber gegenüber den Beschäftigten und ihren Kommunikationspartnern zur Einhaltung des Fernmeldegeheimnisses verpflichtet.*“, vgl. *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder*, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Diensten am Arbeitsplatz, S. 8.

E. Bewertung von People Analytics-Einsatzszenarien

Es wurde herausgestellt, dass sich ein Wandel vom „klassischen Personalmanagement 1.0“ hin zu People Analytics in Kombination mit evidenzbasiertem Management als Teil der Arbeit 4.0 vollzogen hat bzw. noch vollzieht (**Kapitel B**). Der Begriff der „People Analytics“ als Oberbegriff für moderne Ansätze im Personalmanagement und dessen Vor- und Nachteile im Vergleich zum Personalmanagement 1.0 wurden in **Kapitel C** ausführlich dargestellt. Im Anschluss wurden in **Kapitel D** die rechtlichen Grundlagen für den Einsatz moderner HR-Maßnahmen und Tools geklärt.

In diesem Kapitel soll nun in verschiedenen Stufen untersucht werden, inwiefern überhaupt Datenanalysen, die Bewertungen in Form von „Scores“ oder Persönlichkeitsprofile erzeugen sollen, als Rechtsgrundlage für Entscheidungen dienen dürfen (§ **1**), bevor im Anschluss untersucht wird, inwieweit diese Datengrundlagen auch für automatisierte Entscheidungen herangezogen werden dürfen (§ **2**). Ein mögliches und prominentes Beispiel von People-Analytics stellen Dashboards dar, die sowohl dem Arbeitnehmer als auch dem Arbeitgeber die nutzerfreundliche Darstellung der Analyseergebnisse auf dem Computer oder Mobilgerät überhaupt erst ermöglichen. Dieser Art der Datenaufbereitung soll daher besondere Aufmerksamkeit gewidmet werden (§ **3**). Ein mit vielen Analysetools einhergehendes und besonders in jüngerer Zeit aufkommendes Werkzeug sind sog. Netzwerk-Graphen, nunmehr in Form des sog. *Enterprise Social Graph*. Letzterer soll das (innerbetriebliche) Kommunikationsnetzwerk analysieren und weitere Einsichten in die informelle Hierarchie geben. Ein weiterer Abschnitt wird daher den Netzwerk-Graphen gewidmet (§ **4**).

Das nachfolgende Kapitel (**Kapitel F**) soll auf Basis der in diesem Kapitel gefundenen Ergebnisse Regelungsmöglichkeiten der Betriebspartner für die dargestellten Werkezuge und Tools erarbeiten und schließlich in einer Muster-Betriebsvereinbarung münden, die den Verhandlungspartnern als Grundstruktur für die Regelung eigener People-Analytics-Sachverhalte dienen und die Reichweite der Regelungsmöglichkeiten aufzeigen soll.

§ 1 People Analytics als Grundlage bzw. Unterstützung für Personalentscheidungen

In einem ersten Schritt muss geklärt werden, inwiefern Analyseergebnisse – die rechtmäßige Erhebung der Daten (für andere Zwecke) vorausgesetzt – als Grundlage bzw. Unterstützung für Personalentscheidungen dienen dürfen.

I. Grundsatz der Zweckbindung von personenbezogenen Daten

Sofern Daten für einen bestimmten Zweck, beispielsweise für die Begründung des Arbeitsverhältnisses, rechtmäßig erhoben wurden, ist zu beachten, dass diese Daten nicht beliebig für andere Verarbeitungszwecke eingesetzt werden. Art. 5 Abs. 1 lit. b DSGVO statuiert den Grundsatz der Zweckbindung. Hiernach müssen Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesem Zweck nicht zu vereinbarenden Weise weiterverarbeitet werden. Hs. 2 statuiert eine Ausnahme für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke. Eine weitere Auflockerung des Zweckbindungsgrundsatzes stellt Art. 6 Abs. 4 DSGVO dar. Dieser bestimmt, dass wenn die Verarbeitung zu einem anderen Zweck als zu demjenigen erfolgt, zu dem die personenbezogenen Daten erhoben wurden, und weder auf der Einwilligung der betroffenen Person oder einer Rechtsvorschrift beruht, der Verantwortliche die Zweckvereinbarkeit anhand vorgegebener Kriterien zu prüfen hat (sog. *Kompatibilitätstest*): Die Kriterien des Kompatibilitätstestes sind in Art. 6 Abs. 4 lit. a - e DSGVO aufgezählt: Verbindung zwischen den Zwecken der Erhebung und der Weiterverarbeitung (lit. a), Zusammenhang, in welchem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen (lit. b), Art der personenbezogenen Daten, insbesondere ob es sich um sensitive Daten im Sinne von Art. 9 DSGVO handelt oder ob Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 DSGVO verarbeitet werden (lit. c), Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen (lit. d) sowie Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören können (lit. e).

In einem ersten Schritt ist zu prüfen, wie weit ein Verarbeiter den Verarbeitungszweck unter der Maßgabe des Art. 5 Abs. 1 lit. b DSGVO festlegen

kann bzw. wie weit ein gesetzlicher Verarbeitungszweck ist, bevor auf eventuelle Ausnahmen von der Zweckbindung eingegangen wird. Wäre es dem Verarbeiter, z.B. im Rahmen einer Betriebsvereinbarung oder einer Einwilligung möglich, einen sehr weiten Verarbeitungszweck zu definieren, kommt es auf mögliche Ausnahmen nicht mehr an.

1. Spezifität der Zweckbestimmung nach Art. 5 Abs. 1 lit. b DSGVO

Der Grundsatz der Zweckbestimmung wird auch in Erwägungsgrund 39 S. 6 der DSGVO nochmals aufgegriffen. Hier wird verdeutlicht, dass insbesondere die bestimmten Zwecke, zu denen personenbezogene Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung feststehen sollen. Auf den ersten Blick scheint es, dass die Zweckbestimmung daher sehr eng gefasst werden muss[805] und insbesondere Big Data-Auswertungen mit ungewissem Ausgang nach den Erwägungsgründen ausgeschlossen werden sollen.

Tatsächlich ist es so, dass der Grundsatz der Zweckbindung eines der zentralen Prinzipien des Datenschutzrechts ist.[806] So wurde dieser bereits 1990 nach dem Volkszählungsurteil des BVerfG[807] für den öffentlichen Bereich in das BDSG aufgenommen.[808] In Verbindung mit dem Erforderlichkeitsgrundsatz kann hieraus die Forderung entnommen werden, dass der Betroffene genau wissen soll, was andere (bzw. Datenverarbeiter) über ihn wissen,[809] da er seine Daten unter der Erwartung eines bestimmten Verwendungszwecks offenlegt.[810] Es ist somit ein Ausfluss des in Art. 5 Abs. 1 lit. a DSGVO statuierten Transparenzgrundsatzes, denn nur wenn die betroffene Person weiß, zu welchen Zwecken ihre Daten verarbeitet werden, ist die Datenverarbeitung für sie nachvollziehbar. Die Zweckbe-

805 So auch *Schantz*, NJW 2016, 1841 (1842).
806 *Herbst*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 5 DSGVO Rn. 21; *Kühling/Klar/Sackmann*, Datenschutzrecht, S. 146 Rn. 338; *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, S. 201; *Article 29 Data Protection Working Party*, WP 203, S. 4; EuArbRK/*Franzen*, Art. 5 DSGVO Rn. 5.
807 BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1 – Volkszählungsurteil.
808 *Rüpke*, § 12. Rechtsgrundlagen der Verarbeitung, in: Rüpke/von Lewinski/Eckhardt, Datenschutzrecht, Rn. 38.
809 *Rüpke*, § 12. Rechtsgrundlagen der Verarbeitung, in: Rüpke/von Lewinski/Eckhardt, Datenschutzrecht, Rn. 38.
810 *Article 29 Data Protection Working Party*, WP 203, S. 4.

stimmung ist der „Fixpunkt", an dem sich die datenschutzrechtliche Prüfung vollzieht.[811]

Gerade aufgrund moderner Verarbeitungstechniken und der damit verbundenen Verknüpfungsmöglichkeiten verschiedener Daten, nicht zuletzt aufgrund Big Data, gewinnt der Zweckbindungsgrundsatz an immenser Bedeutung.[812] Auswertungen unter dem Stichwort „Big Data" basieren darauf, dass die Daten frei genutzt werden können, um neue Erkenntnisse zu gewinnen.[813] Der Grundsatz steht somit, wie Kritiker behaupten, Innovationsprozessen in der Wirtschaft klar entgegen.[814] Ziel von solchen Auswertungen ist es – wie bereits dargestellt – unbekannte Zusammenhänge zu entdecken, die dem menschlichen Betrachter bislang verborgen blieben.

Bei den Regelungen zur Zweckvereinbarkeit in Art. 6 Abs. 4 DSGVO handelt es sich nunmehr um eine Aufweichung des früher in Deutschland geltenden (relativ) strengen Zweckbindungsgrundsatzes.[815]

Die Zweckvereinbarkeit ist jedoch von der Zweckbestimmung nach Art. 5 Abs. 1 lit. b DSGVO zu unterscheiden. In einem ersten Schritt muss zunächst ein Verarbeitungszweck festgelegt werden, bevor dieser auf weitere mit diesem vereinbare Verarbeitungsmaßnahmen geprüft werden kann.

Bei der Festlegung des Verarbeitungszwecks muss der Verarbeiter so spezifisch sein, dass exakt feststellbar ist, welche Verarbeitungsvorgänge davon erfasst sind und welche nicht. Nur dann kann die Rechtmäßigkeit der Verarbeitung sicher festgestellt werden.[816] Zulässig ist es auch, mehrere Verarbeitungszwecke festzulegen, wobei allerdings jeder genau bestimmt sein muss.[817] Diese Festlegungen sind sowohl in der Datenschutzinformation nach Art. 13 f. DSGVO als auch im grundsätzlich schriftlich bzw. elektronisch zu führenden Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO aufzunehmen.[818]

---

811 Vgl. EuArbRK/*Franzen*, Art. 5 DSGVO Rn. 14; *Dammann*, ZD 2016, 307 (311).
812 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 52 Rn. 5.
813 *Buchner*, DuD 2016, 155 (156).
814 Vgl. hierzu *Grafenstein*, DuD 2015, 789 zum Spannungsfeld von Datenschutz und Innovationsprozessen.
815 *Kremer*, § 2 Zulässigkeit der Verarbeitung, in: Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, Rn. 44; aA *Gierschmann* ZD (2016), 51 (54).
816 *Article 29 Data Protection Working Party*, WP 203, S. 15.; so wohl auch EuArbRK/*Franzen*, Art. 5 DSGVO Rn. 5.
817 Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 13.
818 Insofern ist es nicht ganz korrekt, wenn *Götz*, Big Data im Personalmanagement, S. 121 davon spricht, dass Formvorschriften nicht existierten. Es gibt

Die *Artikel-29-Datenschutzgruppe* nannte in ihrem Arbeitspapier zur Zweckbindung Beispiele für zu vage Zweckfestlegungen. Das wären zum Beispiel „*IT-Sicherheitszwecke*", „*Marketingzwecke*" oder „*zukünftige Untersuchungen*". Die Spezifität der Zweckbestimmung hängt vom Kontext der Datensammlung und -verarbeitung sowie der Art der involvierten Daten ab. Teilweise wird vertreten, dass mit steigender Sensibilität der Erkenntnisse auch die Anforderungen an die Zweckdefinition steigen.[819] Kontraproduktiv sind aber auch zu detaillierte Zweckbestimmungen, insbesondere wenn diese zu sehr in Rechtssprache mit vielen Hinweisen gehalten sind und der Zweck hierdurch verschleiert würde.[820]

Folgende Zweckfestlegungen reichen nach Auffassung der Literatur aus: „*Reise nach Mallorca im Mai 2015*" oder „*Bearbeitung des Antrags auf Sondernutzungsgenehmigung v. 15.07.2015*".[821]

a) Zweckbestimmung im Rahmen der Einwilligung / einer Kollektivvereinbarung

Maßgeblich wird die Zweckbestimmung insbesondere bei der Einwilligung oder der Festlegung in einer Kollektivvereinbarung, bei welchen der Verarbeiter die Zwecke frei angeben kann. Bis auf die oben genannte Bestimmung, dass der Zweck eindeutig und rechtmäßig sein muss, verhält sich die DSGVO nicht zur Frage der Zweckbestimmung. Ebenso wenig hat sich der EuGH bislang dazu geäußert.[822]

Sieht man die Zweckbestimmung – zumindest im Rahmen der Einwilligung – als Ausfluss der informationellen Selbstbestimmung, müsste es strenggenommen, wie *Grafenstein* richtig ausführt, ausreichen, wenn diese in der Allgemeinheit angegeben werden, wenn der Betroffene darüber aufgeklärt ist und dieser weiten Zweckbestimmung zustimmt. Allerdings

---

zahlreiche Vorschriften in der DSGVO, die eine zumindest in Textform vorzunehmende Fixierung des Zwecks erfordern.

819 *Götz*, Big Data im Personalmanagement, S. 126.

820 *Article 29 Data Protection Working Party*, WP 203, S. 16.

821 *Buchner*, 2 Grundsätze des Datenschutzrechts, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 244 Rn. 60.

822 Der EuGH beschäftigte noch unter Geltung der DS-RL mit der Zweckfestlegung, wobei er hierzu jedoch keine näheren Spezifikationen traf, vgl. EuGH, Urt. v. 05.05.2011 – C-543/09, EuZW, 2011, 485 (487 f.) – Deutsche Telekom AG/Deutschland Rn. 64 ff.

kritisiert sie zu Recht, dass Betroffene dann mitunter nicht in der Lage sind, die Folgen richtig abzuschätzen.[823]

Grafenstein spricht sich daher dafür aus, nicht nur die Selbstbestimmung bzw. die Erwartungen des Betroffenen in den Raum zu stellen, sondern „alle verfassungsrechtlich geschützten Risikosphären", also nicht nur die Privatsphäre, sondern auch die allgemeine Handlungsfreiheit und weitere Freiheits- und Gleichheitsrechte.[824] Dies kann jedoch nur insofern gelten, als die Zwecke der Verarbeitung außerhalb der bereits gesetzlich genannten und festgelegten Zwecke liegen, da nur dort ein Spielraum für den Verarbeiter zur Zweckfestlegung besteht. So treffen die Ausführungen ausschließlich auf den Fall der Einwilligung oder der Regelung einer Kollektivvereinbarung zu, denn selbst bei der Verarbeitung im Rahmen von Art. 6 Abs. 1 lit. f DSGVO muss der Zweck der Verarbeitung die Erforderlichkeit zur Wahrung von berechtigten Interessen des Verarbeiters sein.

Da die Einwilligung im Arbeitsverhältnis – zumindest für die hier dargestellten Szenarien – jedoch eine untergeordnete Rolle spielt,[825] wird hierauf an dieser Stelle nicht näher eingegangen. Nicht zuletzt werden Arbeitgeber selbst daran interessiert sein, aufgrund § 26 Abs. 2 S. 2 BDSG eine enge Zweckbestimmung zu treffen, da die Einwilligung im Zweifel nur dann wirksam sein wird, wenn Arbeitnehmer und Arbeitgeber gleichgelagerte Interessen verfolgen. Eine weite Zweckbestimmung würde der Überprüfung der gleichgelagerten Interessen zuwiderlaufen, wobei hier die Überprüfung zu Lasten des Arbeitgebers, der die Daten auf Basis der Einwilligung verarbeiten möchte, ausfallen würde.

Im Rahmen von Betriebsvereinbarungen müssen Arbeitgeber und Betriebsrat aufgrund Art. 88 Abs. 2 DSGVO, § 75 Abs. 2 BetrVG auf eine hinreichend spezifische Zweckbestimmung achten. In der Praxis wird jedoch in aller Regel der Betriebsrat zur Wahrung seiner Mitbestimmungsrechte und zur Sicherung der Überprüfbarkeit der Einhaltung der Betriebsvereinbarung auf eine detaillierte und präzise Zweckbestimmung drängen.

b) § 26 BDSG: Verarbeitung zum Zwecke des Beschäftigungsverhältnisses

§ 26 Abs. 1 BDSG bestimmt, dass eine Verarbeitung von personenbezogenen Daten von Beschäftigten (und gem. Abs. 8 S. 2 auch von Bewerbern)

823 *Grafenstein*, DuD 2015, 789 (793).
824 *Grafenstein*, DuD 2015, 789 (794).
825 Hierzu bereits **D. § 1 III. 2. a**).

für Zwecke des Beschäftigungsverhältnisses verarbeitet werden dürfen, *wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses, für dessen Durchführung oder Beendigung […] erforderlich ist*.

In Konkretisierung der obigen Ausführungen unter **D. § 1 IV. 2. b**) muss an dieser Stelle nunmehr genauer auf die Frage eingegangen werden, wann eine Datenverarbeitung nach § 26 Abs. 1 BDSG zum Zwecke des Beschäftigungsverhältnisses erforderlich ist, insbesondere wie weit die vom Gesetzgeber genannten Zwecke zu verstehen sind.[826]

aa) Erforderlichkeit für die Entscheidung über die Begründung des Beschäftigungsverhältnisses

Der erstgenannte Verarbeitungszweck betrifft insbesondere die in § 26 Abs. 8 S. 2 BDSG genannten Bewerber für ein Beschäftigungsverhältnis. Nach § 26 Abs. 1 S. 1 Var. 1 BDSG ist der Arbeitgeber befugt, personenbezogene Daten dieser Personengruppe zu verarbeiten, wenn dies für seine Entscheidung über die Begründung des Beschäftigungsverhältnisses erforderlich ist.

Angesichts der Formulierung der Norm mag die Vermutung aufkommen, dass der Zweck weit zu verstehen ist und der Arbeitgeber frei bestimmen kann, welche Daten er zur Entscheidung über die Begründung des Beschäftigungsverhältnisses benötigt. Das Kriterium der Erforderlichkeit ist jedoch nicht subjektiv, sondern objektiv zu verstehen.[827] Allerdings darf es gleichfalls nicht im Sinne einer unverzichtbaren Notwendigkeit interpretiert werden. Vielmehr muss es so gelesen werden, dass der Nutzer bei vernünftiger Betrachtung auf die Datenerhebung angewiesen ist.[828] Es kommt darauf an, ob die Wahl einer anderen Datenverarbeitungsmethode oder der Verzicht sinnvoll oder zumutbar wäre, wobei die Organisationsform und Arbeitsweise der datenerhebenden Stelle zugrunde zu legen

826 Die gesetzliche Differenzierung zwischen Begründung, Durchführung und Beendigung wird teilweise in der Literatur als überflüssig bezeichnet, vgl. *Pötters*, in: Gola, Datenschutz-Grundverordnung, Art. 88 DSGVO Rn. 45 Andere wiederum verweisen auf die Wichtigkeit der Zweckbestimmung für die Verhältnismäßigkeitsprüfung, vgl. BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 71.

827 Es hat eine Verhältnismäßigkeitsprüfung stattzufinden, vgl. *Pötters*, in: Gola, Datenschutz-Grundverordnung, Art. 88 DSGVO Rn. 46.

828 OLG Köln, Urt. v. 19.11.2010, BeckRS 2011, 14259 unter II. 1. c) cc) der Gründe.

ist.[829] Bei vielen People-Analytics-Maßnahmen werden die Daten in aller Regel nicht mehr zum Zwecke der Begründung des (konkreten) Beschäftigungsverhältnisses, sondern zur Optimierung von Bewerbungsprozessen eingesetzt, sodass es sich hierbei um einen beschäftigungsfremden Zweck handelt und die Zulässigkeit der Weiterverarbeitung nach Art. 6 Abs. 1 lit. f DSGVO[830] zu prüfen ist.

Insbesondere aufgrund des bestehenden Machtgefälles zwischen Arbeitgeber und Arbeitnehmer in der Bewerbungssituation ist zu beachten, dass die Bewerber keine vollständige Entscheidungsfreiheit haben.[831] Im Zweifel werden sie die Daten dem Arbeitgeber überlassen und sich nicht nur aufgrund einer zu weitgehenden Datenerhebung einen anderen Vertragspartner suchen, zumal oft eine finanzielle Abhängigkeit von diesem Vertrag besteht. Es ist daher eine objektive Überprüfung und Interessenabwägung vorzunehmen.[832]

Gerade in Bewerbungssituationen ist die Gefahr groß, dass Arbeitgeber versuchen, so viel Daten wie möglich über die Bewerber zu sammeln („*Ausforschungsgefahr*"), da zu diesem Zeitpunkt die Bereitwilligkeit, Informationen Preis zu geben, am größten und eine Fehlbesetzung teuer ist. Der Arbeitgeber hat ein großes Interesse daran, ein vollständiges Persönlichkeitsprofil von Bewerbern zu erstellen,[833] nicht zuletzt, weil es sich beim Arbeitsverhältnis um ein Dauerschuldverhältnis mit höchstpersönlichem Charakter (§ 613 S. 1 BGB) handelt.[834]

Die Praxisrelevanz dieser Einschränkung der „Datenerhebungsmacht" zeigt sich an den vielen Entscheidungen des Bundesarbeitsgerichts zum Fragerecht des Arbeitgebers sowie zur Zulässigkeit von psychologischen Untersuchungen an Bewerbern noch unter Geltung des Vorgängergeset-

829 *Wolff*, A. I. Unionsrechtliche Grundlagen, in: Schantz/Wolff, Das neue Datenschutzrecht, S. 32.

830 Ein Rückgriff auf die allgemeinen Erlaubnistatbestände wird in der Literatur überwiegend als zulässig erachtet, vgl. ErfK/*Franzen*, § 26 BDSG Rn. 4 f.; *Kainer/Weber*, BB 2017, 2740 (2743); *Kort*, NZA 2018, 1097 (1099 f.); *Kramer*, NZA 2018, 637 (638); *Ströbel et al.*, CCZ 2018, 14 (19); so wohl auch LAG Hamm, Beschl. v. 19.09.2017 – 7 TaBV 43/17, ZD 2018, 129 (131) Rn. 35; *Kainer/Weber*, BB 2017, 2740 (2741).

831 *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 19.

832 Siehe bereits **D. § 1 I V. 2. b**).

833 Zum Interessenskonflikt im Arbeitsverhältnis, siehe **A. § 2**.

834 Siehe die Kommentierung zum im Wortlaut nahezu identischen § 32 BDSG a.F., *Seifert*, in: Simitis, Bundesdatenschutzgesetz, § 32 BDSG Rn. 21.

zes.[835] Im Kern prüft das BAG hierbei einzelfallbezogen, ob der Arbeitgeber Daten erhebt, an deren Kenntnis er ein „berechtigtes, billigenswertes und schutzbedürftiges Interesse“[836] hat.[837]

Zu beachten sind zwei Dinge, die sich zur bisherigen Rechtslage verändert haben: Erstens: Trotz der Gesetzesbegründung, wonach die zu § 32 BDSG a.F. entwickelten Grundsätze unter § 26 BDSG n.F. fortgelten sollen, ist die Diskussion um das Fragerecht und sonstige Datenerhebungsmaßnahmen nicht mehr unter dem Gesichtspunkt des berechtigten Interesses an der Beantwortung der Frage durch den Bewerber zu führen, sondern am Stichwort der „Erforderlichkeit für die Entscheidung über die Begründung des Beschäftigungsverhältnisses, § 26 Abs. 1 S. 1 Var. 1 BDSG.[838] Der Prüfungsmaßstab der Abwägung verändert sich allerdings nicht,[839] insofern ist inhaltlich die Auffassung des Gesetzgebers richtig. Zweitens: Die Privilegierung von Daten aus „allgemein zugänglichen Quellen“ (§ 28 Abs. 1 S. 1 Nr. 3 BDSG a.F.) ist weggefallen, sodass die Verarbeitung von Daten insbesondere aus dem Internet mitunter nunmehr erhöhten Voraussetzungen unterliegen könnte.[840] Dagegen spricht, dass die DSGVO grundsätzlich keinen ausdrücklichen Vorrang der Direkterhebung mehr kennt[841] und für sensitive Daten eine Verarbeitungserleichterung in Art. 9 Abs. 2 lit. e DSGVO ausdrücklich aufgenommen wurde[842]. Eine solche muss in der Abwägung dann *erst recht* für nicht-sensitive Daten berücksich-

835 Eine Darstellung der Einzelfragen der Datenerhebung würde hier den Rahmen sprengen, sodass auf die unzähligen Spezialbeiträge in der rechtswissenschaftlichen Literatur verwiesen wird. Vgl. daher die ausführliche Kommentierung von *Seifert*, in: Simitis, Bundesdatenschutzgesetz, § 32 BDSG Rn. 22 ff. m.w.N.; ebenso den ausführlichen Aufsatz von *Gola*, RDV 27(3) (2011), 109.

836 *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 22; *Gola*, NZA 2019, 654 (655).

837 Vgl. u.a. BAG, Urt. v. 13.06.2002 – 2 AZR 234/01, NZA 2003, 265 (266).

838 Insofern wurde die sog. „Informationserhebungsfreiheit des Arbeitgebers“ grundsätzlich abgeschafft und durch das allgemeine Verbot des Art. 6 DSGVO ersetzt, vgl. BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 72.

839 *Seifert*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 88 DSGVO Rn. 77 f.

840 So wohl *Schwarz*, ZD 2018, 353 (354).

841 So auch *Däubler*, Digitalisierung und Arbeitsrecht, § 4 Rn. 11 f., der hierdurch zum Ergebnis gelangt, dass die Grenzen des Fragerechts aufgrund eines stärkeren Eingriffs in das Persönlichkeitsrecht weiterhin eingehalten werden müssen.

842 *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 61; ErfK/*Franzen*, § 26 BDSG Rn. 19.

tigt werden. Im Ergebnis gilt also derselbe Maßstab wie unter § 32 Abs. 1 BDSG a.F.[843]

Die Prüfung der „Erforderlichkeit" im Sinne des § 26 Abs. 1 BDSG erfolgt vierstufig: In einem ersten Schritt wird überprüft, ob der Arbeitgeber mit der Datenerhebung/-verarbeitung einen *legitimen Zweck* verfolgt. Im Anschluss daran wird geprüft, ob die Datenverarbeitung zur Erreichung dieses Zwecks auch *geeignet*, also zweckförderlich, ist. Im dritten Schritt wird die *Erforderlichkeit* geprüft, m.a.W., ob es kein milderes und gleich geeignetes Mittel zur Erreichung des Zwecks gibt.[844] Im Anschluss daran wird die *Angemessenheit* oder Verhältnismäßigkeit der Datenverarbeitung geprüft.[845] All diese Punkte erfolgen unter dem (im vorliegenden Fall europarechtlich geprägten[846]) Tatbestandsmerkmal der Erforderlichkeit. Im Rahmen der Abwägung[847] der widerstreitenden (Grundrechts-)Positionen soll versucht werden, praktische Konkordanz zu erreichen, also einen möglichst schonenden Ausgleich unter weitestgehender Berücksichtigung der gegenläufigen Interessen.[848]

Letztlich wird die Eingriffsintensität im Einzelfall geprüft, wobei mögliche Kriterien der Umfang der Verarbeitung, die Anlassbezogenheit, Dauer der Datenverarbeitung, Persönlichkeitsrelevanz der Daten, Verknüpfungsmöglichkeiten sowie mögliche Folgen sein können.[849]

Beispiel: Im Rahmen des Fragerechts des Arbeitgebers wird immer geprüft, ob die Fragen einen Bezug zum konkreten Beschäftigungsverhältnis aufweisen (Anlassbezogenheit) oder dem privaten Bereich zuzuordnen sind. Fragen zur sexuellen Orientierung sind aufgrund der hohen Persönlichkeitsrelevanz unzulässig. Ebenso darf der Arbeitgeber nur so viel Daten

---

843 *Däubler*, Digitalisierung und Arbeitsrecht, § 4 Rn. 12; i.E. ebenso *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 61; ErfK/*Franzen*, § 26 BDSG Rn. 19; wohl auch *Kainer/Weber*, BB 2017, 2740 (2743 f.).

844 *Schwarz*, ZD 2018, 353 (354).

845 *Hamann*, Kapitel 6: Datenschutzrecht, in: Arnold/Günther, Arbeitsrecht 4.0, Rn. 46.

846 *Schwarz*, ZD 2018, 353 (354): Der Begriff der Erforderlichkeit ist unionskonform auszulegen.

847 Kritisch betreffend den Begriff der „Abwägung", *Pötters*, in: Gola, Datenschutz-Grundverordnung, Art. 88 DSGVO Rn. 51.

848 Vgl. BT-Drs. 18/11325, S. 97. Dies ist ein Ausfluss des Verhältnismäßigkeitsgrundsatzes, vgl. *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 21.

849 Beispiele aus *Pötters*, in: Gola, Datenschutz-Grundverordnung, Art. 88 DSGVO Rn. 51 und BeckOK DatenSR/*Wolff*, Syst. A. Prinzipien des Datenschutzrechts 61.1 mit weiteren Beispielen.

über den Arbeitnehmer in Erfahrung bringen, wie er für die Entscheidung des Beschäftigungsverhältnisses benötigt (Umfang der Verarbeitung).

Schlussendlich muss der Arbeitgeber bei einem abgelehnten Bewerber die Daten nach einem bestimmten Zeitraum (Dauer der Datenverarbeitung) wieder löschen, da er dann kein berechtigtes Interesse an der Verarbeitung mehr hat und somit die Interessen des Bewerbers überwiegen. Eine dauerhafte Speicherung würde eine hohe Eingriffsintensität für den Betroffenen darstellen.

Mit einer Spezialfrage, nämlich der Erstellung eines Persönlichkeitsprofils auf Basis der erhobenen Daten durch People-Analytics-Maßnahmen, die sowohl im Bewerbungsprozess, aber auch im weiteren Arbeitsverhältnis stattfinden können, erfolgt nachfolgend bei **E. § 1 II. 4** eine vertiefte Auseinandersetzung. Denn hierbei handelt es sich – wie sich zeigen wird – um einen gesonderten Verarbeitungsvorgang, der einer eigenen Legitimationsgrundlage bedarf.

bb) Erforderlichkeit für die Durchführung des Beschäftigungsverhältnisses

Im Rahmen der Datenverarbeitung zur Durchführung des Beschäftigungsverhältnisses ist die soeben angesprochene Ausforschungsgefahr geringer, da der Arbeitgeber den Arbeitnehmer bereits beschäftigt hat. Die Gefahr, dass der Arbeitnehmer dem Arbeitgeber die Daten freiwillig zur Verfügung stellt, ist ebenso kleiner, da Arbeitnehmer, die bereits in einem Beschäftigungsverhältnis stehen, insofern auch nicht mehr mit anderen Bewerbern konkurrieren müssen. Der Anreiz, die eigenen Daten möglicherweise nur (widerwillig) offenbaren, um sich gegen andere Bewerber durchzusetzen, besteht dort nicht mehr. Zudem genießen die Arbeitnehmer in aller Regel Kündigungsschutz durch das KSchG und können ihre Interessen über das „Instrument" des Betriebsrats weitgehend verteidigen.

Eine Datenverarbeitung für diesen Zweck ist jedenfalls erforderlich, wenn der Arbeitgeber diese zur Erfüllung seiner vertraglichen oder gesetzlichen Pflichten oder Wahrnehmung seiner Rechte zwingend benötigt.[850] Jedoch lassen sich auch weitere Verarbeitungsvorgänge unter diesem Tatbestand legitimieren: Der Tatbestand der „Durchführung" des Arbeitsverhältnisses ist weit zu verstehen, sodass alles erfasst ist, was der Zweckbe-

850 BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 114.

stimmung des Arbeitsverhältnisses dient.[851] Aus diesem Grund fällen auch Verarbeitungsvorgänge im Rahmen von *People-Analytics*-Maßnahmen unter diese Zweckbestimmung, wenn diese dazu dienen, das Arbeitsverhältnis in bestmöglicher Form durchzuführen und die notwendige Entscheidungsdaten in wirtschaftlich sinnvoller Weise gewinnen zu können.[852] Für die Feststellung, ob eine Zweckveränderung vorliegt, ist genau zu prüfen, zu welchem Zweck die Daten ursprünglich erhoben wurden und ob von diesem letztlich auch die weitergehende Analyse der Daten abgedeckt ist.

Bei der Datenerhebung im laufenden Beschäftigungsverhältnis entsteht hierdurch eine neue Gefahr, die mit der Ausforschungsgefahr bei der Begründung vergleichbar ist: Die Gefahr der Überwachung und Vorratsdatenspeicherung. Aufgrund des Charakters als Dauerschuldverhältnis und dem weiterhin grundsätzlich fortbestehenden Interessenskonflikt zwischen Arbeitgeber und Arbeitnehmer sind Arbeitgeber dazu geneigt, ihre Arbeitnehmer möglichst engmaschig zu überwachen, um sicherzustellen, dass sie ihrer arbeitsvertraglichen Pflicht zur Leistung nachkommen.[853] Darüber hinaus fallen über die Dauer eines Arbeitsverhältnisses unzählige (personenbezogene) Daten, meist als Nebenprodukte der Arbeitsleistung, an. Diese können – aus rein technischer Sicht – einfach für Auswertungen genutzt werden.

Vor diesem Hintergrund wird es auch verständlich, dass Arbeitgeber dazu neigen, nicht nur Daten zu erheben, die aktuell benötigt werden, sondern auch welche, die in einer prospektiven Betrachtung möglicherweise von Nutzen sein können. Für die Beurteilung der Zulässigkeit muss daher exakt zwischen erforderlicher Datenverarbeitung und unzulässiger Vorratsdatenspeicherung unterschieden werden.[854] Grundsätzlich ist ein berechtigtes Interesse des Arbeitgebers anzuerkennen, für die Personalplanung und -entwicklung Daten von Arbeitnehmern über einen gewissen Zeitraum zu sammeln, um Veränderungen Rechnung tragen

851 *Zöll*, in: Taeger/Gabel, DSGVO - BDSG, § 26 BDSG Rn. 38.

852 Vgl. MHdB-ArbR/*Reichold*, § 96 Datenschutz im Arbeitsverhältnis, Rn. 46 zur Einführung eines Personalinformationssystems unter Verweis auf BAG, Beschl. v. 11.03.1986 – 1 ABR 12/84, AP BetrVG 1972 § 87 Überwachung Nr. 14; a.A. *Götz*, Big Data im Personalmanagement, S. 61 f.: People Analytics im laufenden Beschäftigungsverhältnis fallen nicht unter die Vorschrift, da sie nicht unmittelbar für den Vollzug des Arbeitsverhältnisses benötigt werden.

853 Hierzu bereits **A. § 2 II**.

854 Zu § 32 BDSG a.F.: *Seifert*, in: Simitis, Bundesdatenschutzgesetz, § 32 BDSG Rn. 57.

zu können.[855] Allerdings darf dies nicht als „Blankoermächtigung" zur Datensammlung verstanden werden.[856] Das datenschutzrechtliche Gebot der Datenminimierung (Art. 5 Abs. 1 lit. b und c DSGVO) gilt auch im Arbeitsverhältnis.[857]

Zu beachten ist ferner, dass die Datenverarbeitung einen Beschäftigungsbezug aufweisen muss. Daten, die der Privatsphäre des Beschäftigten zuzuordnen sind, können deshalb nicht unter dem Zweck „Durchführung des Beschäftigungsverhältnisses" verarbeitet werden. Prominente Beispiele sind Angaben zu Freizeitbeschäftigungen, Hobbys, persönliche Interessen, aber auch Konsumverhalten etc.[858]

Ob ein bestimmtes Datum erhoben und verarbeitet werden darf, muss im Einzelfall anhand der unter **aa**) genannten Kriterien überprüft werden; eine Generalisierung ist hierbei nicht möglich.

cc) Erforderlichkeit für die Beendigung des Beschäftigungsverhältnisses

Unter Beendigung des Beschäftigungsverhältnisses ist die Vorbereitung, Durchführung und Abwicklung zu verstehen.[859] Hier sind in den meisten Fällen keine neuen Daten mehr zu erheben, es sei denn, dass ein Straftatverdacht vorliegt (§ 26 Abs. 1 S. 2 BDSG) und der Arbeitgeber noch die notwendigen Beweise benötigt, um eine Kündigung darauf zu stützen.

In aller Regel können aber bereits bestehende Daten nochmals genutzt werden, wenn ein Arbeitsverhältnis betriebs-, verhaltens- oder personenbedingt beendet wird. So werden bestimmte Daten zur Sozialauswahl nach § 1 Abs. 3 S. 1 KSchG benötigt.[860] Die Prüfung der Erforderlichkeit ist analog der Begründung und Durchführung durchzuführen. Für die Zweckänderung ist § 24 BDSG von besonderer Bedeutung (hierzu unten **E. § 1 I. 3**).

855 Hierzu auch BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 117.
856 *Seifert*, in: Simitis, Bundesdatenschutzgesetz, § 32 BDSG Rn. 58.
857 BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 67.
858 *Seifert*, in: Simitis, Bundesdatenschutzgesetz, § 32 BDSG Rn. 59 f.
859 Vgl. hierzu BT-Drs. 16/13657, S. 21.
860 BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 189; ausführlich *Seifert*, in: Simitis, Bundesdatenschutzgesetz, § 32 BDSG Rn. 135 ff.

dd) Zwischenergebnis

Die möglichen Zweckbestimmungen des § 26 BDSG sind weitreichend. Allerdings sind diese – wie sich bereits aus dem Wortlaut der Norm ergibt – auf das konkrete Beschäftigungsverhältnis bezogen. Es muss also immer am konkreten Arbeitsverhältnis geprüft werden, ob eine Erhebung und Verarbeitung der Daten notwendig ist, um über *dieses* Beschäftigungsverhältnis zu entscheiden, es durchzuführen oder abzuwickeln.[861] Weitergehende Analysen beispielsweise zur Berechnung des zukünftigen Personalbedarfs oder der Fluktuationsquote für bestimmte Stellen, Abteilungen oder des Unternehmens sind vom ursprünglichen Erhebungszweck grundsätzlich nicht gedeckt und lassen sich nicht unter die Zweckbestimmungen des § 26 BDSG fassen.[862] Hier gilt Art. 6 Abs. 1 lit. f DSGVO. Lediglich im Rahmen der Personalplanung und -entwicklung könnte die Zweckbestimmung weitergehende Analysen erfassen, sofern es um die Einsatzplanung und Entwicklung des konkreten Mitarbeiters geht.[863]

2. Vereinbarkeit des weitergehenden Verarbeitungszwecks mit dem ursprünglichen Zweck (Art. 6 Abs. 4 DSGVO)

Für *Analytics*-Maßnahmen, die auf personenbezogenen Daten basieren, die für einen anderen Zweck erhoben wurden, ist daher eine Zweckvereinbarkeitsprüfung anhand der oben aufgeführten Kriterien nach Art. 6 Abs. 4 DSGVO vorzunehmen. Zu beachten ist hierbei, dass die dort genannten Prüfungspunkte nicht abschließend und sehr vage sind, was eine praktische Anwendung schwierig macht.[864]

861 So bereits zu § 28 BDSG a.F. *Lambrich/Cahlik*, RDV 2002, 287 (290).
862 So wohl auch *Hamann*, Kapitel 6: Datenschutzrecht, in: Arnold/Günther, Arbeitsrecht 4.0, Rn. 55.
863 Zustimmend für Leistungsdaten unter altem Datenschutzrecht *Lambrich/Cahlik*, RDV 2002, 287 (290 f.).
864 *Hamann*, Kapitel 6: Datenschutzrecht, in: Arnold/Günther, Arbeitsrecht 4.0, Rn. 55 f.

a) Notwendigkeit einer Rechtsgrundlage für die Weiterverarbeitung

Neben der Zweckvereinbarkeitsprüfung benötigt es einen Erlaubnistatbestand,[865] da es sich bei der Weiterverarbeitung der personenbezogenen Daten um einen eigenen, gesondert zu beurteilenden Verarbeitungsvorgang handelt. Hiervon scheint Erwägungsgrund 50 S. 2 eine Ausnahme zu machen: Wenn die Verarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, soll keine andere gesonderte Rechtsgrundlage erforderlich sein als diejenige für die Erhebung der personenbezogenen Daten.

Überwiegend wird aufgrund Erwägungsgrund 50 in der Literatur argumentiert, dass angesichts des klaren Wortlauts keine neue Rechtsgrundlage für die Verarbeitung erforderlich sei; die Zweckvereinbarkeit also die Weiterverarbeitung ohne (erneute) Legitimation erlaube.[866] Als Argument wird die Systematik von Art. 5 Abs. 1 lit. b DSGVO und Art. 6 Abs. 4 DSGVO angegeben, denn Art. 6 Abs. 4 setzte deutlich voraus, dass eine Rechtsgrundlage für die Verarbeitung zu geänderten Zwecken nicht vorliege und formuliere dann die Voraussetzungen, wonach eine Verarbeitung dennoch möglich ist.[867] Zudem handle es sich um eine Weiterverarbeitung und nicht um eine neue Verarbeitung, weshalb diese keiner neuen legitimierenden Grundlage bedürfe.[868] Bei einem anderen Verständnis bliebe für Art. 6 Abs. 4 kein Anwendungsbereich mehr.[869]

---

865 *Franzen*, EuZA 2017, 313 (326 f.).

866 *Franzen*, EuZA 2017, 313 (327); *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 340; *Kühling/Martini*, EuZW, 448 (451); *Spindler*, DB 2016, 937 (943); HK DSGVO/BDSG (2018)/*Schwartmann*, Art. 6 DSGVO Rn. 186; *Eichenhofer*, PinG 2017, 135 (139); *Monreal*, ZD 2016, 507 (510); *Richter*, DuD 2016, 581 (584); *Roßnagel et al.*, Datenschutzrecht 2016 - "smart" genug für die Zukunft?, S. 158; *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, S. 210; einschränkend *Spindler/Dalby*, in: Spindler/Schuster, Recht der elektronischen Medien, Art. 6 DS-GVO Rn. 22: Der Verantwortliche wird nicht davon entbunden, alle Rechtmäßigkeitsanforderungen der ursprünglichen Verarbeitung einzuhalten wie beispielsweise mindestens eine Bedingung der Rechtmäßigkeit nach Art. 6 Abs. 1 lit. a-e.; wohl auch Plath/*Plath*, Art. 6 DSGVO Rn. 133; nunmehr hiergegen HK DSGVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Abs. 4 DSGVO Rn. 235.

867 *Franzen*, EuZA 2017, 313 (327).

868 *Monreal*, ZD 2016, 507 (510).

869 HK DSGVO/BDSG (2018)/*Schwartmann*, Art. 6 DSGVO Rn. 186; HK DSGVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Abs. 4 DSGVO Rn. 235: Art. 6 Abs. 4 DSGVO ist eine Auslegungsregel über die Zulässigkeit der Zweckänderung.

Dagegen wird argumentiert, dass im Rahmen der Zweckvereinbarkeit grundsätzlich eine *zweistufige* Prüfung erfolge, nämlich zunächst (1) eine Prüfung, ob der neue Zweck mit dem ursprünglichen Zweck vereinbar und damit für den Betroffenen weiter vorhersehbar ist und ferner (2) ob für die weitergehende Weiterverarbeitung eine Rechtsgrundlage bestehe.[870] Aus Art. 5 Abs. 1 lit. a DSGVO folge nichts anderes, denn die Norm verankere die Zweckbindung und stelle keinen Erlaubnistatbestand dar; Erwägungsgrund 50 stelle lediglich klar, dass die Verarbeitung ebenfalls auf die ursprüngliche Rechtsgrundlage gestützt werden könne und ein „gesonderter" Legitimationstatbestand nicht zwingend notwendig ist.[871] Bei Erwägungsgrund 50 handle es sich im Übrigen um ein Redaktionsversehen[872], welches aus den Trilog-Verhandlungen herrühre, da die Kommission und der Rat in größerem Umfang als unter der DS-RL Datenverarbeitungen erlauben wollten,[873] sich jedoch gegenüber der strikteren Auffassung des Parlaments nicht haben durchsetzen können.[874] Eine andere Auffassung wäre zudem „kaum" mit Art. 7 und 8 EU-GRC vereinbar.[875]

Die überwiegende Literaturauffassung überzeugt aus mehreren Gründen nicht: Zunächst spricht Erwägungsgrund 50 immer wieder von der „Erhebung" der Daten. Dies ist auch stimmig, denn bei einer zulässigen (zweckvereinbaren) Weiterverarbeitung kann auf die unter anderem Zweck erhobenen Daten zurückgegriffen werden, ohne diese zuerst wieder neu erheben zu müssen. Somit können sich Verarbeiter die erneute Erhebung beim Betroffenen sparen. Keinesfalls kann die Regelung des

---

870 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 76 Rn. 53 f.; *Schantz*, NJW 2016, 1841 (1844); *Albrecht*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 DSGVO Rn. 12; *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 183; Ehmann/Selmayr/*Heberlein*, Art. 6 DSGVO Rn. 53; Sydow/*Reimer*, Art. 6 DSGVO S. 69; *DSK*, Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO, <www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/12/20191209_Erfahrungsbericht-zur-Anwendung-der-DS-GVO.pdf>, S. 13 f.

871 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 76 Rn. 54.

872 A.A. *Monreal*, ZD 2016, 507 (510): Wer Erwägungsgrund 50 als redaktionellen Fehler werte, verkenne das europäische Verständnis des Begriffs der Verarbeitung.

873 Siehe hierzu *Albrecht*, CR 2016, 88 (92); a.A. *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 3: *„Der Vorschlag des Rates zur Rechtfertigung der Zweckänderung in seinem Abs. 4 wurde in die DSGVO dagegen nicht übernommen. Eine Erläuterung der Vorschrift findet sich in EG 50."*

874 *Schantz*, NJW 2016, 1841 (1844).

875 *Schantz*, NJW 2016, 1841 (1844).

Art. 6 Abs. 4 DSGVO jedoch eine Abweichung des Grundsatzes in Abs. 1 darstellen.[876] Auch in systematischer Hinsicht baut Abs. 4 auf Abs. 1 auf.[877] Folgte man der erstgenannten Auffassung, so wäre auch der Grundsatz der Rechtmäßigkeit der Datenverarbeitung ausgehoben. Dies hätte beispielsweise im Arbeitsverhältnis zur Folge, dass Daten, die zunächst für die Zwecke der Begründung des Arbeitsverhältnisses erforderlich waren, ohne jegliche weitere Erforderlichkeitsprüfung weiterverarbeitet werden könnten, sobald Zweckvereinbarkeit bestünde. Dies stünde nicht im Einklang mit dem datenschutzrechtlichen Erlaubnisvorbehalt aus Art. 8 Abs. 1 S. 1 EU-GRC. Letztlich spricht für die Notwendigkeit einer weiteren Legitimationsgrundlage auch der Wortlaut des Art. 6 Abs. 1 DSGVO, wonach eine Datenverarbeitung *nur* zulässig ist, wenn eine der dort genannten Bedingungen einschlägig ist. Weder Abs. 1 noch Abs. 4 machen hiervon eine Ausnahme.[878] Auch das teilweise vorgebrachte Argument, dass Art. 5 Abs. 1 lit. b DSGVO ein genau solches Verständnis voraussetze,[879] überzeugt bei näherer Betrachtung nicht: Art. 5 Abs. 1 lit. b DSGVO spricht von einer Zulässigkeit der *Weiter*verarbeitung bei Zweckvereinbarkeit. Liegt eine Zweckvereinbarkeit im Sinne von Art. 6 Abs. 4 DSGVO nicht vor, so ist es nicht zulässig, die bereits erhobenen Daten weiterzuverarbeiten. Stattdessen muss ein komplett neuer Datenverarbeitungsprozess (inklusive Datenerhebung) gestartet werden.[880] Insofern hat Art. 6 Abs. 4 DSGVO auch bei engerem Verständnis noch einen bedeutenden Anwendungsbereich. Für die Gegenauffassung könnte lediglich die etwas missglückte Formulierung der Art. 13 Abs. 3 und Art. 14 Abs. 4 DSGVO sprechen, wonach bei einer Zweckveränderung vor der Weiterverarbeitung *Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen […] zur Verfügung* zu stellen sind. Dies ließe sich so interpretieren, dass eine veränderte Rechtsgrundlage gerade nicht bestehe, da im Gegensatz Art. 13 Abs. 1 lit. c und Art. 14 Abs. 1 lit. c DSGVO die Rechtsgrundlage explizit aufführen. Die Verpflichtung zur Information fehlt al-

876 *Albrecht*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 DSGVO Rn. 13; im Ergebnis wohl auch *Spindler/Dalby*, in: Spindler/Schuster, Recht der elektronischen Medien, Art. 6 DS-GVO Rn. 22.

877 Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 19.

878 *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 183.

879 *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, S. 210.

880 *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 185.

lerdings auch bei der Auskunft nach Art. 15 Abs. 1 lit. a DSGVO, obwohl kein überzeugender Grund hierfür ersichtlich ist und ein legitimes Interesse des Betroffenen besteht, zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung auch diese Information zu erlangen.[881] Insofern darf dem fehlenden Verweis nicht zu viel Aussagekraft beigemessen werden. Bei einer veränderten Rechtsgrundlage wäre daher auch nach Art. 13 f. DSGVO darüber zu informieren.[882]

Letztlich führt die Gegenauffassung auch zu Folgeproblemen, wenn der ursprüngliche (Erhebungs-)Zweck und der Weiterverarbeitungszweck nicht mehr kohärent sind: Unklar sind die Anforderungen an die Datenerhebung, die Pflichten des Verantwortlichen sowie die Rechte der Betroffenen.[883]

Im Ergebnis ist also festzuhalten, dass bei Zweckvereinbarkeit die Daten weiterverarbeitet werden dürfen, wenn für die weitere Verarbeitung die Rechtmäßigkeitsvoraussetzungen des Art. 6 Abs. 1 DSGVO oder § 26 Abs. 1 BDSG vorliegen.[884] Nicht in jedem Fall ist eine andere Legitimationsgrundlage erforderlich, beispielsweise dann, wenn es sich um eine mit dem ursprünglichen Zweck vereinbare, erforderliche Datenverarbeitung im Rahmen der Vertragsdurchführung handelt.[885] So können beispielsweise Daten im Rahmen des Vertragsschlusses erhoben worden sein, ebenso aber für die Durchführung erforderlich sein. In diesem Fall bedarf es dann keiner anderen Rechtsgrundlage als Art. 6 Abs. 1 lit. b DSGVO oder im Arbeitsverhältnis § 26 Abs. 1 BDSG. In jedem Falle ist der Betroffene nach Maßgabe der Art. 13 Abs. 3 sowie Art. 14 Abs. 4 DSGVO zu informieren. Im „Erfahrungsbericht der unabhängigen Datenschutzbehörden des Bundes und der Länder zur Anwendung der DS-GVO“ (2019) wird sogar eine Streichung des Erwägungsgrund 50 S. 2 DSGVO empfohlen sowie eine

881 *Bäcker*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 15 DSGVO Rn. 13.

882 *Dix*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 15 DSGVO Rn. 21.

883 Wie *Roßnagel* richtigerweise feststellt, sich dennoch aber der Gegenauffassung anschließt und die Lösung dieser Probleme geschickt umgeht, indem er argumentiert, dass es an der Zweckvereinbarkeit fehle, wenn die Probleme nicht gelöst werden könnten, vgl. *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 13, 64.

884 So auch Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 17, 19.

885 Bzw. den mit der Erhebung begonnen Verarbeitungsvorgang fortsetzt, vgl. Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 20.

weitere Klarstellung in Art. 6 Abs. 4.[886] In diesem Rahmen sollten auch die Art. 13 Abs. 3, 14 Abs. 3 DSGVO angepasst werden.

b) Grundlegendes

Die nicht-abschließend aufgezählten Kriterien des Kompatibilitätstests in Art. 6 Abs. 4 DSGVO („*unter anderem*“) werden als „bewegliches System“[887] angewendet, d.h. je mehr Kriterien erfüllt sind, desto eher wird eine zweckverändernde Verarbeitung zulässig sein.

Unabhängig des Kompatibilitätstests ist eine zweckändernde Verarbeitung zulässig, wenn sie auf der Einwilligung („*Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurde, nicht auf der Einwilligung…*“) oder einer entsprechenden mitgliedsstaatlichen oder unionalen Vorschrift[888] (in Deutschland: §§ 23 f. BDSG) beruht.

c) Vermutung der Zweckvereinbarkeit für (anonymisierte) People-Analytics

Eine unwiderlegliche[889] Vermutung zur Zweckvereinbarkeit ist in Art. 5 Abs. 1 lit. b DSGVO festgeschrieben. In der Literatur herrscht Uneinigkeit darüber, ob diese Vermutung unwiderleglich ist. Ein Teil bejaht dies,[890] ohne jedoch hierfür eine nähere Begründung zu liefern. Wiederum ande-

886 *DSK*, Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO, <www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/12/20191209_Erfahrungsbericht-zur-Anwendung-der-DS-GVO.pdf>, S. 14.

887 *Franzen*, EuZA 2017, 313 (327).

888 Art. 6 Abs. 4 DSGVO stellt hierbei keine Öffnungsklausel dar; hierzu und den Anforderungen an solche Vorschriften, vgl. *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 180, 199 f.; a.A. *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 2: „*Abs. 4 enthält im ersten Satzteil eine Öffnungsklausel[…]*“; ausführlich in Rn. 18.

889 *Schantz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 1 DSGVO Rn. 93; Sydow/*Reimer*, Art. 5 DSGVO Rn. 27; a.A. *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 5 DSGVO Rn. 109.

890 *Schantz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 1 DSGVO Rn. 93; Sydow/*Reimer*, Art. 6 DSGVO Rn. 27; unklar *Eichenhofer*,

re lehnen dies ab[891] und führen als Argument den Verweis auf Art. 89 Abs. 1 DSGVO, wonach geeignete Garantien vorzusehen sind. Zudem werde durch die umständliche doppelte Verneinung klargestellt, dass im Einzelfall ein Kompatibilitätstest nach den Kriterien des Art. 6 Abs. 4 DSGVO notwendig sei; im Regelfall dürfte jedoch von einer Vereinbarkeit ausgegangen werden.[892] Gegen letztgenannte Literaturauffassung spricht allerdings ein Vergleich mit der Vorgängernorm Art. 6 Abs. 1 lit. b DS-RL: Hiernach war die Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken *im Allgemeinen* nicht als unvereinbar mit den Zwecken der vorausgehenden Datenerhebung anzusehen, sofern die Mitgliedsstaaten geeignete Garantien vorsehen. Diese Einschränkung hat Art. 5 Abs. 1 lit. b DSGVO nicht mehr: Dort heißt es, dass eine Weiterverarbeitung für die genannten Zwecke als nicht unvereinbar *gilt*. Insofern ist der Wortlaut – entgegen den kritischen Literaturstimmen[893] – klar: Es handelt sich hier – sofern die Voraussetzungen des Art. 89 Abs. 1 DSGVO eingehalten wurden – um eine unwiderlegliche Vermutung („Fiktion") der Zweckvereinbarkeit.

Zurückgeführt werden kann die Ausnahme vom Zweckbindungsgrundsatz wohl auf das *Volkszählungsurteil* des (deutschen) BVerfG, das bereits 1983 festgestellt hat, dass bei der Datenerhebung für statistische Zwecke eine enge und konkrete Zweckbindung der Daten nicht verlangt werden könne: „*Es gehört zum Wesen der Statistik, dass die Daten nach ihrer statistischen Aufbereitung für die verschiedensten, nicht von vornherein bestimmbaren Aufgaben verwendet werden dürfen; demgemäß besteht auch ein Bedürfnis nach Vorratsdatenspeicherung*"[894].

PinG 2017, 135 (140): Bereichsausnahme; noch zur Datenschutzrichtlinie *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 6 Rn. 16 ff.

891 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 5 DSGVO Rn. 109; Paal/Pauly/*Frenzel*, Art. 5 DSGVO Rn. 32 f.; Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 17.

892 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 5 DSGVO Rn. 109.

893 Vgl. *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 5 DSGVO Rn. 109: „*Der Rechtsgehalt der Fiktion der Nichtunvereinbarkeit ergibt sich nicht aus dem Wortlaut der Vorschrift.*".

894 BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1 (47) – Volkszählungsurteil Rn. 166.

Als Ausnahme vom Zweckbindungsgrundsatz ist diese Norm allerdings eng auszulegen.[895] Wie sich aus den Erwägungsgründen 156 ff. ergibt, gelten hierbei strenge Voraussetzungen. So sollen bereits nach Erwägungsgrund 156 S. 4 die Mitgliedsstaaten geeignete Garantien für die Verarbeitung zu den genannten Zwecken vorsehen. Die Verarbeitung zu wissenschaftlichen Forschungszwecken soll gem. Erwägungsgrund 159 „weit" ausgelegt werden, wobei als Beispiele die technologische Entwicklung und Demonstration, die Grundlagenforschung, die angewandte Forschung sowie die privat finanzierte Forschung genannt werden. Wie sich in Erwägungsgrund 157 zeigt, muss die Forschung allerdings dem Gemeinwohl dienen und soll u.a. die Wissensbasis für politische Entscheidung sichern, sodass unternehmerische bzw. private (Optimierungs-)Zwecke im Rahmen von *People Analytics* nicht von dieser Ausnahme erfasst sind.[896]

Bei der Verarbeitung zu statistischen Zwecken beschreibt Erwägungsgrund 162, dass unter dem Begriff „statistische Zwecke" jeder für die Durchführung statistischer Untersuchungen und die Erstellung statistischer Ergebnisse erforderliche Vorgang der Erhebung und Verarbeitung zu verstehen ist, wobei die Ergebnisse für verschiedene Zwecke verwendet werden können.[897] Allerdings sollte das Unionsrecht oder das Recht der Mitgliedsstaaten den statistischen Inhalt, die Zugangskontrolle, die Spezifikationen für die Verarbeitung personenbezogener Daten zu statistischen Zwecken und geeignete Maßnahmen zur Sicherung der Rechte und Freiheiten der betroffenen Personen und zur Sicherstellung der statistischen Geheimhaltung bestimmen. Hierbei dürfen die Ergebnisse keine personenbezogenen Daten, sondern allenfalls aggregierte Daten sein und die Daten bzw. Ergebnisse nicht für Maßnahmen oder Entscheidungen gegenüber einzelnen natürlichen Personen verwendet werden.

Nach Art. 89 Abs. 1 DSGVO kann die *Pseudonymisierung* eine geeignete Verarbeitungsgarantie darstellen, wenn es möglich ist, die Zwecke hierdurch (noch) zu erfüllen. Die Daten müssen *anonymisiert* werden, wenn dies die Zweckerfüllung nicht beeinträchtigt.[898] Dies entspricht in etwa

---

895 *Buchner*, DuD 2016, 155 (157); *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 341; *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 5 DSGVO Rn. 109.

896 *Richter*, DuD 2016, 581 (584).

897 So wurde bereits zur identischen Formulierung in Art. 6 Abs. 1 lit. b DS-RL von der Artikel-29-Datenschutzgruppe vertreten, dass auch kommerzielle Zwecke davon erfasst werden, vgl. *Article 29 Data Protection Working Party*, WP 203, S. 29.

898 Vgl. hierzu auch *Richter*, DuD 2016, 581 (584).

den Garantien aus dem Kompatibilitätstest aus Art. 6 Abs. 4 lit. e DSGVO, wobei die Regelung des Art. 89 Abs. 1 DSGVO wohl strenger zu verstehen sein dürfte, da hier eine Anonymisierung grundsätzlich verpflichtend ist.

Es wird vereinzelt vertreten, dass Big-Data-Analysen nicht als „Statistik" privilegiert würden.[899] Diese Auffassung ist allerdings zu pauschal ablehnend. Zwar ist es korrekt, dass es keinesfalls für die Inanspruchnahme dieser Ausnahme ausreicht, dass die eingesetzten Verfahren lediglich statistischer oder wissenschaftlicher Natur sind.[900] Kommerzielle Anwendungen sind durch die Ausnahme dennoch nicht ausgeschlossen, wie ein Vergleich mit der im Wortlaut identischen Vorgängerregelung sowie die Formulierung von Erwägungsgrund 162 zeigt. Die Ausnahme vom Zweckbindungsgrundsatz war bereits in Art. 6 Abs. 1 lit. b sowie in Erwägungsgrund 29 der DS-RL geregelt. Hierzu nahm die Artikel-29-Datenschutzgruppe Stellung und verdeutlichte, dass auch kommerzielle Zwecke (wie beispielsweise Big-Data-Auswertungen im Rahmen von Marketing-Zwecken) hierunter fallen können.[901]

Für Profiling- und Scoring-Verfahren im Rahmen von *People Analytics* ist die Ausnahme dennoch irrelevant[902], da die Ergebnisse der Verarbeitung weder personenbezogene Daten sein dürfen noch für Maßnahmen oder Entscheidungen gegenüber einzelnen natürlichen Personen verwendet werden dürfen, wie Erwägungsgrund 162 S. 5 bestimmt.

Dies spricht im Übrigen auch dafür, die Ausnahme der „Statistik" nicht zu eng auszulegen, da die von der Gegenauffassung angesprochenen Gefahren lediglich dann greifen, wenn einerseits die Ergebnisse auf Einzel-

899 So *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 342; *Buchner*, 2 Grundsätze des Datenschutzrechts, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 244 Rn. 61; *Götz*, Big Data im Personalmanagement, S. 130; *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, S. 211 unter zweifelhaftem Verweis auf die Kommissionsbegründung zur DS-RL; wohl auch Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 17: Kein Einfallstor für "Big Data"-Analysen.

900 *Buchner*, DuD 2016, 155; *Buchner*, 2 Grundsätze des Datenschutzrechts, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 244 Rn. 61.

901 *Article 29 Data Protection Working Party*, WP 203, S. 29; kritisch *Richter*, DuD 2015, 735 (738); ebenso *Skistims*, 8.2 Rechtsgrundlagen für datenverarbeitende KI, in: Kaulartz/Ammann/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, Rn. 62.

902 Insofern ist Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 17. zuzustimmen.

personen angewandt werden[903] und andererseits der – wie aufgezeigt – nicht überzeugenden Auffassung gefolgt wird, dass es bei einer Zweckvereinbarkeit die Weiterverarbeitung der personenbezogenen Daten keiner Rechtsgrundlage mehr bedarf. Da die Weiterverarbeitung der Daten jedoch weiterhin einer Legitimation bedarf, ist in diesem Rahmen ohnehin immer das Vorliegen einer Einwilligung oder eine andere Notwendigkeit der Nutzung personenbezogener Daten für die Erstellung derartiger Statistiken erforderlich, sodass auch durch die Ausnahme vom Zweckbindungsgrundsatz keine unbegrenzten Analysen stattfinden dürfen. Für öffentliche Statistiken wird die Legitimation in aller Regel in Art. 6 Abs. 1 lit. e DSGVO liegen. Bei Statistiken im Privatsektor bzw. für kommerzielle Zwecke wird Art. 6 Abs. 1 lit. f DSGVO die einschlägige Norm zur Überprüfung der Rechtmäßigkeit sein, da solch anonyme Analysen in aller Regel nicht zur Vertragsdurchführung erforderlich sind (Art. 6 Abs. 1 lit. e DSGVO bzw. § 26 Abs. 1 BDSG).

People Analytics-Verfahren, die allerdings darauf zielen, bestimmte Kennzahlen im Unternehmen zu ermitteln und deren Ergebnisse somit anonyme Daten darstellen, unterliegen der Ausnahme vom Zweckbindungsgrundsatz. Im Ergebnis dürfen daher die personenbezogenen Daten, soweit ein Legitimationsgrund für die Anonymisierung für statistische *People Analytics*-Verfahren besteht, weiterverarbeitet werden.

d) Kriterien des Kompatibilitätstests

Für die genannten Beispiele des *Profiling* und *Scoring* gilt die Vermutung der Zweckvereinbarkeit im Rahmen der „Statistik-Regelung" nicht, sodass für solche Verarbeitungsvorgänge der Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO vorgenommen werden muss, wenn die Daten zu einem anderen Zweck erhoben wurden. Die oben genannten Kriterien der Zweckvereinbarkeit müssen daher einer genauen Analyse unterzogen werden.

903 Vgl. zum Risiko „tiefgehender Einblicke in einzelne Persönlichkeiten" bei einer Ausnahme für kommerzielle Big-Data-Anwendungen *Götz*, Big Data im Personalmanagement, S. 130

aa) Verbindung zwischen den Zwecken der Erhebung und der Weiterverarbeitung (lit. a)

Als erstes Kriterium der Komptabilitätsprüfung nennt Art. 6 Abs. 4 lit. a DSGVO die Verbindung zwischen den Zwecken der Erhebung und der Weiterverarbeitung. In diesem Rahmen muss vor allem der Inhalt der Beziehung zwischen dem Ursprungszweck und dem Weiterverarbeitungszweck betrachtet werden.[904] Insbesondere, wenn die ursprüngliche Verarbeitung bereits die Weiterverarbeitung impliziert oder als nächster logischer Schritt angesehen werden kann, ist dieses Kriterium als erfüllt anzusehen. Hieraus darf jedoch nicht der Gegenschluss gezogen werden, dass bei einem „Missing-Link" eine Weiterverarbeitung nie zulässig wäre.[905]

Zur Beurteilung kann folgende Faustregel angewandt werden: Je kleiner die inhaltliche Distanz zwischen dem ursprünglichen Erhebungs- und dem weitergehenden Verarbeitungszweck ist, desto eher ist von einer Zweckvereinbarkeit auszugehen.[906] Hintergrund ist, dass der Betroffene dann mit der Verarbeitung rechnen und dies gegebenenfalls bei der Entscheidung, die Verarbeitung im ersten Schritt zu erlauben, berücksichtigen kann.[907]

Roßnagel nennt hier einige Beispiele[908]: So soll es zweckvereinbar sein, wenn die Daten der Kunden beispielsweise bei einem entsprechenden Vertrag für selbstlernende Systeme wie Smart Home oder Smart Car weiterverwendet werden, um sich besser an seine Gewohnheiten und Präferenzen anzupassen. Das gleiche gelte bei Social Networks. Etwas anderes gelte allerdings, wenn der Verarbeiter den kommerziellen Wert der Daten ausnutze. Als Beispiel hierfür kann der Verkauf dieser Datensätze z.B. zu Werbezwecken genannt werden.

Für People Analytics kann eine Zweckvereinbarkeit auch im Rahmen von Profiling oder Scoring-Maßnahmen vorliegen, wenn die Daten zum Zwecke der Durchführung des Beschäftigungsverhältnisses erhoben wur-

---

904 *Article 29 Data Protection Working Party,* WP 203, S. 23.

905 So aber *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 36; wie hier *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 205 unter Bezugnahme auf das WP 203.

906 *Article 29 Data Protection Working Party,* WP 203, S. 24.

907 *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 187; ebenso *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 36.

908 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 37 ff.

den. Hier hängt der durch People Analytics verfolgte Zweck der Weiterverarbeitung (Optimierung der Betriebsabläufe, Verbesserung des Betriebsklimas etc.) eng mit dem ursprünglichen Erhebungszweck zusammen, sodass dieses Kriterium grundsätzlich als erfüllt angesehen werden kann.

bb) Zusammenhang, in welchem die Daten erhoben wurden (lit. b)

Als weiteres Kriterium wird der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen genannt. Erwägungsgrund 50 ergänzt das erste und das zweite Kriterium dahingehend, dass es auf die *„vernünftigen Erwartungen der betroffenen Person […] in Bezug auf die weitere Verwendung der Daten*" ankomme, also die Sichtweise des Betroffenen eine maßgebliche Rolle spiele.[909] Erforderlich ist letztlich eine Gesamtbetrachtung der Beziehung, wobei es insbesondere auf die ursprüngliche Verarbeitungssituation ankommt: Je enger und restriktiver die Verarbeitung im Rahmen der Erhebung war, desto enger sind die Grenzen der Weiterverarbeitung.[910]

Eine fehlende Vertragsbeziehung zum Verantwortlichen spricht grundsätzlich gegen eine Zweckvereinbarkeit der Weiterverarbeitung, da es gerade auf diese (Vertrauens-)Beziehung zwischen Verantwortlichem und Betroffenen ankommt.[911] Ebenso wird bei einem langjährigen Vertrauensverhältnis in aller Regel eine Verarbeitung in Form einer Übermittlung an Dritte ausgeschlossen sein.[912]

Des Weiteren ist eine gegenseitige Abhängigkeit entscheidend, insbesondere, ob ein Gleichgewicht der Entscheidungsfreiheit herrscht.[913] Wenn die Betroffenen (faktisch) gezwungen sind, die Daten zu offenbaren, spricht dies eher gegen eine Zweckvereinbarkeit unter diesem Gesichts-

909 *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 188.
910 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 306; *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 188.
911 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 45; Paal/Pauly/*Frenzel*, Art. 6 DSGVO Rn. 49.
912 Paal/Pauly/*Frenzel*, Art. 6 DSGVO Rn. 49.
913 *Monreal*, ZD 2016, 507 (510).

punkt.[914] Dies ist besonders relevant bei Datenverarbeitungen im Beschäftigungsverhältnis.[915]

Der Schluss einer pauschalen Verneinung der Zweckvereinbarkeit bei Ungleichgewicht der Entscheidungsfreiheit darf hieraus allerdings nicht gezogen werden. Gerade für die genannten Profiling und Scoring-Verfahren im Rahmen von *People Analytics* ist besonders auf die Sichtweise des Betroffenen und die vernünftigen Erwartungen im Rahmen einer Arbeitsbeziehung abzustellen. Werden die Verfahren eingesetzt, um „Profile" der Arbeitnehmer zu erstellen, beispielsweise für die Einsatzplanung, mögliche Weiterbildungen, aber auch Leistungsbeurteilungen, so ist dies vernünftigerweise im Rahmen des Beschäftigungsverhältnisses zu erwarten. Solche Verarbeitungsvorgänge erfolgen schließlich nicht zum Nachteil des Beschäftigten, sondern in aller Regel zu einer Optimierung der Arbeitsabläufe, aber auch zur Förderung von Arbeitnehmern. Somit besteht in aller Regel ein gleichgerichtetes Interesse. Jedenfalls aber sind diese Datenverarbeitungen in einer arbeitsvertraglichen Beziehung nicht überraschend für Arbeitnehmer.

cc) Art der personenbezogenen Daten (lit. c)

Als weiterer Aspekt im Rahmen des Kompatibilitätstests ist die Art der personenbezogenen Daten zu berücksichtigen, insbesondere ob sensitive Daten gem. Art. 9 DSGVO oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 DSGVO verarbeitet werden.

Hintergrund ist, dass diese Daten eine besondere Schutzbedürftigkeit haben und ein besonders hohes Risiko bei der Datenverarbeitung besteht. Wie sich bereits aus dem Einschub „*insbesondere*" ergibt, ist die Überprüfung der Sensibilität der Daten nicht auf die beiden Kategorien beschränkt, sondern es können auch andere Daten als besonders schutzbedürftig eingestuft werden, wenn der Aussagegehalt der Daten sehr hoch ist.[916] Als Beispiele werden Kommunikations- und ortsbezogene Daten genannt.[917]

---

914 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 46; *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 206.

915 *Monreal*, ZD 2016, 507 (510).

916 I.E. auch *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 54.

917 *Article 29 Data Protection Working Party*, WP 203, S. 25.

Als Faustregel gilt: Je sensibler die Daten, desto enger ist der Spielraum für eine mögliche Weiterverarbeitung.[918]

Im Rahmen von *People Analytics* dürfte offensichtlich sein, dass sensitive Daten, die dem Arbeitgeber offenbart werden, in aller Regel für weitergehende Analysen ausscheiden, da aufgrund des hohen Risikos eines Missbrauchs der Zweck sehr eng gefasst werden muss. Ein genereller Ausschluss ist aber nicht zwingend: Werden Gesundheitsdaten der Beschäftigten, die der Arbeitgeber im Rahmen von ärztlichen Untersuchungen oder Krankmeldungen erhalten hat, beispielsweise verwendet, um Arbeitsplätze sicherer oder ergonomischer zu gestalten, indem er die Daten nutzt, um besonders risikobehaftete Positionen und typische Krankheiten zu identifizieren, so spricht auch die Art der Daten nicht gegen eine Weiterverwendung dieser Daten außerhalb des Erhebungszweckes „Krankmeldung". Dies gilt insbesondere dann, wenn die Daten ausreichend durch technische und organisatorische Maßnahmen wie Pseudonymisierung und Anonymisierung geschützt werden, sodass negative Folgen für den Beschäftigten ausgeschlossen sind.

dd) Möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen (lit. d)

Als weiterer Aspekt im Rahmen des Kompatibilitätstests sind die zuletzt genannten (möglichen) Folgen der Zweckänderung für die betroffenen Personen zu berücksichtigen. Dabei dürfen nicht nur negative Folgen berücksichtigen werden, sondern auch positive.[919] Zur Beurteilung können die Erkenntnisse aus der Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO genutzt werden.[920] Könnte die Weiterverarbeitung zu einer Diskriminierung führen, so wird diese regelmäßig ausscheiden.[921]

Ein wichtiges Kriterium ist, ob im Rahmen der Weiterverarbeitung Dritte Kenntnis von den personenbezogenen Daten erlangen. Denn in einem solchen Fall ist es für die betroffene Person deutlich schwieriger, abzuschätzen, welche Folgen eine Weiterverarbeitung hat und für welche

---

918 *Article 29 Data Protection Working Party,* WP 203, S. 25.

919 *Article 29 Data Protection Working Party,* WP 203, S. 25; *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 56; *Monreal*, ZD 2016, 507 (511).

920 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 56.

921 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 208.

Zwecke der Dritte die Daten im Rahmen weiterer zweckkompatibler Verarbeitungsvorgange nutzen könnte.[922] So müssen in diesem Zusammenhang auch mögliche emotionale Folgen berücksichtigt werden, wie beispielsweise die Angst, die Kontrolle über die eigenen Daten zu verlieren oder Datenskandalen zu unterliegen.[923]

Bei Maßnahmen der Profilbildung ist zu beachten, dass solche in aller Regel schon bei der Datenerhebung vorhersehbar sind. Deshalb sollten bei der Erfassung hinreichend transparente Informationen gegeben werden sollten, um eine Zweckvereinbarkeit sicherzustellen.[924] Sofern ein konkreter Profiling-Zweck vorgesehen ist, muss dieser bereits bei Erhebung angegeben werden; auf eine Zweckvereinbarkeit kommt es dann nicht mehr an.

Die Art, wie die Daten weiterverarbeitet werden, hat einen großen Einfluss auf die möglichen Folgen für die betroffenen Personen, insbesondere dann, wenn im Rahmen von Profilingmaßnahmen mittels *Big Data* verschiedenartige Datensätze miteinander verknüpft werden. Mögliche Erkenntnisse sind vielfach nicht vorhersehbar (bzw. ist gerade Zweck der Verknüpfung und Analyse unbekannte Zusammenhänge zu entdecken und somit unvorhergesehene Ergebnisse zu erzeugen).[925] Aus diesem Grund wird in der Literatur vertreten, dass dieses Kriterium „im Kontext von Big Data, künstlicher Intelligenz, *selbstlernenden System*, *Kontexterfassung, Internet der Dinge und anderen Anwendungen des Ubiquitous Computing […] nur restriktiv wirken kann.*"[926]

Die Personalakte eines Arbeitnehmers ist ein typisches Beispiel für eine Profilbildung, die vorhergesehen werden kann, ohne dass diese explizit

---

922 Ähnlich *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 190; gegen eine Zweckvereinbarkeit in der Regel daher *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 57 : "*Durch Übermittlungen entsteht das Risiko nicht mehr kontrollierbarer Parallelspeicherungen, für die Schutzmaßnahmen wie Verwertungsverbote, Zugriffsbeschränkungen, Auskunftssperren und ähnliche nicht mehr wirken. Auch entsteht die große Gefahr, dass die Betroffenenrechte auf Berichtigung, Sperrung und Löschung ihre Wirksamkeit verlieren, wenn die Kette der Übermittlungen nicht mehr lückenlos nachvollzogen werden kann oder für die praktische Wahrnehmung der Rechte zu lang wird.*".

923 *Article 29 Data Protection Working Party*, WP 203, S. 25 f.

924 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 208.

925 Vgl. hierzu auch *Article 29 Data Protection Working Party*, WP 203, S. 26.

926 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 56.

als Zweck der Datenerhebung aufgeführt wird. Diese wird in aller Regel elektronisch geführt.

Inwiefern weitergehende Analysen und Profiling- oder Scoring-Maßnahmen vom Zweck abgedeckt sind oder zweckkompatibel sind, hängt vom Einzelfall ab. Grundsätzlich muss aber davon ausgegangen werden, dass betriebsnotwendiges Profiling, z.B. zur optimalen Stellenbesetzung oder gezielten Förderung von Arbeitnehmern zweckkompatibel ist, da die Folgen für den Arbeitnehmer positiver Natur sind. Hier sind die Interessen von Arbeitgeber und Arbeitnehmer in aller Regel gleichläufig: Der Arbeitgeber sucht die optimale Besetzung für eine bestimmte Stelle bzw. möchte seine Arbeitnehmer bestmöglich auf die Stelle ausbilden und Schwächen gezielt ausmerzen. Dadurch profitiert der Arbeitnehmer, der seine Arbeitsaufgaben somit zufriedenstellend ausführen und im Rahmen von Weiterbildungen gezielt auf bestimmte (Beförderungs-)Positionen ausgebildet werden kann. Hierfür spricht auch das Argument, dass in solchen Fällen die Freiwilligkeit einer Einwilligung vermutet wird (§ 26 Abs. 2 S. 2 BDSG).[927]

Bei der weitergehenden Zwecksetzung ist freilich darauf zu achten, dass die Verknüpfung mit anderen Datensätzen so stark wie möglich eingegrenzt wird und eine entsprechende Information stattfindet. Ansonsten sind die Folgen für den Betroffenen unübersehbar und die Zweckkompatibilität ist zu verneinen.

ee) Vorhandensein geeigneter Garantien (lit. e)

Als letzten Prüfungspunkt der beispielshaft aufgezählten Kriterien nennt die DSGVO das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann. Nach Erwägungsgrund 50 S. 6 sollen hierbei sowohl die Garantien beim ursprünglichen Verarbeitungsvorgang als auch bei der Weiterverarbeitung maßgeblich sein. Wie sich bereits an den beiden genannten Verfahren zeigt, sind diese Garantien weniger auf der juristischen Seite als auf der technischen Seite anzusiedeln.[928]

---

927 Dagegen wohl *Rudkowski*, NZA 2019, 72 (73).

928 *Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, Art. 6 DSGVO Rn. 142 Juristische Garantien sind aber nicht ausgeschlossen, wie nachfolgend unter **E. § 1 III. 2. b**) (**2**) begründet wird.

Die „geeigneten Garantien" sind in Zusammenhang mit dem Kriterium der möglichen Folgen aus lit. d zu sehen: Durch technisch-organisatorische Maßnahmen wie Pseudonymisierung oder Verschlüsselung können bei der Weiterverarbeitung der Daten die Risiken für die Betroffenen gesenkt[929] und somit eine zweckändernde Verarbeitung (wieder) legitimiert werden.[930] Dabei kommt es maßgeblich auf die Schutzwirkung der Maßnahmen an.[931] Eine Vereinbarkeit unter diesem Aspekt ist anzunehmen, wenn bei gleichem (Verarbeitungs-)Risiko auch gleichwertige Schutzmechanismen angewandt werden; bei höherem Risiko müssen Daten entsprechend besser geschützt werden.[932] Für Big Data-Anwendungen können nach Auffassung des BfDI die Garantien im Rahmen eine ansonsten inkompatible Weiterverarbeitung sogar ermöglichen.[933]

Für die in dieser Arbeit untersuchten *People Analytics*-Verfahren können – sofern nicht ohnehin von einer Zweckvereinbarkeit aufgrund „Statistik" (wie hier vertreten) ausgegangen wird – solche Garantien, insbesondere die Pseudonymisierung eine Zweckvereinbarkeit herstellen. Wird wirksam anonymisiert (zu den Voraussetzungen siehe bereits **D. § 1 I. 4. b**)), fällt die weitergehende Auswertung nicht mehr in den Anwendungsbereich der DSGVO.[934] Zu beachten ist jedoch, dass der Vorgang der Anonymisierung selbst aber einer Legitimation bedarf.[935] Die zweckändernde Verarbeitung (Verarbeitung der personenbezogenen Daten zu anonymisierten Daten für weitergehende Auswertungen) wird daher aufgrund geeigneter Garantien in aller Regel als zulässig zu erachten sein, wenn das Risiko der Re-Identifikation ausgeschlossen ist.

Im Hinblick auf die eingangs erwähnten Profiling und Scoring-Methoden darf nicht der gleiche Schluss gezogen werden: Es ist gerade erforderlich, dass die Daten personenbezogen, wenn auch in pseudonymisierter Form, bleiben, um die Auswertungsergebnisse einzelnen Arbeitnehmern wieder zuordnen zu können. Denkbar als Verarbeitungsgarantie zur Minderung möglicher Folgen für den Betroffenen ist jedoch eine Aggregati-

929 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 209.
930 *Article 29 Data Protection Working Party*, WP 203, S. 26 spricht hierbei von Kompensation.
931 Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 60.
932 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 60 f.; dagegen wohl Sydow/*Reimer*, Art. 6 DSGVO Rn. 75.
933 *Voßoff/Hermerschmidt*, DANA 2016, 68 (69).
934 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 61.
935 Hierzu nachfolgend **E. § 1 III. 1. a) aa)** und **E. § 1 III. 1. b) aa)**.

on[936] der Daten auf Team- oder Abteilungsebene und somit eine gewisse „Anonymisierung" (auch wenn nicht zwingend vollständige, sofern aufgrund von Ausreißern in den Daten der Team- oder Abteilungsleiter in der Lage wäre, Rückschlüsse auf einzelne Arbeitnehmer zu ziehen). Letztlich ist es dann aber nur noch für bestimmte Personen möglich, Rückschlüsse auf den einzelnen Arbeitnehmer zu ziehen.

3. § 24 BDSG: Nationale Regelung zur Zweckänderung

Eine nationale Sonderregelung zur Zweckänderung stellt § 24 BDSG dar. Sie stellt eine Spezifizierung in Ausfüllung der Öffnungsklausel in Art. 6 Abs. 4 DSGVO dar[937] und schafft somit neben den in Art. 6 Abs. 4 BDSG genannten Zweckänderungsmöglichkeiten zwei weitere Erlaubnistatbestände. Nach § 24 Abs. 1 BDSG ist die Verarbeitung personenbezogener Daten zu einem anderen als dem Erhebungszweck nur zulässig, wenn sie (1.) zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten, alternativ (2.) zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist. In beiden Fällen dürfen die Interessen der betroffenen Person am Ausschluss der Verarbeitung nicht überwiegen.

Unabhängig davon, ob der Weiterverarbeitungszweck nach Art. 6 Abs. 4 DSGVO mit dem ursprünglichen vereinbar ist, darf der Verarbeiter nach § 24 BDSG die Daten für die genannten Zwecke weiterverarbeiten.[938] Die Vorschrift stellt keine Einschränkung des Zweckkompatibilitätstests dar, sondern eine Ausnahme vom strengen Grundsatz der Zweckbindung.[939]

Beide Erlaubnistatbestände sind allerdings für die Arbeit nicht weiter von Bedeutung, da die hier untersuchten Analytics weder dem Zwecke der Gefahrenabwehr für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten dienen noch im Rahmen der Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche eingesetzt werden. Letztere könnten im Rahmen der Datenverarbeitung für die Zwecke der Beendigung des Beschäftigungsverhältnisses erforderlich sein,

936 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 209.
937 *Heckmann/Scheurer*, in: Gola/Heckmann, BDSG, § 24 BDSG Rn. 3; vgl. auch BT-Drs. 18/11325, S. 96.
938 BT-Drs. 18/11325, S. 96; *Herbst*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, § 24 BDSG Rn. 1.
939 ErfK/*Franzen*, § 24 BDSG Rn. 2 f.

wenn beispielsweise ein kündigungsrechtlicher Streit geführt wird oder Schadensersatzansprüche aus Pflichtverletzungen im Arbeitsverhältnis geltend gemacht werden sollen und hierfür IT-Daten zum Nachweis genutzt werden.

4. Zwischenergebnis

Der Grundsatz der Zweckbindung ist der Kern des Datenschutzrechts. Ohne Zweckfestlegung kann die Rechtmäßigkeit der Verarbeitung nicht überprüft werden. Aus diesem Grund ist es von höchster Bedeutung, dass die Zwecke eindeutig und unmissverständlich spezifiziert sowie dem Betroffenen nach Art. 13 und 14 DSGVO mitgeteilt werden. Die Zweckfestlegung erfolgt aber auch zum Selbstzweck des Verarbeiters, der sich hierdurch bereits im Vorfeld Gedanken machen muss, für welche Zwecke er die Daten verwenden möchte und somit mögliche Folgen der Datenverarbeitung (z.B. bei besonders risikobehafteten Verarbeitungssituationen im Rahmen der Datenschutzfolgenabschätzung gem. Art. 35 DSGVO) absehen kann.

Treten mögliche Weiterverarbeitungszwecke auf, die im Rahmen der Datenerhebung noch nicht feststanden, so ist eine Weiterverarbeitung nicht grundsätzlich ausgeschlossen, sondern es muss geprüft werden, ob die weitere Verarbeitung mit dem ursprünglichen Erhebungszweck vereinbar ist. Hierbei wird die Statistik, wobei auch die kommerziell genutzte Statistik, wie beispielsweise anonyme *People Analytics*, durch Big-Data-Auswertungen darunter zu fassen sind, gemäß Art. 5 Abs. 1 lit. b DSGVO privilegiert. Werden die in Art. 89 Abs. 1 DSGVO genannten Verarbeitungsgarantien eingehalten, ist von einer Zweckvereinbarkeit auszugehen.

Für andere Zwecke ist – sofern keine wirksame Einwilligung für die Weiterverarbeitung vorliegt – ein Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO vorzunehmen. Die Verordnung nennt beispielshaft einige Kriterien, die ein Verarbeiter zu prüfen hat: Im Ergebnis ist eine Weiterverarbeitung in der Regel dann zweckkompatibel, wenn diese für den Betroffenen vorhersehbar war und die Folgen sowie Risiken der Weiterverarbeitung möglichst geringgehalten werden. So sind im Bereich der personalisierten *People Analytics*, die nicht unter die Privilegierung der Statistik fallen, durchaus zweckkompatible Weiterverarbeitungen denkbar. Als Beispiele können genannt werden: Arbeitnehmerprofile zur optimalen Stellenbesetzung oder gezielten Förderung. Ebenfalls in begrenztem Maße auch für die gesundheitliche Förderung bzw. Unfallverhütung. Es muss jedoch im-

mer im Einzelfall geprüft werden, ob die Voraussetzungen der Zweckkompatibilität vorliegen.

In jedem Fall muss für die weitergehende Verarbeitung eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO oder § 26 Abs. 1 BDSG vorliegen, sodass keine unbegrenzte Nutzung der Daten für Analytics zulässig ist, sondern – insbesondere im Arbeitsverhältnis – eine erneute Interessensabwägung stattzufinden hat.

II. People Analytics als Profiling im Sinne von Art. 4 Nr. 4 DSGVO

Eine mögliche (Weiter-)Verarbeitungsform stellt das sog. *Profiling* dar, welches in Art. 4 Nr. 4 der Datenschutzgrundverordnung legaldefiniert ist. Es handelt sich um einen gesonderten Verarbeitungsvorgang, der im Kern dazu dient, bestimmte persönliche Aspekte einer Person vorherzusagen.[940] Er unterliegt gegenüber der Verarbeitung der dafür erforderlichen Grunddaten erhöhten Voraussetzungen. Zu beachten ist, dass nicht jede (An-)Sammlung an Daten über eine Person als *Profiling* im Sinne der DSGVO aufzufassen ist, weshalb im Folgenden genau geklärt werden muss, ab wann die hier dargestellten und untersuchten Verarbeitungsvorgänge als *Profiling* gelten und somit gesondert legitimationsbedürftig[941] sind.

1. Grundlagen

Profiling beruht auf der Annahme, dass menschliches Verhalten mathematisch berechenbar ist und sich somit bestimmte Verhaltensweisen und Interessen prognostizieren lassen.[942]

Der Begriff des *Profiling* wurde mit der Datenschutz-Grundverordnung neu eingeführt; weder das BDSG a.F. noch die Datenschutzrichtlinie kannten diesen Begriff. Lediglich für das *Scoring* enthielt § 28b BDSG a.F. eine Regelung, die die Berechnung eines Wahrscheinlichkeitswerts für ein bestimmtes zukünftiges Verhalten des Betroffenen unter gewisse Voraussetzungen stellte. Eine ähnliche Regelung enthält nunmehr § 31

940 Siehe bereits die grundlegenden Ausführungen in **D. § 1 V. 3. b**).
941 Zur Notwendigkeit einer gesonderten Legitimation des Profilings, siehe oben **D. § 1 V. 3. b**).
942 *Härting*, CR 2014, 528 (529).

BDSG.[943] Scoring darf jedoch nicht gleichgesetzt werden mit Profiling. Profiling erfordert im Gegensatz zum Scoring keine Berechnung eines Wahrscheinlichkeitswerts für ein zukünftiges Verhalten; ausreichend ist bereits die Verarbeitung personenbezogener Daten zur Bewertung persönlicher Aspekte. Der DSGVO ist der Begriff des Scorings unbekannt.[944]

Eine eigenständige Rechtsgrundlage hat das Profiling in der DSGVO jedoch nicht.[945] Wie sich aus Erwägungsgrund 72 S. 1 ergibt, unterliegt das Profiling den Vorschriften der Verordnung für die Verarbeitung personenbezogener Daten, wie etwa dem Erfordernis einer Rechtsgrundlage für die Verarbeitung oder der Beachtung der Datenschutzgrundsätze.

Verschiedene Normen in der DSGVO knüpfen an das Profiling an. So haben Betroffene nach Art. 21 Abs. 1 DSGVO ein Widerspruchsrecht, wenn das Profiling auf die Legitimationsgrundlagen Art. 6 Abs. 1 lit. e oder f DSGVO gestützt wird oder es für Direktwerbung genutzt wird (Art. 21 Abs. 2 DSGVO). Nach Art. 35 Abs. 3 lit. a DSGVO ist eine Datenschutz-Folgenabschätzung zwingend vorzunehmen, ohne dass es hierfür einer automatisierten Einzelfallentscheidung bedürfte.[946]

2. Die zwei bzw. drei Stufen des Profilings

Härting beschreibt den Profiling-Vorgang als zweistufigen Vorgang. Danach werden in einem ersten Schritt zunächst die für die Analysen notwendigen Daten erfasst, gespeichert und vorgehalten und in einem zweiten Schritt anhand komplexer Formeln bzw. Algorithmen bestimmte Wahrscheinlichkeiten (Prognosen) berechnet.[947] Je größer die zugrundeliegende Datenbasis, desto aussagekräftiger kann ein Profil werden.

---

943 Spezifisch zum Scoring siehe **E. § 1 III. 2. c) bb)**.

944 *Kort*, RdA 2018, 24 (29).

945 *Veil*, in: Gierschmann et al., Kommentar Datenschutz-Grundverordnung, Art. 4 DSGVO Rn. 1.

946 So auch *Kremer*, § 2 Zulässigkeit der Verarbeitung, in: Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, Rn. 98; a.A. *Veil*, in: Gierschmann et al., Kommentar Datenschutz-Grundverordnung, Art. 4 DSGVO Rn. 3, der verkennt, dass die Formulierung des Art. 35 Abs. 3 lit. a DSGVO gerade nicht erfordert, dass eine automatisierte Einzelfallentscheidung vorliegt Hierfür spricht auch ErwG 60 S. 3 DSGVO, der explizit statuiert, dass der Betroffene über Profilingmaßnahmen zu informieren ist.

947 *Härting*, CR 2014, 528 (529); so auch *Rudkowski*, NZA 2019, 72 (75).

Der Europarat differenziert in seiner Empfehlung zu Profiling sogar noch feingliedriger: In einem ersten Schritt würden die Eigenschaften und das Verhalten von Einzelpersonen digitalisiert überwacht und in großem Umfang gespeichert (sog. *Data Warehousing*). Das Ergebnis der Datenerhebung können pseudonymisierte oder anonyme Daten sein. Im nächsten, zweiten Schritt werden die Daten analysiert und getestet, um Zusammenhänge zwischen verschiedenen Charakteristiken und Verhalten zu erkennen (sog. *Data Mining*). Im letzten, dritten Schritt werden die aus dem Data-Mining-Vorgang gewonnen Erkenntnisse wiederum auf Individualpersonen angewandt, um Prognosen über das Verhalten oder Charakteristiken treffen zu können.[948]

Hinweis: Beiden Definitionen ist gemein, dass sie den Unterschied zum Scoring nach § 31 BDSG nicht trennscharf darstellen. Während das Scoring lediglich Wahrscheinlichkeitswerte über zukünftiges Verhalten betrifft, sind vom weiteren Begriff des Profilings unter anderem auch Wahrscheinlichkeiten für vergangenes Verhalten erfasst.

Zu beachten ist, dass die erste Stufe des Profilings, die Datenerhebung, noch nicht als Profiling im Sinne der DSGVO zu verstehen ist, da unter Profiling lediglich die Bewertung des Verhaltens (meist in Form der Berechnung von Wahrscheinlichkeitswerten) fällt, wie Art. 4 Nr. 4 DSGVO ausdrücklich vorgibt (*„jede Art der automatischen Verarbeitung, die darin besteht […], um bestimmte persönliche Aspekte […] zu bewerten, […]*). Die Datenerhebung unterliegt daher den allgemeinen Rechtmäßigkeitsvoraussetzungen und weitergehende Informationspflichten oder die Pflicht zur Fertigung einer Datenschutzfolgenabschätzung entstehen in diesem Schritt noch nicht. Die Datenbasis, die dem Profiling zugrunde liegt, muss oft nicht gesondert dafür erhoben werden, da diese Daten bereits aus anderen Datenerhebungsvorgängen dem Verarbeiter bekannt sind und ggf. in zweckverändernder Weise weiterverarbeitet werden können.[949]

Der Vorgang des Profilings bzw. die Notwendigkeit, Daten über einen längeren Zeitraum zu speichern, um später weitergehende Analysen an diesen Daten vornehmen zu können, steht dabei grundsätzlich im Widerspruch zum Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c sowie der Speicherbegrenzung aus lit. e DSGVO. Gerade, wenn die Daten nicht im Zeitpunkt der Erhebung für die Zwecke des Profilings bestimmt wurden und daher vorgehalten werden, müssen diese grundsätzlich gelöscht werden, sobald diese nicht mehr erforderlich sind.

---

948 *Council of Europe*, CM/Rec(2010)13, S. 25

949 Hierzu bereits im Detail **E. § 1 I. 2.**

Im Arbeitsverhältnis können als Grundlage beispielsweise die Stammdaten zur Begründung des Arbeitsverhältnisses oder die Verkehrsdaten aus den Serverlogdateien (*Wer hat sich wo wie lange angemeldet? Welche E-Mails gingen von welchem Absender an welchen Empfänger? etc.*) herangezogen werden. Voraussetzung ist – sofern die weitergehenden Auswertungen nicht bereits im Rahmen der Erhebung als Verarbeitungszweck festgelegt wurden –, dass eine Zweckvereinbarkeit besteht.

3. Notwendige Unterscheidung: Profilbildung vs. Profiling

Eine weitere wichtige Unterscheidung, die getroffen werden muss, ist die „Profilbildung" durch eine reine Datensammlung über eine bestimmte natürliche Person und *Profiling* im Sinne der DSGVO. Wie bereits erwähnt, stellt nicht jede Profilbildung zugleich ein Profiling dar. Profiling erfolgt zu dem Zweck, bestimmte Persönlichkeitsaspekte einer Person zu bewerten, in aller Regel, um Aussagen über deren künftiges Verhalten zu treffen.[950] Ein „Profil" kann aber bereits die Personalakte, ein (elektronischer) Lebenslauf oder Social-Media-Profil[951] darstellen, ohne dass in diesem Rahmen Persönlichkeitsaspekte bewertet werden oder künftiges Verhalten vorhergesagt werden soll.

Da nur im Fall des Profilings eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO vorzunehmen ist, ist der Vorgang von der „allgemeinen" Verarbeitung und sortierten Speicherung z.B. in einer Datenbank oder einem Dateisystem nach Art. 4 Nr. 2 DSGVO genau abzugrenzen.

a) Automatisierte Verarbeitung erforderlich

Profiling erfordert, wie sich bereits aus Art. 4 Nr. 4 DSGVO ergibt, eine automatisierte Verarbeitung. Diese ist abzugrenzen von der nichtautomatisierten Verarbeitung, vgl. Art. 2 Abs. 1 DSGVO.

---

950 *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 4 DSGVO Rn. 1.

951 Bei Social-Media-Profilen erfolgt durch den Verarbeiter (z.B. Facebook, Twitter, Instagram etc.) jedoch in aller Regel ein Profiling im Hintergrund, um beispielsweise Freundschaftsvorschläge zu generieren, insbesondere aber um gezielte Werbung anzuzeigen und hierdurch Gewinn erwirtschaften zu können.

Eine bloß manuelle Verknüpfung der Daten zum Zweck der Persönlichkeitsbewertung und -analyse, beispielsweise im Assessment-Center durch Psychologen, ist daher von dieser Vorschrift nicht erfasst.[952]

b) Merkmal: Persönliche Aspekte

Wesentlich für das Profiling ist, dass persönliche Aspekte, die sich auf eine natürliche Person beziehen, verarbeitet werden. Beispielshaft werden in Art. 4 Nr. 4 Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel genannt.[953] Art. 4 Nr. 4 DSGVO knüpft daher die Verarbeitung allein an das verfolgte Ziel, unabhängig vom zugrundeliegenden Datenverarbeitungsvorgang.[954] Scoring ist aufgrund des engeren Anwendungsbereichs (siehe oben) als Unterfall des Profilings einzustufen.[955]

c) Verarbeitungsinhalt: Verarbeitung zum Zwecke der Bewertung

Das Ziel der Verarbeitung muss beim Profiling die Bewertung persönlicher Aspekte einer natürlichen Person sein.[956] Eine Bewertung stellt hierbei noch nicht die Wiedergabe von Information dar, die ein personenbe-

952 Vgl. *Buchner*, 2 Grundsätze des Datenschutzrechts, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 272 Rn. 142. *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 4 Nr. 4 DSGVO Rn. 5; *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 4 DSGVO Rn. 3.

953 Ebenso für eine nicht-abschließende Aufzählung: *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 4 DSGVO Rn. 4; *Zahariev*, PinG 2017, 73 (75 f.); *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 4 Nr. 4 DSGVO Rn. 7.

954 *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 4 Nr. 4 DSGVO Rn. 6.

955 *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 4 Nr. 4 DSGVO Rn. 7.

956 *Artikel-29-Datenschutzgruppe*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679 (WP 251), S. 7; *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 4 DSGVO Rn. 6.

zogenes Datum oder ein Persönlichkeitsmerkmal repräsentiert, sondern erfordert eine Interpretation dieser.[957]

Eine einfache Einteilung von Personen anhand bekannter Merkmale (im Beschäftigungsverhältnis z.B. Statusgruppe, Position, Teilzeit/Vollzeit, Geschlecht u.a.) stellt noch kein Profiling dar, selbst wenn die Einteilung dazu dient, einen zusammenfassenden Blick über die Gruppe der leitenden Angestellten, Vollzeitkräfte oder die Frauenquote im Unternehmen zu erhalten. In diesen Fällen werden keine Vorhersagen oder Schlussfolgerungen über einzelne Personen getroffen, daher liegt keine Bewertung individueller Merkmale und somit kein Profiling vor.[958]

4. Profiling im Arbeitsverhältnis

Die Erstellung einer Personalakte zum Zwecke der Verwaltung des Arbeitsverhältnisses stellt selbst dann kein Profiling dar, wenn es dadurch mit Hilfe der IT möglich ist, die Belegschaft nach Kriterien zu sortieren und filtern, um daraus beispielsweise Statistiken oder Reporte zu generieren. In keinem der genannten Fälle werden persönlichen Aspekte natürlicher Personen im Rahmen automatisierter Verarbeitung *bewertet*. Es liegt auch kein Profiling vor, wenn im Anschluss an diese Sortierung und mit Hilfe der Reporte ein Personalverantwortlicher eigene Schlüsse zieht und daher ein „manuelles Profiling" vorliegt (s.o.).

Beispiel: Es stellt kein Profiling dar, wenn HR-Software einen Bericht über die Fehlzeiten der einzelnen Arbeitnehmer einer Abteilung über die letzten fünf Jahre generiert (und diesen z.B. grafisch darstellt) und der Abteilungsleiter daher den Schluss zieht, dass bestimmte Arbeitnehmer (mit hohen Fehlzeiten) unzuverlässig sind. Es liegt keine Bewertung durch eine automatisierte Verarbeitung vor.

Dieses „klassische Reporting" ist von People Analytics abzugrenzen. Während das genannte Szenario auf Level 2 der eingangs darstellen Automationsstufen der Arbeitnehmeranalyse anzusiedeln ist, beginnen People Analytics erst ab Level 3.[959] Analysen unterhalb Level 3 stellen noch kein Profiling im Sinne der DSGVO dar.

---

957 *Deuster*, PinG 2016, 75 (76); Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 22.

958 *Artikel-29-Datenschutzgruppe*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679 (WP 251), S. 7.

959 Siehe **C. § 2 III**.

Erst ab Level 3 werden sog. *People Models* erstellt, die auf Basis vorhandener Daten Trendanalysen erstellen, wobei diese mit zunehmendem Reifegrad (Level) immer detaillierter werden. Auf Level 4 erfolgt eine Verknüpfung verschiedener Daten zum Zwecke der Feststellung von Korrelationen und ab Level 5 automatisierte Entscheidungen auf Basis der berechneten Daten.

Zu beachten ist jedoch, dass durch eine alleinige Berechnung von Trends, im oben genannten Fall der Fehlzeiten z.B. durch das Verfahren der linearen Regression, keine Bewertung persönlicher Aspekte vorliegt, sondern lediglich die Fehlzeiten für das kommende Jahr prognostiziert werden. Nach der Definition der DSGVO stellt dies ebenfalls kein Profiling dar, sofern diese Daten nicht mit den Fehlzeiten von anderen Arbeitnehmern zum Zwecke der Bewertung verknüpft werden oder mit der durchschnittlichen Fehlzeit automatisiert verknüpft und hierdurch beispielsweise ein „Zuverlässigkeits-Score" für jeden Arbeitnehmer erstellt wird.

Über neuartige Zusatzmodule (z.B. Workforce Analytics für die Personalverwaltungssoftware SAP Success Factors[960]) können sich Arbeitgeber neue Funktionen dazukaufen und Analysemöglichkeiten erweitern. In vielen neuen Modulen findet nunmehr ein Profiling statt, im Zuge dessen über einzelne Arbeitnehmer oder Bewerber entweder ein „Overall-Rating" im Sinne einer Gesamtnote erstellt wird[961] oder die Arbeitnehmer als „Low Performer" bzw. „High Performer" eingestuft werden, um anhand dieser Klassifizierung weitere Schritte planen zu können.[962]

Für ein Profiling muss aber nicht notwendigerweise eine komplexe (und teure) HR-Software eingesetzt werden. Ausreichend, um als Profiling im Sinne der DSGVO zu gelten, wäre es bereits, wenn Personalverantwortliche bzw. Personalanalysten eine entsprechende Excel-Liste führen und dort anhand von Formeln bestimmte Kennzahlen errechnen lassen und diese Kennzahlen zu einer Einteilung in bestimmte Kategorien („unzuverlässig", „oft krank", „extrem förderungswürdiger Arbeitnehmer", „Kün-

960 Vgl. https://www.sap.com/germany/products/human-resources-hcm/workforce-planning-hr-analytics.html#analytics (letzter Abruf am: 29.07.2020).

961 So beispielweise bei der HR-Lösung „Workday" des Herstellers Gartner, vgl. *Sommer*, CuA 2017, 8 (10).

962 SAP Success Factors Workforce Analytics nimmt eine solche Einteilung vor, siehe hierzu die Website des Herstellers, https://www.successfactors.com/products-services/planning-analytics/hr-analytics.html (letzter Abruf am: 13.12.2019). Zur Klassifizierung im Allgemeinen *Schürmann*, Auswertung von Mitarbeiterdaten - (Any)/(No)thing possible?, in: Taeger, Smart world - smart law?, S. 502 f.

digungskandidat“) führen. In diesem Beispielsfall findet keine schlichte Anzeige von Daten mehr statt, sondern eine Interpretation anhand vorgegebener Formeln.

III. Maßstab zur Beurteilung der Rechtmäßigkeit: § 26 BDSG, ggf. Art. 6 Abs. 1 lit. f DSGVO

Für die Beurteilung der Zulässigkeit von People Analytics müssen daher zwei verschiedene Varianten der Analytics beurteilt werden.[963] Auf der einen Seite stehen „einfache“ Analytics (im Folgenden: **Simple People Analytics**) ohne Profiling-Verfahren und weitere Datenerhebungen und auf der anderen die „fortgeschrittenen“ Analytics (im Folgenden: **Advanced People Analytics**), bei welchen in vielen Fällen (aber nicht notwendigerweise) zusätzliche Echtzeitdaten erhoben werden, jedenfalls aber Arbeitnehmer anhand von Algorithmen in bestimmte Kategorien eingeteilt werden bzw. ein Scoring im Sinne einer Notenvergabe stattfindet.

1. Simple People Analytics

Unter dem Topos „Simple People Analytics“ (kurz: **SPA**) werden im nachfolgenden Analyseverfahren betrachtet, die bestimmte Personalkennzahlen ermitteln und beispielsweise anhand linearer Regression Trends vorhersagen, damit Personalverantwortliche hieraus weitere Schlüsse ziehen und Maßnahmen einleiten können.

Beispiel: Im Unternehmen sind die Fluktuationszahlen der vergangenen Jahre bekannt; hieraus wird aus den vergangenen Zahlen mittels linearer Regression eine Vorhersage der Fluktuation für das nächste Jahr berechnet. Ebenso könnten solche Versuche mit Fehlzeiten von Arbeitnehmern auf Monatsbasis gestartet werden, um vorherzusagen, in welchem Monat ein Arbeitnehmer vermutlich wie oft fehlen wird.

Vor allem bei KMUs werden in der Praxis aufgrund der dadurch entstehenden Software-Kosten und dem dafür notwendigen Know-How derzeit wohl keine fortgeschrittenen People Analytics eingesetzt werden. Nichtsdestotrotz besteht auch oftmals dort der Wunsch bzw. das Bedürfnis Perso-

963 Andere Autoren unterscheiden hier zwischen „find“, „grow“ und „keep“, die typische Anwendungsfelder von People-Analytics darstellen würden, vgl. *Götz*, Big Data im Personalmanagement, S. 37.

nalentscheidungen stärker informationsbasiert, anstatt intuitiv zu treffen, da solche Entscheidungen im Durchschnitt eine höhere Vorhersagekraft als Expertenurteile haben.[964]

Vielfach benötigt es als Datenbasis keine personenbezogenen Daten. So beispielsweise, wenn Analytics dazu genutzt werden sollen, die Ursache für eine hohe Fluktuationsquote in bestimmten Bereichen bzw. Zusammenhänge zwischen der Fluktuationsquote und anderen Kennzahlen zu ermitteln. Hierfür reichen vielfach hinreichend aggregierte (und hierdurch anonymisierte) Daten aus. Die durch Analytics erkannten Zusammenhänge können in weiterer Folge wieder dafür genutzt werden, um Maßnahmen zu planen.[965] Sieht der Algorithmus Vorschläge für einzelne (besetzte) Stellen vor, handelt es sich wieder um personenbezogene Daten, jedoch nicht um ein Profiling, da keine Bewertung der einzelnen Stelleninhaber erfolgt, sondern lediglich auf Basis von Kennzahlen bestimmte Empfehlungen für bestimmte Stellen bzw. deren Inhaber vorgeschlagen werden. Letztere wären dann legitimationsbedürftig nach § 26 Abs. 1 BDSG.

Zu beachten ist, dass bereits die Verarbeitung zum Zwecke der Anonymisierung (also das Anonymisieren der personenbezogenen Daten selbst) ein Datenverarbeitungsvorgang im Sinne von Art. 4 Nr. 2 DSGVO und somit legitimationsbedürftig ist.[966] Aus diesem Grund sind bei weitergehender Verarbeitung zum Zwecke der Anonymisierung auch die Kriterien der Zweckvereinbarkeit (Art. 5 Abs. 1 lit. b, Art. 6 Abs. 4 DSGVO) zu prüfen.[967] Erst nach erfolgreicher Anonymisierung[968] unterliegen die Daten nicht mehr den datenschutzrechtlichen Bestimmungen. Möglich ist es aber, bestimmte Daten bereits anonym zu erheben, um somit den Zwischenschritt der (legitimationsbedürftigen) Anonymisierung zu vermeiden.

Sowohl für die Anonymisierung als auch die Nutzung der personenbezogenen Daten kommen verschiedene Legitimationsgrundlagen in Betracht, die im Folgenden näher analysiert werden sollen:

---

964 Vgl. *Jäger/Petry*, Digital HR - Ein Überblick, in: Petry/Jäger, Digital HR, S. 44.

965 *Atabaki/Biemann*, Potenziale der Datenanalyse für HR (People Analytics), in: Petry/Jäger, Digital HR, S. 130.

966 *Article 29 Data Protection Working Party*, Opinion 05/2014 on Anonymization Techniques (WP 216), S. 8; *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 5 Rn. 23; a.A. wohl *Dzida/Groh*, ArbRB 2018, 179 (181).

967 *Article 29 Data Protection Working Party*, Opinion 05/2014 on Anonymization Techniques (WP 216), S. 7.

968 Zu den Voraussetzungen wirksamer Anonymisierung siehe **D. § 1 I. 4. b**).

a) Einwilligung

Die Einwilligung kann grundsätzlich die Datenverarbeitung umfassend legitimieren (Art. 6 Abs. 1 S. 1 DSGVO), wenn die Bedingungen aus Art. 7 DSGVO eingehalten wurden.[969] Im Arbeitsverhältnis ist aufgrund der bestehenden Abhängigkeit die Freiwilligkeit der Einwilligung problematisch, wobei diese nicht von vornherein ausscheidet (hierzu bereits oben **D. § 1 III. 2. a) bb) (2)**).

aa) Einwilligung zum Zwecke der Anonymisierung

Die Einwilligung zum Zwecke der Anonymisierung ist von der Einwilligung für personenbezogene Analytics zu unterscheiden. Durch die Anonymisierung ist es nicht mehr möglich, die Daten des einzelnen Arbeitnehmers diesem zuzuordnen. Aus diesem Grund entsteht für den Arbeitnehmer kein Risiko unmittelbarer nachteilhafter Folgen. § 26 Abs. 2 S. 2 BDSG bestimmt, dass die Freiwilligkeit insbesondere dann vorliegen kann, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird. Es ist nun die Frage aufzuwerfen, ob auch bei „neutralen Einwilligungen", an welche jedenfalls keine unmittelbaren Folgen geknüpft werden können, eine Vermutung für die Freiwilligkeit besteht.

Beispiele für eine Einwilligung für die Nutzung personenbezogener Daten, bei welcher lediglich ein rechtlicher oder wirtschaftlicher Vorteil erlangt wird, sind nach der Gesetzesbegründung die Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung oder die Erlaubnis zur Privatnutzung von betrieblichen IT-Systemen.[970] In der Literatur werden als weitere Beispiele noch die Aufnahme von Beschäftigtendaten in konzernübergreifende Personalentwicklungssysteme oder Firmenrabattsysteme[971] sowie die Weitergabe an Daten zum Zwecke der Sonderzuteilung an Unternehmensaktien[972] genannt.

Ebenso sehen manche Autoren die Einwilligung als wirksam an, wenn der Arbeitnehmer keine Nachteile von der Datenverarbeitung zu befürchten hat.[973] Zu beachten ist in jedem Fall das Koppelungsverbot aus Art. 7

969 Siehe hierzu im Detail **D. § 1 III. 2. a)**.
970 BT-Drs. 18/11325, S. 97.
971 *Ernst*, ZD 2017, 110 (112).
972 *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 132.
973 *Ernst*, ZD 2017, 110 (111 f.).

Abs. 4 DSGVO, wonach die Erfüllung des Vertrags nicht davon abhängig gemacht werden darf, dass die Einwilligung zur Verarbeitung erteilt wird, wenn diese Daten für die Vertragserfüllung nicht erforderlich sind.[974] Da für die Beurteilung der Freiwilligkeit auch die Eingriffstiefe der Verarbeitung entscheidend ist,[975] ist bei der Anonymisierung mangels Eingriff unter diesem Gesichtspunkt von einer Freiwilligkeit auszugehen.

Als weiteres Kriterium für die Beurteilung nennt die Gesetzesbegründung noch die Art des verarbeiteten Datums[976], wobei es hier auch auf die Nähe zum Beschäftigungsverhältnis ankommt (*Verarbeitet der Arbeitgeber die Daten ohnehin und möchte diese nur für einen weiteren Zweck nutzen?*).[977] Bei der Nutzung der Daten zum Zwecke der Anonymisierung ist dies ebenfalls der Fall. Dem Arbeitgeber liegen diese Daten bereits in personenbezogener Form vor, für die weitergehende Nutzung zu Analyticszwecken sollen diese Daten jedoch in anonymisierter Form weiterverarbeitet werden (z.B. um diese unabhängig von bestimmten Datenschutzstandards auch an Konzern- oder Partnerunternehmen im Ausland übermitteln zu können).

Aus diesem Grund ist die Einwilligung durch Beschäftigte für die Zwecke der Anonymisierung grundsätzlich als zulässig zu beurteilen, solange Arbeitgeber keinen Druck auf Beschäftigte ausüben und das Kopplungsverbot des Art. 7 Abs. 4 DSGVO einhalten. Letztlich spricht dafür auch, dass durch *Analytics* vielfach gleichgelagerte Interessen verfolgt werden (§ 26 Abs. 2 S. 2 BDSG), wenn diese genutzt werden sollen, um Arbeitsbedingungen zu optimieren, das Gesundheitsmanagement zu fördern oder Probleme im Betriebsablauf zu entdecken.

Zwar ist die Einwilligung *vor* Abschluss eines Arbeitsvertrages grundsätzlich ausgeschlossen[978]; denkbar ist eine wirksame Einwilligung in solche Analytics allerdings durchaus *mit* Abschluss des Vertrages, z.B. wenn der Arbeitgeber dem Arbeitnehmer (wie in der Praxis häufig) bereits einen einseitig unterzeichneten Arbeitsvertrag zusendet und als Anhang

---

974 Zu weitgehend daher *Seifert*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 88 DSGVO Rn. 218, der von einer generellen Unwirksamkeit der Einwilligung nach § 134 BGB ausgeht, wenn die Datenverarbeitung für den Beschäftigten keinen Vorteil bringt.

975 BT-Drs. 18/11325, S. 97; vgl. auch *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 131.

976 *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 97.

977 Paal/Pauly/*Gräber/Nolden*, § 26 BDSG Rn. 29.

978 Da hier in aller Regel nicht von einer Freiwilligkeit ausgegangen werden darf, hierzu bereits oben **D. § 1 III. 2. a) bb) (2)**.

zum Arbeitsvertrag sich die Einwilligung der Nutzung der Arbeitnehmerdaten zum Zwecke der Analytics einholt. In einem solchen Fall unterliegt der Bewerber grundsätzlich keiner Drucksituation mehr, da er durch die Unterzeichnung des Arbeitsvertrags bereits einen wirksamen Vertrag geschlossen hätte, unabhängig von der beigefügten Einwilligung zur Datennutzung.[979] In diesem Zusammenhang müssen Arbeitgeber jedoch darauf achten, dass im Rahmen der Einwilligung verdeutlicht wird, dass diese nicht Bestandteil des Arbeitsvertrages ist und die Freigabe der Daten für die vorgesehenen Analytics-Zwecke absolut freiwillig ist. Dem Arbeitnehmer muss eine echte Wahlmöglichkeit geboten werden.[980]

bb) Einwilligung für personenbezogene Analytics (ohne Profiling)

Bei der Einwilligung für personenbezogene Analytics liegt die Situation im Vergleich zur eben untersuchten der Anonymisierung anders: Aufgrund der Zuordenbarkeit der Analytics-Ergebnisse muss grundsätzlich von einer gewissen Eingriffsintensität ausgegangen werden und für den Betroffenen ist die Einwilligung kein „neutrales Geschäft" mehr. Etwaige Analytics-Ergebnisse können zu unmittelbaren Folgen für den Beschäftigten führen. Dennoch ist auch in diesem Fall nicht von einer generellen Unwirksamkeit der Einwilligung auszugehen.[981] Auch hier sind die konkreten Analyticszwecke unter die Beispiele aus § 26 Abs. 2 S. 2 BDSG zu subsumieren, sodass – wie sich bereits aus der Gesetzesbegründung ergibt[982] – durchaus wirksame Einwilligungen möglich sind. Ein Beispiel hierfür sind die unter **E. § 3 I** untersuchten persönlichen Dashboards für den Arbeitnehmer ohne Arbeitgeberzugriff auf die Daten. Da bei „Simple People Analytics" kein Profiling vorgenommen wird, ist die Eingriffsintensität mangels Bewertung persönlicher Aspekte geringer.

Nichtsdestotrotz besteht in diesem Fall für den Arbeitgeber eine rechtliche Unsicherheit, da er im Streitfall für die Freiwilligkeit der Einwilligung

979 Etwas anderes könnte gelten, wenn sich der Bewerber aufgrund einer im Arbeitsvertrag vereinbarten Probezeit dazu genötigt fühlt, die Unterzeichnung ebenfalls zu unterschreiben, weil er die Befürchtung hat, ansonsten unmittelbar wieder gekündigt zu werden.

980 Diese muss er auch subjektiv so wahrnehmen können, vgl. *Rudel*, Personalmagazin 2019, 76 (78).

981 So wohl auch BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 118.3: *Erlaubnis [für People Analytics] könnte daher nur eine Einwilligung geben.*".

982 BT-Drs. 18/11325, S. 97.

darlegungs- und beweispflichtig ist.[983] Will sich der Arbeitgeber mit der Einwilligung zusätzlich absichern, so darf es sich nicht um Daten handeln, für die ein Verarbeitungsgebot besteht. Dies wäre beispielsweise bei Daten der Fall, die er für die Erfüllung seiner gesetzlichen Pflichten benötigt (Daten des Arbeitnehmers für die Sozialversicherung etc.).[984] Ferner muss er darauf hinweisen, dass seiner Auffassung nach mehrere Erlaubnistatbestände einschlägig sind, die Einwilligung also als rechtliche Absicherung eingeholt wird.[985] In jedem Falle aber muss der Arbeitgeber bei Einholung der Einwilligung nach § 26 Abs. 3 S. 4 BDSG auf den Zweck der Datenverarbeitung sowie auf das in Art. 7 Abs. 3 DSGVO niedergelegte Widerrufsrecht in Textform aufmerksam machen.

Die Einwilligung eignet sich aufgrund des jederzeitigen Widerrufsrechts daher nur bedingt, da Arbeitgeber im Falle eines Widerrufs sicherstellen müssen, dass die aufgrund der Einwilligung verarbeiteten Daten vollständig für zukünftige Auswertungen aus den Datensätzen entfernt werden. Die darauf basierenden Analysen werden daher unvollständig, weshalb in weiterer Folge zu prüfen ist, ob andere Erlaubnistatbestände einschlägig sein könnten, die nicht dem Widerrufsrecht unterliegen. Nur als letzte Option sollte auf die Einwilligung des Arbeitnehmers zurückgegriffen werden.

b) Erforderlichkeit: Interessensabwägung

Es stellt sich die Frage, ob SPA als erforderlich für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses im Sinne von § 26 Abs. 1 BDSG angesehen werden können. Erforderlich sind Daten grundsätzlich nur dann, wenn der Arbeitgeber ein „berechtigtes, billigenswertes und schutzwürdiges Interesse“[986] an der Verarbeitung der Daten hat.

In diesem Rahmen ist – wie bereits aufgeführt – zu prüfen, ob das zu erreichende Ziel legitim und das eingesetzte Mittel zur Erreichung

983 Siehe bereits **D. § 1 III. 2. a**).

984 Hierzu oben **D. § 1 III. 2. c**).

985 Zur Problematik der Einschlägigkeit mehrerer Erlaubnistatbestände, insbesondere der Möglichkeit der Einholung einer Einwilligung neben einem gesetzlichen Erlaubnistatbestand aus Art. 6 Abs. 1 DSGVO, siehe **D. § 1 III. 1**.

986 So im Ansatz bereits BAG, Urt. v. 05.12.1957 – 1 AZR 594/56, NJW 1958, 516; zuletzt zum Fragerecht des Arbeitgebers Urt. v. 18.09.2014 – 8 AZR 759/13, AP AGG § 15 Nr. 20.

des Ziels geeignet (d.h. zweckförderlich) ist. Im Anschluss muss geprüft werden, ob es das relativ mildeste Mittel zur Erreichung des gewünschten Ziels ist, es also keine milderen, *gleich geeigneten* Mittel gibt. Zuletzt muss das Mittel (*in concreto:* Die Verarbeitung der spezifischen Daten.) auch angemessen sein, wobei in diesem Rahmen die widerstreitenden Interessen der Vertragsparteien bzw. von Verarbeiter und Betroffenen miteinander abgewogen und in praktische Konkordanz gebracht werden müssen.

Zu pauschal und deshalb im Ergebnis falsch wäre es, an dieser Stelle festzustellen, dass die Erhebung und Auswertung von Mitarbeiterdaten zur Personalauswahl und -führung mit Hilfe von größeren Datenmengen und Algorithmen nicht der Durchführung des Beschäftigungsverhältnisses *dient* und deshalb nicht von § 26 BDSG gedeckt sei.[987] Unzweifelhaft dient die Personalplanung und somit die prospektive Betrachtung einzelner Arbeitnehmer der Durchführung des Beschäftigungsverhältnisses, ist aber auch erforderlich, um als Arbeitgeber bei stetig steigendem Wettbewerbsdruck noch konkurrenzfähig zu bleiben.[988]

So hat das BAG bereits im Jahr 1979 festgestellt, dass Arbeitgeber die Eignung, Befähigung und fachliche Leistung der bei ihm beschäftigten Arbeitnehmer beurteilen und diese Beurteilungen in den Personalakten festgehalten werden dürfen.[989] Auch hier handelt es sich um eine Sammlung von Daten, die heutzutage – insbesondere bei einer Sammlung über mehrere Jahre bei einer Vielzahl von Arbeitnehmern – unter den Begriff *Big Data* gefasst würde, sofern die Daten (wie in moderner Personalverwaltungssoftware üblich) schnell und übersichtlich darstellbar sind.

aa) Erforderlichkeit der Anonymisierung

In vielen Fällen reichen dem Arbeitgeber anonyme Daten für Analytics aus[990], sodass er die Daten vor einer Nutzung anonymisieren muss, um weitgehende Privilegien bei der Verarbeitung zu erhalten. Durch die Anonymisierung wird der Personenbezug gelöscht und somit das Risiko für die betroffenen Arbeitnehmer gesenkt. Es handelt sich daher um ein mil-

987 So aber BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 118.3.

988 Insofern widerspricht sich *Riesenhuber* hier selbst, wenn er feststellt, dass die Personalplanung zur Durchführung des Beschäftigungsverhältnisses gehört, ebenso wie Regelbeurteilungen, vgl. BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 117 f.

989 BAG, Urt. v. 28.03.1979 – 5 AZR 80/77, AP BPersVG § 75 Nr. 3.

990 Anwendungsbeispiele nennt *Jentzsch*, HR Performance 2013, 48.

deres, gleich effektives Mittel, wenn hierdurch die gewünschten Zahlen erzeugt werden können.

Zu beachten ist, dass der Vorgang der Anonymisierung selbst legitimiert werden muss,[991] also an den Kriterien des § 26 Abs. 1 BDSG bzw. Art. 6 Abs. 1 lit. f DSGVO bei beschäftigungsfremden Zwecken gemessen werden und somit einer Interessensabwägung standhalten. Das durch Arbeitgeber mit SPA verfolgte Ziel, einen Überblick über die Belegschaft zu be- bzw. erhalten und Personalplanung zu betreiben und hierdurch letztlich das Unternehmen wirtschaftlich zu führen, ist (wie bereits das BAG dargestellt hat[992]) ein legitimes Ziel. Hierdurch übt ein Arbeitgeber nur seine Grundrechte aus Art. 15 und 16 EU-GRC bzw. Art. 12 und 14 GG aus. Die hierfür genutzten Personaldaten (insbesondere Leistung, Eignung, fachliche Befähigung, Beurteilungen) und Methoden der SPA sind für die Erreichung des Ziels auch geeignet. Ebenso gibt es kein milderes, gleich geeignetes Mittel, wenn im Rahmen von SPA lediglich grundlegende Daten über das Arbeitsverhalten von Arbeitnehmern ohne Bewertung für Vergleiche oder Prognosen herangezogen werden. Schließlich werden bei SPA lediglich Vergangenheitswerte interpoliert oder mithilfe linearer Regression fortgeschrieben, um Trends erkennen zu können, ohne dass weitere Bewertungen durch automatisierte Verarbeitung stattfinden. Dies stellt bereits das absolute Minimum an Verarbeitung dar, um wenigstens im Ansatz aussagekräftige Zukunftsdaten zu bekommen.

Geprüft wurde in diesem Schritt lediglich, ob der Verarbeitungsvorgang der Anonymisierung, genauer die Nutzung der personenbezogenen Daten zum Zwecke der Anonymisierung für die weitergehende Nutzung für SPA „erforderlich" ist bzw. einer Interessenabwägung standhält.[993] Personenbezogene Daten werden in diesem Fall nicht weiteren Analysen unterzogen, sondern lediglich anonymisierte Daten, sodass die weitergehenden Analysen nicht mehr am Datenschutzrecht zu messen sind.

Zuletzt muss auch eine Zweckvereinbarkeit des Anonymisierungsvorgangs (nicht: der weitergehenden Analysen, da diese nicht mehr dem Datenschutzregime unterliegen) mit dem Erhebungszweck nach Art. 6

991 So wohl auch *Götz*, Big Data im Personalmanagement, S. 88.

992 BAG, Urt. v. 28.03.1979 – 5 AZR 80/77, AP BPersVG § 75 Nr. 3.

993 Der Vorgang der Anonymisierung ist grundsätzlich legitimationsbedürftig, da zunächst personenbezogene Daten verarbeitet werden zum Zwecke der Entfernung des Personenbezugs, wie hier *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 5 Rn. 23; *Article 29 Data Protection Working Party*, Opinion 05/2014 on Anonymization Techniques (WP 216), S. 8 Diese Problematik übersehen wohl *Dzida/Groh*, ArbRB 2018, 179 (181).

Abs. 4 DSGVO vorliegen. Da weitergehende Analysen dann keine Rückschlüsse auf einzelne Personen mehr zulassen, fällt das Recht auf Privatheit aus Art. 7, 8 EU-GRC (dies entspricht in etwa dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) als mögliches entgegenstehendes Interesse des Arbeitnehmers weg, sodass die Interessenabwägung hier klar zugunsten des Arbeitgebers ausfällt. Mangels negativer Folgen für den Betroffenen (keine Zuordenbarkeit der SPA-Ergebnisse[994] mehr erreichbar), fällt auch die Zweckvereinbarkeitsprüfung nach Art. 6 Abs. 4 DSGVO positiv aus.

bb) Erforderlichkeit der Nutzung personenbezogener Daten für Analytics

Ebenso gibt es Fälle, in denen die Nutzung anonymisierter Daten unmöglich ist, beispielsweise dann, wenn Arbeitgeber konkrete Daten über einzelne Arbeitnehmer benötigen. Hier kann die Personaleinsatzplanung, Personalentwicklung oder mitunter auch das Gesundheitsmanagement genannt werden. Bei letzterem ist zu beachten, dass es sich hier in aller Regel um sog. *sensitive Daten* im Sinne von Art. 9 Abs. 1 DSGVO handelt, die weitgehenden Verarbeitungsbeschränkungen unterliegen.[995]

(1) Nutzung nicht-sensitiver Daten für SPA

Sollen personenbezogene Daten von Arbeitnehmern, die nicht für SPA-Zwecke, aber für die Zwecke des Personalmanagements, erhoben wurden, für Analytics weiterverarbeitet werden, so ist zunächst eine Zweckvereinbarkeitsprüfung nach Art. 6 Abs. 4 DSGVO vorzunehmen. Nicht nur in diesem Rahmen, sondern auch bei der Interessenabwägung im Rahmen der Prüfung des Erlaubnistatbestands für die Verarbeitung sind die geeigneten Garantien, insbesondere die Pseudonymisierung von hoher Bedeutung. Pseudonymisierung ist eine Verarbeitungsgarantie, da sie es

994 Aufgrund des weiten Wortlauts des Art. 6 Abs. 4 lit. d DSGVO ist bei der Zweckvereinbarkeit des Anonymisierungsvorgangs mit dem Erhebungsvorgang auch die Analyse, die selbst dem Datenschutzrecht nicht mehr unterliegt, in die Folgenabschätzung miteinzubeziehen (so wohl auch *Article 29 Data Protection Working Party*, WP 203, S. 26, wo ausdrücklich auf die Anonymisierung als Schutzmechanismus verwiesen wird).

995 Siehe hierzu bereits **D. § 1 V. 1.**

Dritten es unmöglich[996] macht, die Daten einer bestimmten Person zuzuordnen;[997] diese Verarbeitung stellt somit ein geeignetes, milderes Mittel der Datenverarbeitung dar. Dies ist vor allem in Fällen von Datenlecks von besonderer Bedeutung. Für Analytics ist eine solche problemlos möglich, sodass die Verarbeitung unter Pseudonym als milderes Mittel zu erfolgen hat und eine Zuordnung der Ergebnisse zu den Namen (oder Personalnummern) der Beschäftigten erst zum Ende des Verarbeitungsvorgangs wieder erfolgen darf (wenn beispielsweise der Sachbearbeiter die Person auf seinem Bildschirm aufruft).

Da die für SPA genutzten Daten ausschließlich das betriebliche Verhalten oder Stammdaten von Arbeitnehmern betreffen, ist in der Angemessenheitsprüfung, also der Abwägung der jeweiligen Interessen bzw. Positionen von einem Überwiegen der Interessen des Arbeitgebers gegenüber den Geheimhaltungsinteressen des Arbeitnehmers auszugehen, zumal die Datengrundlage dem Arbeitgeber bereits in rechtmäßiger Weise vorliegt[998]. Außer der Fortschreibung bereits bestehender Daten mithilfe einfacher statistischer Methoden erfolgt keine Erzeugung neuer personenbezogener Daten, insbesondere keine Persönlichkeitsbewertung einzelner Arbeitnehmer durch automatisierte Verarbeitungsvorgänge.

Nicht-sensitive Daten dürfen daher im Rahmen von SPA in den hier aufgezeigten Grenzen nach § 26 Abs. 1 BDSG verarbeitet werden, sofern zumindest eine Pseudonymisierung (bspw. in Form einer Verschlüsselung) erfolgt und eine Anonymisierung untunlich ist.

(2) Nutzung sensitiver Daten für SPA

Bei sog. *sensitiven Daten* im Sinne von Art. 9 Abs. 1 DSGVO könnte die Interessensabwägung zu einem anderen Ergebnis führen, da diese Daten – wie bereits dargestellt – einem erhöhten Schutz unterliegen und die Verarbeitung daher deutlich höheren Rechtfertigungsanforderungen unterliegt. Zur Verarbeitung solcher Kategorien von Daten durch Arbeitgeber muss

996 Oder jedenfalls sehr schwer, da eine Zuordnungstabelle zur Auflösung der Pseudonyme erforderlich ist, die für die wirksame Pseudonymisierung von den Daten getrennt (und sicher) aufzubewahren ist.

997 Zu den Voraussetzungen und Wirkungen der Pseudonymisierung, siehe **D. § 1 I. 4. c**).

998 Der Fokus der Arbeit liegt auf der Datenverarbeitung für Analytics-Zwecke, weshalb davon ausgegangen wird, dass die vorhandenen Daten in rechtmäßiger erhoben wurden.

die Verarbeitung gem. § 26 Abs. 3 BDSG zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit oder des Sozialschutzes erforderlich sein. Ferner dürfen entgegenstehende Interessen der betroffenen Beschäftigten nicht überwiegen. Gemäß § 26 Abs. 3 S. 4 BDSG sind bei einer Verarbeitung angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen (§ 22 Abs. 2 BDSG). Hierzu kann u.a. gehören, dass die Daten pseudonymisiert und verschlüsselt werden. Weitere mögliche Maßnahmen sind, dass die an den Verarbeitungsvorgängen beteiligten Personen sensibilisiert werden, der Zugang zu den Daten innerhalb der verantwortlichen Stelle beschränkt wird und Maßnahmen eingeführt werden, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind.

Bei genauerer Betrachtung der in § 22 Abs. 2 BDSG aufgezählten technisch-organisatorischen Maßnahmen (insbesondere der Ziff. 1, 2, 5, 6 und 7) fällt auf, dass diese Maßnahmen trotz des Wortlauts („*soll*“) nicht nur optionale Vorschriften im Rahmen von SPA darstellen, sondern vielmehr zwingend sind. Der Datenverarbeiter hat ein hohes, aber (in Bezug auf die hierdurch entstehenden Kosten) risikoadäquates Datenschutzniveau zu gewährleisten. So erfordert es weder großen technischen noch finanziellen Aufwand, die Server, auf denen solche Daten gespeichert werden, entsprechend dem Stand der Technik zu verschlüsseln, die Datenverarbeitung unter Pseudonymen erfolgen zu lassen und den Zugang zu solchen Daten zu beschränken. Dies sind Grundanforderungen an einen technischen Datenschutz, die bei allen Verarbeitungsvorgängen eingehalten werden sollten, insbesondere aber bei sensitiven Daten zwingend einzuhalten sind.

Schwieriger ist die Frage zu beantworten, ob die Verarbeitung solcher Kategorien von Daten im Rahmen von SPA für der in § 26 Abs. 3 BDSG genannten Rechte und Pflichten erforderlich sind.

Pflichten aus dem Arbeitsrecht könnten sich insbesondere aus den Arbeitsschutzgesetzen sowie § 618 BGB ergeben: So bestimmt § 3 ArbSchG, dass der Arbeitgeber verpflichtet ist, die erforderlichen Maßnahmen des Arbeitsschutzes *unter Berücksichtigung der Umstände* zu treffen, die Sicherheit und Gesundheit der Beschäftigten bei der Arbeit beeinflussen. Dabei hat der Arbeitgeber ebenfalls die Maßnahmen auf ihre Wirksamkeit zu überprüfen und erforderlichenfalls sich ändernden Gegebenheiten anzupassen. § 5 ArbSchG in Verbindung mit § 3 ArbStättV konkretisiert die Pflichten des Arbeitgebers dahingehend, dass er auch eine Gefährdungs-

beurteilung der Arbeitsstätten vorzunehmen hat, wobei alle möglichen Gefährdungen der Sicherheit und der Gesundheit der Beschäftigten zu beurteilen sind, bei der ebenfalls die physischen und psychischen Belastungen zu berücksichtigen sind. Dementsprechend müssen entsprechende Maßnahmen zum Schutz der Beschäftigten getroffen werden. Eine Spezialregelung für Mütter findet sich in § 9 MuSchG, wonach der Arbeitgeber bei der Gestaltung der Arbeitsbedingungen einer schwangeren oder stillenden Frau alle auf Grundlage einer Gefährdungsbeurteilung erforderlichen Maßnahmen für den Schutz der psychischen und physischen Gesundheit der Mutter sowie des Kindes zu treffen hat, die Maßnahmen auf die Wirksamkeit zu prüfen und erforderlichenfalls den sich ändernden Gegebenheiten anzupassen hat.

Daneben sind allgemeine gesetzliche Pflichten des Arbeitgebers zu berücksichtigen, die ihn zum Schutz der Gesundheit der Arbeitnehmer verpflichten (so z.B. §§ 617 ff. BGB und noch relevanter § 62 HGB).[999] Nicht nur gesetzliche Pflichten, sondern auch arbeitsvertragliche (Fürsorge-)Pflichten können den Arbeitgeber zur Erhebung von Gesundheitsdaten berechtigen und verpflichten; § 26 Abs. 3 S. 1 BDSG ist nicht auf gesetzliche Pflichten beschränkt.[1000] So nennt die Gesetzesbegründung ausdrücklich das Beispiel der Verarbeitung von Daten zur Beurteilung der Arbeitsfähigkeit.[1001]

Eine effektive Überprüfung der Wirksamkeit sowie die Reaktion auf verändernde Gegebenheiten ist dem Arbeitgeber aber nur möglich, wenn er bestimmte Gesundheitsdaten des Arbeitnehmers verarbeiten kann. Aus diesem Grund wird man insbesondere im Bereich des Gesundheitsschutzes eine Zulässigkeit der Verarbeitung sensitiver Daten aus den arbeitsschutzrechtlichen Spezialgesetzen in Verbindung mit § 26 Abs. 3 BDSG herleiten müssen. Um nicht nur retroaktiv, sondern aus prospektiv handeln zu können, sind SPA erforderlich, um ggf. steigende Gefährdungen oder verändernde Umstände frühzeitig zu erkennen und gegebenenfalls erforderliche Maßnahmen einleiten zu können. Allerdings muss in diesem Zusammenhang genau darauf geachtet werden, *welche Daten* zwingend für den Gesundheitsschutz erforderlich sind, denn nur solche dürfen nach § 26 Abs. 3 BDSG durch Arbeitgeber im Rahmen von Simple People Analytics verarbeitet werden. Bei diesen Daten sprechen auch gewichtige Belange der Beschäftigten (z.B. das Grundrecht auf körperliche Unversehrtheit aus

999 *Martini/Botta*, NZA 2018, 625 (632 f.).
1000 *Wybitul*, NZA 2017, 413 (417); *Martini/Botta*, NZA 2018, 625 (633).
1001 BT-Drs. 18/11325, S. 98.

Art. 3 Abs. 1 EU-GRC bzw. Art. 2 Abs. 2 S. 1 GG) für eine Verarbeitung der Daten; hier ist weitestgehend von einem Gleichlauf der Interessen auszugehen, sodass eine Verarbeitung der Daten für diese Zwecke unter den genannten Voraussetzungen grundsätzlich als zulässig zu betrachten ist.

Sollen Daten hingegen nur zur Gesundheitsvorsorge verarbeitet werden, so ist darauf zu achten, dass eine solche Verarbeitung nicht durch den Arbeitgeber selbst vorgenommen werden darf, sondern gem. § 22 Abs. 1 Nr. 1 lit. b BDSG nur von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen. Möglich ist auch eine Verarbeitung unter deren Verantwortung (Auftragsverarbeitung).

c) Möglichkeit des Abschlusses einer Betriebsvereinbarung

Als weitere Möglichkeit der Legitimation der Datenverarbeitung bietet sich auch der Abschluss einer Betriebsvereinbarung nach § 26 Abs. 4 S. 1 BDSG an, in denen die Betriebspartner nach Maßgabe von Art. 88 DSGVO *spezifischere* Vorschriften zur Datenverarbeitung treffen können.[1002] Da weder § 26 Abs. 4 BDSG noch Art. 88 Abs. 1 DSGVO eine Ermächtigungsgrundlage für die Vereinbarung von Betriebsvereinbarungen vorsehen, sondern lediglich statuieren, dass durch Kollektivvereinbarungen Datenvereinbarungen legitimiert werden können, müssen die allgemeinen Voraussetzungen des § 77 BetrVG eingehalten werden.[1003] So bestimmt § 77 Abs. 2 BetrVG, dass Betriebsvereinbarungen von Betriebsrat und Arbeitgeber gemeinsam zu beschließen und schriftlich niederzulegen sind. Sie müssen von beiden Seiten unterzeichnet werden, sofern sie nicht auf einem Spruch der Einigungsstelle beruhen und im Betrieb an geeigneter Stelle ausgelegt werden. Nach § 77 Abs. 4 BetrVG haben sie normative Wirkung und gelten somit für alle Arbeitsverhältnisse im betreffenden Betrieb, ohne dass es hierfür einer individualvertraglichen Implementierung bedarf. Wie schon unter **D. § 2 I** erörtert, werden People Analytics-Verfahren selten nur auf Betriebsebene umgesetzt, sodass nach § 50 Abs. 1 BetrVG der Gesamtbetriebsrat (sofern vorhanden) oder gar nach § 58 Abs. 1 BetrVG der Konzernbetriebsrat – je nach Reichweite der Imple-

1002 Siehe grundlegend bereits **D. § 1 V. 1**.

1003 *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 247.

mentierung derartiger Verfahren – richtiger Ansprechpartner für solche Vereinbarungen ist.

Betriebsvereinbarungen können ebenfalls – wie § 26 Abs. 4 S. 1 BDSG ausdrücklich klarstellt – die Verarbeitung sensitiver Daten legitimieren.

aa) Einhaltung der Datenschutzgrundsätze erforderlich

Aufgrund der Formulierung in Art. 88 Abs. 1 DSGVO, aber auch der Voraussetzung des § 26 Abs. 4 S. 2 BDSG i.V.m. Art. 88 Abs. 2 DSGVO können die Betriebspartner weder auf den Grundsatz der Datenminimierung noch auf die grundsätzliche Zweckbindung und Rechtmäßigkeit der Datenverarbeitung verzichten.[1004]

Ebenfalls muss die Verarbeitung aufgrund einer Betriebsvereinbarung für alle Beschäftigten transparent sein. Es müssen auf jeden Fall die Datenverarbeitungsgrundsätze aus Art. 5 DSGVO eingehalten werden, wobei – wie bereits erläutert[1005] – den Betriebspartnern den Betriebspartnern eine Einschätzungsprärogative zusteht.

bb) Erfasster Personenkreis geringer als nach § 26 Abs. 8 BDSG

Der Betriebsrat kann im Rahmen von Betriebsvereinbarungen nur die in § 5 BetrVG genannten Personen vertreten. Nach Absatz 1 sind dies Angestellte, Auszubildende sowie in der Hauptsache für den Betrieb tätige Heimarbeiter.[1006] Es sind daher nicht alle in § 26 Abs. 8 BDSG genannten Personen wie beispielsweise Bewerber oder arbeitnehmerähnliche Personen erfasst. Die wichtigste Ausnahme dürfte § 5 Abs. 3 BetrVG statuieren: Die Ausnahme für leitende Angestellte; für deren Belange ist der Sprecherausschuss nach § 25 Abs. 1 SprAuG zuständig.

Auch für diese Personengruppen kann jedoch durch Betriebsvereinbarung eine Erhöhung des Datenschutzniveaus zu erreicht werden, indem Arbeitgeber und Betriebsrat statuieren, dass die Vereinbarung wie ein Vertrag zugunsten Dritter gem. § 328 BGB wirken soll, an welchen (le-

1004 Ausführlich hierzu **D. § 1 IV**.
1005 Siehe **D. § 1 V. 2**.
1006 *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 252.

diglich) der Arbeitgeber gebunden ist.[1007] Mangels normativer Wirkung für diese Gruppen, kann eine Betriebsvereinbarung jedoch datenschutzrechtlich nicht legitimierend wirken.[1008] Sprecherausschüsse können mit Sprechausschussrichtlinien nach § 28 SprAuG eigene Verarbeitungsgrundlagen schaffen.[1009]

Relevant ist diese Beschränkung jedoch vor allem für Bewerberdaten, denn hier können Betriebsrat und Arbeitgeber keine spezifischen Regelungen treffen, die Nachteile für die Bewerber bringen könnten, da es sich insoweit um einen unzulässigen Vertrag zu Lasten Dritter handeln würde bzw. die unmittelbare Regelungswirkung des § 77 Abs. 4 BetrVG sich gerade nicht auf diese Personengruppe erstreckt.[1010] Zwar hat der Betriebsrat aus den §§ 92, 94 f. und 99 BetrVG Mitwirkungsrechte auch bezüglich Bewerbern, dennoch lässt sich hieraus kein (datenschutzrechtliches) Mandat für die Gruppe der Bewerber ableiten.[1011] Geregelt werden können daher allenfalls datenschutzrechtliche Bestimmungen für die Daten, die dem Betriebsrat zu übermitteln sind, wobei auch hier die Einschränkung gilt, dass lediglich ein zusätzlicher Schutz zum bereits durch das gesetzliche Datenschutzrecht vorhandenen geschaffen werden darf (z.B. Verkürzung von Speicherfristen für Bewerberunterlagen, weitergehende Auskunfts- und Informationspflichten des Arbeitgebers), nicht hingegen Spezialregelungen, die die gesetzlichen Regelungen (teilweise) verdrängen.

cc) Möglicher Inhalt der Betriebsvereinbarung

In der Betriebsvereinbarung können Arbeitgeber und Betriebsrat festlegen, dass sie die Verarbeitung von Arbeitnehmerdaten zum Zwecke von SPA als erforderlich ansehen und daher die Verarbeitung durch die BV legiti-

---

1007 So z.B. für Abfindungen aus einem Sozialplan auch für leitende Angestellte bereits BAG, Urt. v. 31.01.1979 – 5 AZR 454/77, BAGE 31, 266 = NJW 1979, 1621 Ls. 2.

1008 Für leitende Angestellte *Dzida/Grau*, DB 2018, 189 (191).

1009 *Dzida/Grau*, DB 2018, 189 (191); BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 53.

1010 Wie hier *Bausewein*, DuD 2016, 139 (140).

1011 So aber *Kort*, NZA-Beilage 2016, 62 (65), der hierbei auch auf die Möglichkeit des Abschlusses einer freiwilligen Betriebsvereinbarung hinweist, ohne hierauf einzugehen, dass auch solche nur für die in § 5 BetrVG genannten Personen eine rechtlich bindende Wirkung nach § 77 Abs. 4 BetrVG entfalten kann.

mieren. In diesem Rahmen werden dann spezifische Vorschriften zum Umgang mit den Arbeitnehmerdaten sowie zu den SPA selbst festgelegt.

Da nach der obigen Definition von SPA lediglich bereits vorhandene Werte fortgeschrieben werden und keine weiteren Daten z.B. durch Analyse von Logdateien von Computern o.ä. gesammelt oder generiert werden, besteht für die Analytics kein Mitbestimmungsrecht aus § 87 Abs. 1 BetrVG in Bezug auf die analysierten Arbeitnehmer.[1012] Zwar handelt es sich grundsätzlich um Personalplanungsmaßnahmen im Sinne von § 92 Abs. 1 BetrVG; allerdings hat der Betriebsrat aber nur einen Anspruch auf umfassende und rechtzeitige Unterrichtung.[1013] Es besteht aber ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG im Hinblick auf die Nutzung der Software durch das HR-Management. Beim Zugriff auf die Software werden nämlich IT-Daten generiert, die Rückschlüsse auf die Leistung oder das Verhalten der Personalsachbearbeiter haben könnten.

Über den Inhalt der Analysen von SPA kann der Betriebsrat aber dennoch keine Betriebsvereinbarung erzwingen. Möglich bleibt aber der freiwillige Abschluss. § 88 BetrVG verdeutlicht jedoch die Möglichkeit des Abschlusses freiwilliger Betriebsvereinbarungen für soziale Angelegenheiten.[1014] In dieser können aufgrund der normativen Wirkung, die auch bei freiwilligen Betriebsvereinbarungen besteht (§ 77 Abs. 4 S. 1 BetrVG nimmt insofern keine Unterscheidung vor), legitimierende Regelungen für die Datenverarbeitung für SPA nach § 26 Abs. 4 S. 1 BDSG geschaffen werden.

d) Zwischenergebnis

Die Nutzung von personenbezogenen Arbeitnehmerdaten für *Simple People Analytics* ist im Regelfall erforderlich. Wenn möglich, ohne dass die Aussagekraft der Analysen darunter leidet, müssen die Daten jedoch anonymisiert werden. In jedem Falle sind die Daten aber durch technisch-organisatorische Maßnahmen zu schützen. Hierzu gehört eine Pseudonymisierung (worunter auch entsprechende Verschlüsselung fällt) sowie eine Zugriffs-

1012 Zu den Mitbestimmungsrechten aus § 87 Abs. 1 BetrVG, siehe **D. § 2 II. 1.**

1013 Zum Mitbestimmungsrecht aus § 92 BetrVG, siehe **D. § 2 II. 4.**

1014 Die Aufzählung in § 88 BetrVG ist nicht abschließend, wie sich bereits aus dem offenen Wortlaut („insbesondere") ergibt; h.M., vgl. BAG, Beschl. v. 18.08.1987 – 1 ABR 30/86, AP BetrVG 1972 § 77 Nr. 23; BAG GS, Beschl. v. 07.11.1989 – GS 3/85, AP BetrVG 1972 § 77 Nr. 46; ferner ErfK/*Kania*, § 88 BetrVG Rn. 1 m.w.N.

kontrolle, um die Daten vor unbefugten Zugriffen Dritter zu schützen. Auch im Falle der Anonymisierung vor der Durchführung von Analytics ist zu prüfen, ob die zur Anonymisierung genutzten Daten tatsächlich für die späteren Analysevorgänge erforderlich sind. Sind sie dies nicht, so ist bereits die Nutzung der Daten für den zu legitimierenden Vorgang der Anonymisierung unzulässig. Im Rahmen der Zweckvereinbarkeitsprüfung nach Art. 6 Abs. 4 DSGVO sind unter anderem die möglichen Folgen für den Beschäftigten zu berücksichtigen; hier darf bei SPA davon ausgegangen werden, dass der Kompatibilitätstest positiv ausfällt, da grundsätzlich keine neuen persönlichkeitsrelevanten Daten geschaffen werden, sondern lediglich mit Hilfe einfachster statistischer Methoden die Daten fortgeschrieben werden; eine Nachvollziehbarkeit ist hier auch ohne mathematische Kenntnisse grundsätzlich gegeben.

Für SPA dürfen unter bestimmten Umständen auch sensitive Daten im Sinne des Art. 9 DSGVO genutzt werden. Dies gilt etwa im Bereich des Arbeitsschutzes und der Gesundheitsvorsorge, da hier den Arbeitgeber nicht zuletzt aus seiner Fürsorgepflicht gem. § 241 Abs. 2 BGB Pflichten treffen, die eine Verarbeitung der Daten erforderlich machen und somit nach § 26 Abs. 3 S. 1 BDSG legitimieren. Diese Daten bedürfen nach § 22 Abs. 2 BDSG eines besonderen Schutzes, der durch technisch-organisatorische Maßnahmen herzustellen ist.

Obwohl in dieser Arbeit die Auffassung vertreten wird, dass die Nutzung personenbezogener Arbeitnehmerdaten für SPA erforderlich ist nach § 26 Abs. 1 BDSG, ist die bevorzugende Variante der Abschluss einer (die Datenverarbeitung legitimierenden) Betriebsvereinbarung, die den Komplex der Simple People Analytics ausführlich regelt. Hierfür sprechen mehrere Gründe: Einerseits erhöht dies die Akzeptanz für *Analytics*-Maßnahmen bei den Beschäftigten[1015], andererseits können rechtliche Unsicherheiten bei der Einschätzung hierdurch aus dem Weg geschaffen werden. Die Betriebsvereinbarung schafft einen spezifischen Legitimationstatbestand, sodass im Streitfall ein Gericht nicht die Erforderlichkeit von SPA bezweifeln, sondern lediglich die Einhaltung der Grundsätze aus Art. 88 Abs. 2, Art. 5 DSGVO sowie der Grenzen aus § 75 Abs. 2 BetrVG überprüfen kann.

1015 *Bodie et al.*, Colorado Law Review 2017, 961 (1036 f.).

2. Fortgeschrittene People Analytics

In Abgrenzung zu den Simple People Analytics sind fortgeschrittene People Analytics oder **Advanced People Analytics** (im Folgenden: **APA**) Methoden, die nicht mehr mit Hilfe einfacher Statistik (z.B. linearer Regression) zu bewerkstelligen sind. Mithilfe komplexer Algorithmen (z.B. multivariate Regression, Einsatz künstlicher Intelligenz bzw. neuronaler Netze) und Auswertung von Echtzeit-Daten sollen Vorhersagen über das (Arbeits-)Verhalten oder sonstige Eigenschaften der Arbeitnehmer getroffen werden. Dies kann so weit führen, dass Arbeitnehmer „gescored" werden und mit Hilfe dieses Scores in bestimmte Kategorien eingeordnet werden (z.B. zuverlässiger Arbeitnehmer, unzuverlässiger Arbeitnehmer, leistungsfähiger aber unzuverlässiger Arbeitnehmer etc.).

Der Score stellt beispielsweise eine Zahl zwischen 1 und 10 dar, die einen Wahrscheinlichkeitswert für zukünftiges Verhalten repräsentiert und aus den verschiedenen zugrundeliegenden Daten anhand eines bestimmten Algorithmus (unter Vergleichsbetrachtung zu anderen Arbeitnehmern) generiert wird. Hierdurch können im Anschluss Personalverantwortliche z.B. im Falle des Einsatzes künstlicher Intelligenz die Vorschläge des Algorithmus bewerten und ggf. nachbessern, aus welchen der Algorithmus dann wiederum „lernt", indem er den Input zum Output erneut in die Berechnungen einfließen lässt.

Mit Hilfe von APA sollen Daten geschaffen oder Umstände aufgedeckt werden, die mit klassischen Methoden oder durch nur durch menschliche Rechenarbeit nur schwer oder unmöglich erkennbar sind. In aller Regel ist für solche Analysen eine sehr große Datenbasis (*Big Data*) notwendig. Dies rührt aus dem Umstand, dass zu Beginn der Analysen oftmals nicht feststeht, welche Daten letztendlich von Relevanz sind.

Bei Advanced People Analytics liegt in aller Regel ein Profiling nach Art. 4 Nr. 4 DSGVO vor, da hier – anders als bei den SPA – eine Bewertung persönlicher Aspekte durch automatisierte Verarbeitung im Vordergrund steht.[1016]

Im Folgenden müssen mehrere Schritte geprüft werden, um eine rechtliche Bewertung von APA vornehmen zu können: Zunächst muss in einem ersten Schritt (a) die Datengrundlage geklärt werden. Da bei APA deutlich mehr Daten herangezogen werden müssen, sind etwaige Grenzen aus dem Datenschutz- und insbesondere auch (aufgrund der vorherrschenden

1016 Siehe bereits **E. § 1 II.**

Auffassung der Datenschutzbehörden[1017]) Telekommunikationsrecht zu beachten. In einem weiteren Schritt muss die grundsätzliche Zulässigkeit solcher Auswertungen (*Profiling*) durch Arbeitgeber eingeschätzt werden (b), bevor im weiteren Verlauf die Erstellung von Scores als Grundlage für weitere Analytics (c) analysiert und rechtlich beurteilt wird. Ferner soll – analog der Vorgehensweise bei einfachen People Analytics – geklärt werden, inwiefern eine Einwilligung ein tauglicher Legitimationstatbestand darstellen könnte, ob solch weitgehende Analysen als „erforderlich" im Rahmen von § 26 Abs. 1 BDSG angesehen werden oder ob ggf. andere Legitimationstatbestände aus Art. 6 DSGVO herangezogen werden müssen. Zum Abschluss wird wiederum analysiert, ob APA grundsätzlich durch Betriebsvereinbarungen legitimiert werden können.

a) Die Datengrundlage bei fortgeschrittenen People Analytics

aa) Stark erweiterte Datenbasis durch Digitalisierung der Arbeitswelt (Arbeit 4.0)

Neben den klassisch vorhandenen Stamm- und Leistungsdaten (etwa aus Leistungsbeurteilungen) benötigt APA eine deutlich größere Datenbasis. Insbesondere, wenn etwa „Live-Auswertungen" erstellt werden sollen, ist es nicht ausreichend, dass nur etwa monatlich, quartalsweise oder nur jährlich erfolgende Leistungsbeurteilungen der Arbeitnehmer das Datenbasis herangezogen werden, da hierdurch nur sehr träge auf etwaige Veränderungen reagiert werden könnte. Aus diesem Grund müssen Datensätze gesucht werden, die ein aktuelles Abbild des Verhaltens oder der Leistung der Beschäftigten abbilden, wie etwa IT-Nutzungs- und Sensordaten.[1018] Aufgrund der zunehmenden Digitalisierung des Arbeitslebens[1019] fallen

1017 Diese sind der Auffassung, dass bei erlaubter Privatnutzung von betrieblicher Infrastruktur der Arbeitgeber Telekommunikationsanbieter im Sinne des TKG ist; diese Auffassung ist zwar nicht überzeugend, aufgrund der Rechtsunsicherheit und der strafrechtlichen Sanktionsgefahr ist dies in der Praxis aber weiterhin zu beachten, vgl. hierzu **D. § 3**.

1018 Eine beispielshafte Aufzählung möglicher Datensätze für *People* oder *Workforce Analytics* ist unter **C. § 1** zu finden; weitere Beispiele nennt *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 4 DSGVO Rn. 7.

1019 *Däubler*, Digitalisierung und Arbeitsrecht, S. § 1 Rn. 11 ff.; *Däubler*, AuR Sonderausgabe Juli 2016, 2; speziell zu Big Data *BMAS*, Weißbuch Arbeiten 4.0, S. 62 ff.

nicht nur an Computerarbeitsplätzen, sondern an jeglichen Arbeitsplätzen entsprechende IT-Daten an.[1020] Sei es beim Außendienstmitarbeiter durch das Mobiltelefon oder ein im Kfz eingebautes Ortungsmodul, bei der Kassiererin an der Supermarktkasse das digitale Kassensystem, das die Eingaben erfasst oder beim Lagermitarbeiter die benutzten Scanner zur Warenerfassung[1021]. Mit zunehmender Digitalisierung kommen weitere Daten beispielsweise von Smart Glasses, anderen *Wearables* oder digitalen Assistenten hinzu.[1022] Da Wearables eine besonders neuartige Erscheinung sind, werden diesen in der nachfolgenden Analyse besondere Beachtung geschenkt.

bb) Zulässigkeit der Erhebung von IT-Nutzungs- und -Sensordaten

Anders als bei SPA, wo die zulässige Erhebung der Daten für die Zwecke dieser Arbeit angenommen wird, ist bei APA zunächst zu untersuchen, inwiefern Sensordaten erhoben und für weitere Analyticszwecke verwendet werden dürfen. Dies hat den Hintergrund, dass diese Daten nicht primär für die Personalverwaltung erhoben wurden, sondern mitunter für ganz andere Zwecke wie beispielsweise der Aufrechterhaltung der Funktionsfähigkeit und Integrität von IT-Systemen oder deren Sicherheit sowie der Möglichkeit des Datenmissbräuche nachverfolgen zu können. Aufgrund der hohen Relevanz und datenschutzspezifischen Besonderheiten ist daher im Folgenden genauer darauf einzugehen, wobei in einem ersten Schritt die Erhebung solcher Daten zum Zwecke der Analytics geprüft wird, be-

1020 Diese Daten werden auch als „Metadaten" bezeichnet, vgl. *Götz*, Big Data im Personalmanagement, S. 26.

1021 So erfassen die Handscanner von Amazon angeblich nicht nur Scandaten, sondern enthalten wie Smartphones Kameras und Mikrofone und speichern detaillierte Bewegungsdaten. Zwar gibt Amazon an, keine individualisierten Evaluierungen von Bewegungsdaten zu erfassen und die Mikrofone nicht zu nutzen, andererseits berichten Beschäftigte, in Personalgesprächen mit Daten über die individuelle Arbeitsleistung konfrontiert zu werden, sodass vermutet wird, dass im Hintergrund ein automatisierter Bewertungsalgorithmus laufe, der die Daten auswerte und so Einzelbewertungen erstelle, vgl. *Staab/Nachtwey*, APuZ 2016, 24 (27).

1022 *Krause*, Forschungsbericht 482 - Digitalisierung und Beschäftigtendatenschutz, <www.bmas.de/SharedDocs/Downloads/DE/PDF-Publikationen/Forschungsberichte/fb482-digitalisierung-und-beschaeftigtendatenschutz.pdf?__blob=publicationFile&v=1>, S. 12 ff.

vor in einem zweiten Schritt auf die Verwendung von für andere Zwecke erhobenen Daten eingegangen wird.

Zuvor aber muss aber noch auf zwei Datenschutzgrundsätze, die bei der Bewertung eine maßgebliche Rolle spielen (nachfolgend (1)), kurz eingegangen sowie die maßgebliche Legitimationsnorm als Dreh- und Angelpunkt der Zulässigkeitsuntersuchung (2) herausgearbeitet werden.

(1) Privacy by Design und Privacy by Default

Der europäische Gesetzgeber hat den in Art. 5 Abs. 1 lit. c DSGVO festgelegten Grundsatz der Datenminimierung und den in lit. e niedergeschriebenen Grundsatz der Speicherbegrenzung positivrechtlich durch die Aufnahme der Grundsätze *Privacy by Design* und *Privacy by Default* als technisch-organisatorische Maßnahmen in Art. 25 DSGVO gestärkt.[1023] Hiernach müssen nach Möglichkeit und Risiko bereits entsprechende technische Maßnahmen wie eine Pseudonymisierung in die Software integriert werden sowie datenschutzfreundliche Einstellungen als Standard ausgewählt sein. Diese Ansätze verfolgen das Ziel, dass die datenschutzrechtlichen Anforderungen am effektivsten umgesetzt werden können, wenn sie bereits in frühen Planungsphasen der Datenverarbeitungssysteme berücksichtigt und integriert werden.[1024] Allerdings ist diese Vorschrift auf den ersten Blick misslungen, da sie die Datenverarbeiter und nicht die Hersteller, die gerade solche Systeme konzipieren und programmieren, in die Pflicht nimmt.[1025] Im Ergebnis werden aber die Verarbeiter die Hersteller dazu drängen, ihre Systeme entsprechend zu konzipieren, da sie diese ansonsten nicht einsetzen dürfen. Mittelbar wird die Vorschrift also Auswirkungen auf die Hersteller haben und somit das damit verfolgte Ziel erreicht werden können.

Aufgrund dieser Vorgaben ist davon auszugehen, dass nicht alle für fortgeschrittene People Analytics nützliche Daten bereits automatisch von

---

1023 *Hackenberg*, Teil 15.2 Big Data und Datenschutz, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Rn. 44.

1024 Paal/Pauly/*Martini*, Art. 25 DSGVO Rn. 10; *Jandt*, DuD 41(9) (2017), 562; *EDPS*, Opinion 7/2015 - Meeting the challenges of big data, <edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf>, S. 14 f.; so bereits *Roßnagel*, MMR 2005, 71 (74): "*Die Einhaltung von Verarbeitungsregeln zu kontrollieren, darf nicht eine permanente persönliche Aufmerksamkeit erfordern, sondern muss automatisiert erfolgen.*"

1025 Kritisch daher auch *Jandt*, DuD 41(9) (2017), 562 (563).

den Systemen erfasst werden und einfach zweckändernd weiterverarbeitet werden können. Eine Speicherung solcher Daten ist in der Regel aktiv vom Arbeitgeber zu veranlassen. Aufgrund dieser Grundsätze, aber auch aufgrund § 26 Abs. 1 BDSG bzw. Art. 6 Abs. 1 lit. f DSGVO ist im Detail zu prüfen, welche Daten erforderlich sind.

(2) Maßstab der Beurteilung der Rechtmäßigkeit: § 26 Abs. 1 BDSG und/oder Art. 6 Abs. 1 lit. f DSGVO

Die Erforderlichkeit der Daten für die Entscheidung über die Begründung, die Durchführung oder Beendigung des Beschäftigungsverhältnisses ist – wie im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO – im Ergebnis eine Verhältnismäßigkeitsprüfung,[1026] die auf einer Abwägung der jeweiligen Grundrechte und Interessen basiert.

Neben der Spezialregelung gem. § 26 Abs. 1 S. 1 BDSG zum Beschäftigtendatenschutz kann die „Auffangklausel" des Art. 6 Abs. 1 lit. f DSGVO eingreifen,[1027] wenn es sich um Daten handelt, die nicht für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich sind, die Daten also anderen Zwecken dienen. Ein Beispiel hierfür wäre, dass Beschäftigtendaten im Rahmen einer Due Diligence bei einem Unternehmenskauf verarbeitet werden.[1028] Mangels Regelungskompetenz der Mitgliedstaaten kann es in diesem Bereich auch bei Beschäftigtendaten nicht zu einem Ausschluss der allgemeinen Erlaubnistatbestände kommen.[1029] Wie das Beispiel zeigt, dürfte der Rückgriff auf Art. 6 DSGVO aber deswegen eher die Ausnahme sein,[1030] da die Zweckbestimmung „Durchführung des Arbeitsverhältnisses" sehr weit zu verstehen ist.[1031] Es gibt jedoch auch Fälle, in denen die Datenverarbeitung von Daten eines bestimmten Arbeitnehmers nicht für die Durchführung

1026 Zu den Kriterien der Erforderlichkeit im Rahmen von § 26 Abs. 1 BDSG, siehe **D. § 1 IV. 2. b)** sowie **E. § 1 I. 1. b)**.

1027 ErfK/*Franzen*, § 26 BDSG Rn. 4 f.; *Kainer/Weber*, BB 2017, 2740 (2743); *Kort*, NZA 2018, 1097 (1099 f.); *Kramer*, NZA 2018, 637 (638); *Ströbel et al.*, CCZ 2018, 14 (19); so wohl auch LAG Hamm, Beschl. v. 19.09.2017 – 7 TaBV 43/17, ZD 2018, 129 (131) Rn. 35.

1028 *Kort*, NZA 2018, 1097 (1099).

1029 *Ströbel et al.*, CCZ 2018, 14 (19).

1030 So auch *Kramer*, NZA 2018, 637 (638).

1031 *Zöll*, in: Taeger/Gabel, DSGVO - BDSG, § 26 BDSG Rn. 38 Hierzu bereits oben **E. § 1 I. 1. b) bb)**.

dessen Arbeitsverhältnisses erforderlich sind, sondern für die Zwecke eines anderen Beschäftigungsverhältnisses verarbeitet werden sollen.[1032] Das wäre beispielsweise dann der Fall, wenn für ein Scoring aggregierte Daten als Vergleichsbasis herangezogen werden sollen.[1033] Für den Anonymisierungsvorgang der Daten eines anderen Arbeitnehmers ist nicht § 26 Abs. 1 BDSG die einschlägige Legitimationsgrundlage, sondern Art. 6 Abs. 1 lit. f DSGVO.

Die beiden Tatbestände schließen sich insofern auch gegenseitig aus: Werden die Daten für die Zwecke des Beschäftigungsverhältnisses verarbeitet, ist § 26 Abs. 1 BDSG die einschlägige Norm zur Beurteilung der Rechtmäßigkeit, während für alle anderen Zwecke die allgemeinen Tatbestände aus Art. 6 Abs. 1 DSGVO anwendbar bleiben. Im Endeffekt führt dies – jedenfalls bei Maßnahmen, die nicht der Aufdeckung von Strafdaten dienen[1034] – zum selben Ergebnis: Wie bereits gezeigt wurde, ist auch im Rahmen von § 26 Abs. 1 S. 1 BDSG die Erforderlichkeit mehr als ein Abwägungsgebot zu verstehen als eine strikte Erforderlichkeit, wobei die Verarbeitungsinteressen des Arbeitgebers mit den Geheimhaltungsinteressen des Arbeitnehmers abzuwägen und praktische Konkordanz herzustellen ist. Nichts anderes gilt im Rahmen der Interessensabwägung nach Art. 6 Abs. 1 lit. f DSGVO, mit der Folge, dass Arbeitgeber zwar bei der Angabe der Legitimationsgrundlage im Verzeichnis der Verarbeitungstätigkeiten die korrekte Norm nennen müssen, sich aber inhaltlich an der Abwägungsentscheidung nichts ändert.[1035]

Wenn eine Maßnahme nach § 26 Abs. 1 S. 1 BDSG zulässig ist, so ist sie es auch außerhalb des Kontextes des konkreten Beschäftigungsverhältnisses im Rahmen von Art. 6 Abs. 1 lit. f DSGVO und vice versa, wenn

---

1032 Dagegen WHWS/*Byers*, B. VII. GPS-Ortung, Rn. 27: Zu den Rechten aus dem Beschäftigungsverhältnis gehört auch die Organisation des Betriebs, weshalb eine hierfür erforderliche Datenverarbeitung ebenfalls unter § 26 Abs. 1 S. 1 BDSG zu subsumieren ist.

1033 So wohl auch *Rudkowski*, NZA 2019, 72 (73).

1034 Repressive Maßnahmen sind dem Bereich der *Compliance* zuzuordnen und daher nicht Teil dieser Untersuchung.

1035 Dies kann mitunter auch damit begründet werden, dass auch im Rahmen der Abwägung von § 26 Abs. 1 BDSG subsidiär die Grundrechte aus der EU-GRC den Abwägungsmaßstab festlegen. Selbst wenn unterschiedliche Grundrechte herangezogen würden, wäre von einem Gleichlauf der Interessensabwägung bei europäischen und nationalen Grundrechten auszugehen (so wohl auch der deutsche Gesetzgeber, der die bisherige Regelung des § 32 BDSG a.F. schlicht fortführen wollte, vgl. BT-Drs. 18/11325, S. 96 f.); siehe hierzu bereits **D. § 1 IV. 2. b**).

die beiderseitigen Interessen identisch sind.[1036] Auch bei der Abwägung der berechtigten Interessen ist das besondere Abhängigkeitsverhältnis zwischen Arbeitgeber und Arbeitnehmer zu berücksichtigen, sodass keine milderen Voraussetzungen gelten.

cc) Erhebung von IT-Nutzungs- und Sensordaten für Analyticszwecke

(1) Log-Daten von IT-Systemen

Wie bereits angedeutet, fallen bei der Nutzung von IT-Systemen gewisse System- und Logdaten an, die von der jeweiligen Anwendung bzw. dem Betriebssystem zum Zwecke der Fehleranalyse für einen gewissen Zeitraum gespeichert werden.[1037] Der Umgang des Systems mit den Log-Files kann in aller Regel durch den Systemadministrator konfiguriert werden.[1038]

Bereits nach dem alten Datenschutzrecht war anerkannt, dass auch für Log-Dateien die Grundsätze der Erforderlichkeit, Angemessenheit und Zweckbindung der Daten einzuhalten sind, wobei im Hinblick auf die Zweckbindung bereits im Vorfeld präzise Aussagen zur Zielstellung von Protokollen erforderlich und allgemeine Formulierungen wie „Gewährleistung der Datensicherheit und Sicherungszwecke" unzureichend sind.[1039] Aus diesem Grund dürfen auch nur so wenig personenbezogene Daten gespeichert werden, wie möglich; wenn der Zweck es zulässt, ist zu anonymisieren und/oder – falls eine Anonymisierung ausscheidet – pseudonymisieren.[1040]

1036 *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 18 unter Verweis auf BAG, Urt. v. 12.02.2015 – 6 AZR 845/13, NZA 2015, 741 Das Gericht ließ es hierbei im Rahmen einer Verdachtskündigung dahinstehen, ob § 32 Abs. 1 S. 1 BDSG a.F. oder § 28 Abs. 1 S. 1 Nr. 2 BDSG a.F. einschlägig ist.

1037 Vgl. hierzu auch HdbIT-DSR/*Conrad/Schneider*, § 14 Softwarepflege und Support, Rn. 127.

1038 Bei Linux beispielsweise durch das in alle Distributionen integrierte Tool „logrotate", mit welchem solche Dateien automatisch komprimiert, nach einem bestimmten Zeitraum gelöscht oder an bestimmte Personen gesendet werden können, vgl. https://linux.die.net/man/8/logrotate (letzter Abruf am:: 30.01.2020); zur Praxis der Systemprotokollierung bei UNIX-basierten Systemen, siehe *Seeger*, DuD 2006, 285; zu den Grundlagen der Windows-Protokollierung, siehe *Marnau*, DuD 2006, 288.

1039 *Knorr*, DuD 2006, 268.

1040 *Knorr*, DuD 2006, 268; *Kort*, NZA 2011, 1319 (1320 f.).

Wesentlich ist, dass Logdateien also nicht ausschließlich anonyme Systemdaten erfassen, sondern mitunter auch personenbezogene, wenn die jeweilige Anwendung bzw. das System die Benutzererkennung bei der Speicherung miterfasst oder sich aus anderen Umständen ergibt, dass ein bestimmter Arbeitnehmer gerade das System benutzt hat.

Beispiel: Eine Website löst einen Darstellungsfehler aus, die vom Browser erfasst wird. Der Browser speichert die Fehlermeldung inklusive der Adresse der Website im Fehlerlog. Anhand einer späteren Auswertung des Systemlogs und der Kenntnis, dass ein bestimmter Arbeitnehmer in dieser Zeit den Computer nutzt, lässt sich – ohne den Browserverlauf explizit zu prüfen – feststellen, dass Arbeitnehmer X zu einer ganz bestimmten Uhrzeit die Website aufgerufen hat. Ist beispielsweise die Privatnutzung des Internets verboten, so ließe sich allein durch die Fehlermeldung ein Verstoß gegen arbeitsvertragliche Pflichten feststellen.

Solche Log-Daten können (unerwünschte) Login-Versuche, E-Mail-Transport- und -Abruf-Daten, Zugriffe auf Webseiten oder Dateien, Nutzungen von Anwendungen, Firewall-Daten etc. enthalten. Der Anfall an solchen Daten ist vielfältig und mitunter sehr weitreichend.

Grundsätzlich kann davon ausgegangen werden, dass die Daten zur Gewährleistung eines sicheren und fehlerfreien IT-Betriebs erforderlich sind.[1041] Problematisch ist, dass im betrieblichen Bereich die Administratoren unter Druck gesetzt werden könnten, zur Überwachung der Arbeitsleistung oder aus anderen Gründen auf die Logdateien, die bestimmte Mitarbeiter betreffen, zuzugreifen.[1042] Allerdings sieht bereits die DSGVO gewisse Protokollierungen vor, wenn sie den Verarbeitern in Art. 32 im Rahmen der technisch-organisatorischen Maßnahmen vorschreibt, Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzuführen.[1043] Datenschutzverstöße müssen nach Art. 33 an die Behörden und nach Art. 34 an die Betroffenen gemeldet werden, was ohne eine Protokollierung der Zugriffe nur schwer möglich ist. Für sensitive Daten im Sinne des Art. 9 DSGVO schreibt § 22 Abs. 2 S. 2 Ziff. 2 BDSG als mögliche Garantie sogar explizit

1041 *Heidrich/Wegener*, MMR 2015, 487.

1042 *Heidrich/Wegener*, MMR 2015, 487 (490).

1043 So gehört Protokollierung zur Sicherstellung der Kontrolle der Ordnungsgemäßheit der Datenverarbeitung, bspw. durch die Revision, vgl. *Hof*, 5 Datenschutz mittels IT-Sicherheit, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 523 Rn. 124; als mögliche TOM auch *Wolff*, E. Technisch-Organisatorische Pflichten, in: Schantz/Wolff, Das neue Datenschutzrecht, Rn. 829.

vor, dass nachträglich überprüft und festgestellt werden können muss, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind. Für öffentliche Stellen regelt § 76 BDSG bei automatisierten Verarbeitungsvorgängen bestimmte Protokollpflichten; eine vergleichbare Vorschrift gibt es für nicht-öffentliche Stellen allerdings nicht.

Sieht man die Erhebung und Speicherung von Log-Daten also als technisch-organisatorische Schutzmaßnahme zum Datenschutz an, so ist die Legitimationsgrundlage für die Erhebung solcher Daten Art. 6 Abs. 1 lit. c DSGVO. Diese Daten werden jedoch nicht für die Zwecke der *People Analytics*, sondern für die Gewährleistung der Integrität und Funktionsfähigkeit von IT-Systemen erhoben und sind daher entsprechend zweckgebunden; sie dürfen also grundsätzlich nicht für andere Zwecke verarbeitet werden.

(2) Spezifische Datenerhebung für People Analytics

Im Rahmen der Datenerhebung für People Analytics sind daher in einem ersten Schritt nur solche Erhebungs- und Verarbeitungsvorgänge zu analysieren, die nicht ohnehin bereits durch die Systeme erfasst werden. Für diese Vorgänge ist Legitimationsgrundlage der Erhebung § 26 Abs. 1 S. 1 BDSG, da diese Daten bereits mit dem Zweck der Durchführung des Beschäftigungsverhältnisses erhoben werden.[1044] Es kommt daher bereits bei der Erhebung auf die Erforderlichkeit und Angemessenheit der Datennutzung für den konkreten Zweck an, d.h. bereits vor Erhebung der Daten muss geprüft werden, ob schutzwürdige Arbeitgeberinteressen solchen des Arbeitnehmers überwiegen. Dabei muss darauf geachtet werden, dass die Erhebung von IT-Systemdaten nicht zu einer unzulässigen Dauerüberwachung führt.[1045] 2017 hat der BGH in der bekannten *Keylogger*-Entscheidung[1046] seine ständige Rechtsprechung erneut bestätigt: (Präventive) Überwachungsmaßnahmen sind grundsätzlich zulässig, sofern bei den Betroffenen kein solcher psychischer Anpassungsdruck erzeugt wird, dass

1044 Zum Zweck der Durchführung des Beschäftigungsverhältnisses siehe **E. § 1 I. 1. b) bb)**.

1045 Vgl. hierzu BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205 (1211) Rn. 30 zu § 75 II BetrVG; im Rahmen von § 26 I BDSG kann ebenso kein milderer Maßstab gelten.

1046 BAG, Urt. v. 27.07.2017 – 2 AZR 681/16, NZA 2017, 1327 = BAGE 159, 389 = CR 2018, 27.

diese bei objektiver Betrachtung in der Ausübung ihrer Freiheit und ihrem Handeln aus eigener Selbstbestimmung wesentlich gehemmt werden.[1047]

Wenn allerdings für People Analytics auch Kommunikationsdaten ausgewertet werden sollen, müssen Arbeitgeber die §§ 88 ff. TKG im Blick haben. Aufgrund der mangels höchstrichterlichen Rechtsprechung bestehenden Unsicherheit ist dem Arbeitgeber anzuraten, nach Möglichkeit die Privatnutzung des Firmennetzwerks zu verbieten, wenn diese Daten für People Analytics-Zwecke genutzt werden sollen.

Für sensitive Daten, insbesondere Gesundheitsdaten, sind die zusätzlichen Vorgaben aus Art. 9 DSGVO, § 22 Abs. 2 BDSG zu beachten.[1048] Da solche Daten nur dann genutzt werden dürfen, wenn Arbeitgeber dadurch ihre Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erfüllen oder eine Einwilligung oder Betriebsvereinbarung hierzu vorliegt, sind die Daten nur bedingt für Advanced People Analytics geeignet: Im Bereich des Arbeits- und Gesundheitsschutzes können solche Daten erhoben werden, wenn sie spezifisch diesem Zweck dienen. Eine Einwilligung im Hinblick dieser Daten ist auch im Beschäftigungsverhältnis nach § 26 Abs. 3 S. 2 BDSG grundsätzlich möglich, wobei die Freiwilligkeit problematisch sein kann.[1049] Ist sichergestellt, dass Arbeitgeber und Arbeitnehmer die gleichen Interessen verfolgen oder Analysen nur Vorteile für die Arbeitnehmer bringen, und werden diese nicht vom Arbeitgeber unter Druck gesetzt, die Einwilligung hierzu abgeben, so kann – sofern keine anderen Anhaltspunkte bestehen – von einer Zulässigkeit der Einwilligung ausgegangen werden (§ 26 Abs. 2 S. 2 BDSG). Ebenfalls möglich ist nach § 26 Abs. 4 S. 1 DSGVO der Abschluss einer Betriebsvereinbarung für die Erhebung von IT-Systemdaten (inklusive sensitiver Daten), wobei keine maßgeblichen Abweichungen vom Schutzniveau der DSGVO möglich sind. Dennoch können Spezialregelungen getroffen werden.[1050] Dies hat aber zur Folge, dass auch im Rahmen von Kollektivvereinbarungen Vorgänge der Verarbeitung von Gesundheitsdaten für Analytics-Zwecke nicht generell legitimiert werden dürfen. Vielmehr muss

---

1047 St. Rspr., vgl. statt aller BAG, Urt. v. 27.07.2017 – 2 AZR 681/16, NZA 2017, 1327 (1330) = BAGE 159, 389 = CR 2018, 27 Rn. 31; Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205; Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (Rn. 15) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54 m.w.N.

1048 Grundlegend hierzu bereits **E. § 1 III. 1. b) bb) (2)**.

1049 Zur Freiwilligkeit der Einwilligung im Beschäftigungsverhältnis, siehe **D. § 1 III. 2. a)** und **E. § 1 III. 1. a)**.

1050 Zum Verhältnis zwischen Betriebsvereinbarung und DSGVO, siehe **D. § 1 IV** und **D. § 1 V. 2**.

die gesetzgeberische Wertung beachtet werden, sensitive Daten nur zur Erfüllung arbeitsrechtlicher Pflichten zu erfassen und nutzen. Solche Pflichten des Arbeitgebers können jedoch– wie § 26 Abs. 1 S. 1 a.E. BDSG zeigt – auch durch eine Betriebsvereinbarung geschaffen werden. Hierbei haben aber die Betriebspartner die Persönlichkeitsrechte der Arbeitnehmer zu wahren (§ 75 Abs. 2 BetrVG).[1051] Dementsprechend wäre es nicht möglich, das Datenschutzrecht dergestalt zu umgehen, dass umfassende Pflichten zur Verarbeitung sensitiver Daten in der Betriebsvereinbarung zu regeln und hierdurch sogar nach § 26 Abs. 1 BDSG gesetzlich zu legitimieren. Der Maßstab im Rahmen von § 75 Abs. 2 BetrVG ist dem der Abwägung in § 26 Abs. 1 BDSG vergleichbar,[1052] wobei bei ersterer zusätzlich noch die Gesamtbelastung des Kollektivs betrachtet werden muss.[1053]

Beispiel: Während die Verarbeitung eines personenbezogenen Datums für einzelne Arbeitnehmer aufgrund ihrer Position im Unternehmen noch nicht zu einem unzulässigen Überwachungsdruck führen muss, kann bei einer Betrachtung aller Arbeitnehmer des Betriebs hingegen ein solcher vorliegen, sodass die Datenverarbeitung nach § 75 Abs. 2 BetrVG als unzulässig einzustufen ist und eine entsprechende Betriebsvereinbarung beispielsweise nicht geschlossen werden dürfte.

(3) Sensordaten von Wearables

Eine weitere, für Beschäftigungszwecke neuartige Datenquelle können Wearables darstellen, die Vitalfunktionen des Beschäftigten aufzeichnen. Das können Smartwatches oder Fitness Tracker sein. Inzwischen gibt es auch „smart clothes", die u.a. Vitalwerte aufzeichnen, aber auch andere Daten wie beispielsweise die Umgebungstemperatur oder -feuchtigkeit bei Schutzanzügen (beispielsweise der Feuerwehr) aufzeichnen können.[1054]

1051 Für eine entsprechende Abwägungspflicht auch bei gesetzlichen Pflichten, *Böhm*, NZA-RR 2019, 530 (531); *Wybitul*, NZA 2017, 413 (415 f.); dagegen BAG, Beschl. v. 07.05.2019 – 1 ABR 53/17, NZA 2019, 1218 (1222) Rn. 42.

1052 Vgl. BAG, Beschl. v. 29.06.2004 – 1 ABR 21/03, NZA 2004, 1278 (1280 f.) = BAGE 111, 173 = AP BetrVG § 87 1972 Überwachung Nr. 41 (m. Anm. Ehmann) zu den Kriterien der Abwägung.

1053 Hierzu **D. § 2 II. 1. b) ee)**.

1054 *Blinn*, Wearables und Arbeitnehmerdatenschutz - Vom freiwilligen Selbstoptimierer zum Kontrollinstrument des Arbeitgebers?, in: Taeger, Smart world - smart law?, S. 519 ff.; weitere Beispiele bei *Putschli*, DuD 2017, 721.

Diese Geräte haben gemein, dass sie Gesundheitsdaten im Sinne von Art. 4 Nr. 15 DSGVO[1055] und somit sensitive Daten nach Art. 9 DSGVO bzw. § 26 Abs. 3 S. 1 BDSG erheben und verarbeiten. Solche Daten geben besonders tiefe Einblicke in das Privatleben der Nutzer[1056] und unterliegen – wie bereits mehrfach aufgezeigt – besonders strengen Verarbeitungsbeschränkungen.[1057]

Arbeitgeber können beispielsweise Fitnessarmbänder an Arbeitnehmer verteilen, um diesen einen Anreiz zu geben, gesünder zu leben, ohne die hierdurch gewonnen Daten zu verarbeiten. Ein solcher Einsatz ist aus Arbeitgebersicht datenschutzrechtlich irrelevant. Sobald allerdings die von den Armbändern generierten Daten auch für People Analytics genutzt werden sollen, muss die Verarbeitung von solchen Daten am Maßstab des § 26 Abs. 1 S. 1, Abs. 4 S. 1 BDSG gemessen werden.

Im Bereich des Arbeitsschutzes, beispielsweise bei Sensoren in der Kleidung von Rettungs- und Feuerwehrleuten, dürfte eine datenschutzrechtliche Abwägung zugunsten des Arbeitgebers ausfallen: Die Daten werden nicht zur Leistungskontrolle, sondern zum Zwecke des Schutzes von Leib und Leben der Beschäftigten verarbeitet. Voraussetzung ist, dass nur solche Daten erhoben werden, die zum Schutz des Beschäftigten auch erforderlich sind. Zwar greift Art. 9 Abs. 2 lit. c DSGVO als Erlaubnistatbestand nicht, da dieser es erfordert, dass die betroffene Person außerstande ist, die Einwilligung zu erteilen. Legitimationsgrundlage hierfür kann aber § 26 Abs. 3 S. 1 BDSG sein, da Arbeitgeber verpflichtet sind, im Rahmen des Arbeitsschutzes, ihre Beschäftigten zu schützen. Ein weiteres Beispiel wäre das Agieren mit gefährlichen Stoffen.[1058] In diesem Fall dient die Aufzeichnung der Sensordaten nicht nur dem Schutz des konkret betroffenen Arbeitnehmers, sondern auch der anderen Beschäftigten.

Beispiel: Ein Arbeitnehmer hantiert im Labor mit einem gefährlichen Stoff, wobei hiervon eine kleine Menge dieses Stoffes austritt. Dieser Stoff ist hoch reizend, erste Symptome treten aber erst nach wenigen Minuten auf. Der Laborant merkt diesen Austritt des Stoffes nicht sofort. Die Sensoren in der smarten Kleidung erfassen den Austritt, woraufhin automatisiert ein Alarm im Labor ausgelöst wird, sodass alle im Labor Beschäftig-

1055 Auch die Schrittanzahl lässt Rückschlüsse auf den Gesundheitszustand zu und ist daher von Art. 9 DSGVO umfasst, vgl. *Blinn*, Wearables und Arbeitnehmerdatenschutz - Vom freiwilligen Selbstoptimierer zum Kontrollinstrument des Arbeitgebers?, in: Taeger, Smart world - smart law?, S. 528.

1056 *Putschli*, DuD 2017, 721.

1057 Siehe bereits **E. § 1 III. 1. b) bb) (2)**.

1058 *Kopp/Sokoll*, NZA 2015, 1352 (1356).

ten das Labor schnellstmöglich räumen können. Ohne diesen Alarm wäre es bei allen Laboranten zu einer Reizung der Augen und Schleimhäute gekommen, was eine Arbeitsunfähigkeit von mindestens zwei Tagen nach sich gezogen hätte.

Wie sich aus der Wertung des Art. 9 Abs. 2 lit. c DSGVO ergibt, sind Arbeitgeber grundsätzlich gehalten, eine Einwilligung einzuholen, falls die Sensorik ausschließlich dem Schutz des mit dieser ausgestatteten Beschäftigten dient: Art. 9 Abs. 2 lit. c DSGVO schreibt vor, dass eine Verarbeitung zum Schutz *lebenswichtiger* Interessen des Betroffenen nur zulässig ist, wenn dieser außerstande ist, eine Einwilligung zu geben. Für andere Verarbeitungen, die ausschließlich dem Schutz dienen, muss dies also erst recht gelten. Sollen hingegen auch andere Beschäftigte geschützt werden, so dient die Sensorik dem höheren Zweck der Betriebssicherheit und Schutz von Gesundheit und Leib und Leben vieler Beschäftigten, sodass das Arbeitgeberinteresse an einer Verarbeitung solcher Daten (Daten von Sensoren in der Kleidung von Beschäftigten zur Messung der Luftbelastung) überwiegt. Diese Wertung ergibt sich bereits aus § 26 Abs. 3 S. 1 sowie aus Art. 9 Abs. 2 lit. b DSGVO, wonach der Verarbeiter die Daten verarbeiten darf, wenn diese erforderlich sind, um seine Pflichten aus dem Arbeitsrecht (und somit dem Arbeitsschutz) zu erfüllen.

Zu beachten ist, dass die Daten aus dem obigen Beispiel jedoch anonymisiert werden müssten, da keine Zuordnung der Daten zu einem Beschäftigten erforderlich ist, um eine Warnung auszulösen. Ist das Labor besonders groß und müsste daher nur ein bestimmter Bereich geräumt werden, so könnten die Daten trotz Anonymisierung personenbezogen sein (wenn beispielsweise nur ein Beschäftigter in diesem konkreten Bereich arbeitet). Dies wäre aber unschädlich, da die Verarbeitung der Lokalisationsdaten, die zu einer Zuordenbarkeit führen, erforderlich ist, um den mit der Verarbeitung verfolgten Schutzzweck zu erfüllen und insofern das Interesse des Beschäftigten nicht überwiegt. Letztlich dient die Verarbeitung auch zu seinem eigenen Schutz.

Etwas anderes gilt, wenn etwa Fitness-Armbänder für betriebliche Gesundheitsprogramme eingesetzt werden sollen, um etwa *Health-Scores* generieren, die es ermöglichen, dass sich Arbeitnehmer in den internen Wettbewerb zu anderen Arbeitnehmern zu stellen. Aufgrund der besonderen Sensibilität der Vitaldaten und mangels Legitimationsgrundlage zur Verarbeitung kommt eine Verarbeitung auf rein gesetzlicher Grundlage nicht in Betracht. Ebenfalls scheiden eine zwingende Verarbeitung und Pflicht zur Teilnahme per Betriebsvereinbarung aus (§ 75 Abs. 2 BetrVG). Eine Verarbeitung, die so stark in die Persönlichkeitssphäre des Arbeitneh-

mers eingreift und deren Zweck ebenfalls mehr in der Privatsphäre als im Interesse des Arbeitgebers liegt, kann nicht ohne Einwilligung des Arbeitnehmers stattfinden.

Letztlich bleibt nur daher noch die Einwilligung als Legitimation für die Datenerhebung und -verarbeitung. Zu beachten ist, dass das Angebot tatsächlich freiwillig sein muss und nicht an ein Bonusprogramm o.ä. gekoppelt sein sollte, da hierdurch ein emotionaler oder gar wirtschaftlicher Druck erzeugt werden könnte. Ein solcher könnte auch betriebsintern entstehen. Die Veröffentlichung der Daten an Kollegen o.ä. kann mangels Erforderlichkeit nur auf Grundlage einer Einwilligung erfolgen. Werden Preise für die Teilnahme ausgeschrieben und muss ein Arbeitgeber dafür Daten verarbeiten, so empfiehlt es sich, diese nur auf Abteilungsebene und nicht für individuelle Arbeitnehmer auszuschreiben, da ein Zugriff des Arbeitgebers auf diese sensiblen Daten auf das Mindestmaß beschränkt sein muss; in Betracht kommt eine anonyme, aggregierte Datenbasis für den Zugriff des Arbeitgebers.[1059]

(4) Abwägungsmaßstab

Der generelle Abwägungsmaßstab zur Zulässigkeit der Erhebung und Nutzung von Daten, die geeignet sind, einen Überwachungsdruck zu erzeugen, wurde durch die Rechtsprechung des BAG und BVerfG über Jahre konkretisiert. Maßgeblicher Faktor ist die sog. Eingriffsintensität der Maßnahme. Nach ständiger Rechtsprechung sind verschiedene Kriterien bei der Beurteilung der Maßnahme zu berücksichtigen: Anlassbezogenheit[1060] (also hat der Arbeitgeber einen konkreten Grund, die Daten zu erheben; hat der Arbeitnehmer möglicherweise die Verarbeitung sogar selbst veran-

1059 So wohl *Kopp/Sokoll*, NZA 2015, 1352 (1357).

1060 BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (1190) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54; Beschl. v. 29.06.2004 – 1 ABR 21/03, NZA 2004, 1278 = BAGE 111, 173 = AP BetrVG § 87 1972 Überwachung Nr. 41 (m. Anm. *Ehmann*).

lasst), Dauer der Überwachung[1061], Inhalt/Persönlichkeitsrelevanz[1062] bzw. Kernbereichsbezug[1063], Folgen[1064] und Heimlichkeit[1065].

(a) Belastungsstatistik-Entscheidung des BAG v. 25.04.2017

Eine aktuelle und besonders aufschlussreiche Entscheidung zum Thema Überwachung für Analytics stellt der Beschluss des BAG aus dem Jahr

1061 BAG, Beschl. v. 29.06.2004 – 1 ABR 21/03, NZA 2004, 1278 = BAGE 111, 173 = AP BetrVG § 87 1972 Überwachung Nr. 41 (m. Anm. Ehmann).

1062 BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54; BVerfG, Urt. v. 13.06.2007 – 1 BvR 1550/03, 2357/04, 603/05, BVerfGE 118, 168 (196 f.) – Kontostammdaten; Beschl. v. 04.04.2006 – 1 BvR 518/02, BVerfGE 115, 320 (348) = NJW 2006, 1939 – Rasterfahndung II; Urt. v. 14.07.1999 – 1 BvR 2226/94, 2420/95, 2437/95, BVerfGE 100, 313 (376) – Telekommunikationsüberwachung I; Urt. v. 03.03.2004 – 1 BvR 2378/98, 1084/99, BVerfGE 109, 279 (353) – Großer Lauschangriff.

1063 BVerfG, Urt. v. 27.02.2008 – 1 BvR 370, 595/07, BVerfGE 120, 274 (335 f.) – Online-Durchsuchungen; Urt. v. 03.03.2004 – 1 BvR 2378/98, 1084/99, BVerfGE 109, 279 (313) – Großer Lauschangriff; Beschl. v. 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367 (373 f.) – Tagebuch; BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (1189) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54.

1064 BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (1190) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54; BVerfG, Urt. v. 11.03.2008 – 1 BvR 2074/05, 1 BvR 1254/07, BVerfGE 120, 378 (403) = NJW 2008, 1505 – Automatische Kennzeichenerfassung; Urt. v. 13.06.2007 – 1 BvR 1550/03, 2357/04, 603/05, BVerfGE 118, 168 (197) – Kontostammdaten; Beschl. v. 04.04.2006 – 1 BvR 518/02, BVerfGE 115, 320 (351) = NJW 2006, 1939 – Rasterfahndung II; Urt. v. 03.03.2004 – 1 BvR 2378/98, 1084/99, BVerfGE 109, 279 (353) – Großer Lauschangriff; Urt. v. 14.07.1999 – 1 BvR 2226/94, 2420/95, 2437/95, BVerfGE 100, 313 (376) – Telekommunikationsüberwachung I.

1065 Grundlegend BVerfG, Urt. v. 03.03.2004 – 1 BvR 2378/98, 1084/99, BVerfGE 109, 279 – Großer Lauschangriff; ferner Beschl. v. 04.04.2006 – 1 BvR 518/02, BVerfGE 115, 320 (353) = NJW 2006, 1939 – Rasterfahndung II; Urt. v. 13.06.2007 – 1 BvR 1550/03, 2357/04, 603/05, BVerfGE 118, 168 (197) – Kontostammdaten; Urt. v. 11.03.2008 – 1 BvR 2074/05, 1 BvR 1254/07, BVerfGE 120, 378 (402 f.) = NJW 2008, 1505 – Automatische Kennzeichenerfassung; Urt. v. 27.02.2008 – 1 BvR 370, 595/07, BVerfGE 120, 274 (325) – Online-Durchsuchungen; spezifisch zum Arbeitnehmerdatenschutz BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (1189) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54.

2017 zu einer *Belastungsstatistik*[1066] dar, der im Folgenden näher betrachtet werden soll:

Im Rechtsstreit stand die Wirksamkeit eines Einigungsstellenspruchs im Fokus. Die Arbeitgeberin, ein Versicherungsunternehmen mit bundesweit 38 Schadenaußenstellen, hat mit dem Gesamtbetriebsrat nach einem Einigungsstellenverfahren per Spruch eine „Gesamtbetriebsvereinbarung zur Belastungsstatistik von Schadenaußenstellen" geschlossen. Die Zielsetzung dieser Vereinbarung war, Ungleichgewichte in der Belastungssituation der Außenstellen, der Gruppen und der Mitarbeiter zu erkennen und analysieren, um steuernd eingreifen zu können, sodass die Gruppenleiter eine gleichmäßigere Verteilung der Arbeitslast sowie eine sach- und mitarbeitergerechte Arbeitssteuerung vornehmen können. Ebenso sollte den einzelnen Sachbearbeitern ermöglicht werden, die eigene Arbeitssituation und das eigene Arbeitsverhalten zu erkennen und bewerten, um es im Bedarfsfall verändern zu können, sodass die Rahmenbedingungen der Arbeit verbessert werden. Hierfür sollte eine Reihe von spezifischen Kennzahlen ermittelt werden, bei denen jeweils Schwellenwerte hinterlegt sind. Auf diese Daten haben lediglich die Mitarbeiter in Bezug auf ihre eigenen Daten Zugriff sowie die Gruppenleiter im Rahmen ihrer Zuständigkeit für ihre Mitarbeiter. Erfasst wurden hierbei ausschließlich die Arbeitsmengen, unerledigten Rückstände der einzelnen Sachbearbeiter sowie die Merkmale der Leistungserbringung und Belastung nach einem in der Betriebsvereinbarung vorgegebenem Schema. Diese Werte wurden dann ins Verhältnis zu dem entsprechenden Durchschnittswert aller Sachbearbeiter der Gruppe (differenziert nach Einsatzkriterien) gesetzt. Wenn gewisse Schwellenwerte überschritten wurden, erfolgte der Ausweis der betreffenden Sachbearbeiterdaten.

Für die wöchentlichen Berichte wurden die Daten soweit möglich anonymisiert und grundsätzlich auf Gruppenebene aggregiert. Einzelne Sachbearbeiterberichte waren nur dann zugreifbar, wenn ein Mitarbeiter bei mindestens einer Haupt-Kennzahl erheblich vom Gruppendurchschnitt abwich. In diesem Fall waren dem Gruppenleiter jedoch auch nur die Kennzahlen mit erheblicher Abweichung zugänglich.

Für alle Daten gab es bestimmte Zugriffsfristen, in welchen die Vorgesetzten darauf zugreifen konnten; danach war der Zugriff technisch gesperrt.

Hiergegen hat der Gesamtbetriebsrat Klage erhoben und die Unwirksamkeit des Einigungsstellenspruchs geltend gemacht: Die Statistik führe

1066 BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205.

zu einer umfassenden Leistungs- und Verhaltensüberwachung mit einer unverhältnismäßigen Kontrolldichte, die das nach § 75 Abs. 2 BetrVG zu beachtende Persönlichkeitsrecht der Arbeitnehmer verletze.

Das BAG hat der Klage stattgegeben und den Einigungsstellenspruch für unwirksam erklärt. Zunächst führte es zum allgemeinen Persönlichkeitsrecht gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG aus und stellte fest, dass Eingriffe am Grundsatz der Verhältnismäßigkeit zu messen seien, welcher die Verpflichtung nach § 75 Abs. 2 BetrVG konkretisiere (Rn. 19). Weiterhin folge aus dem Normzweck des § 87 Abs. 1 Nr. 6 BetrVG, dass Arbeitnehmer vor Beeinträchtigungen des Persönlichkeitsrechts durch den Einsatz technischer Überwachungseinrichtungen bewahrt werden müssen, sofern diese nicht durch schützenswerte Belange des Arbeitgebers gerechtfertigt oder unverhältnismäßig sind.

Der Grundsatz der Verhältnismäßigkeit erfordere eine Regelung, die geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen ist, um den erstrebten legitimen Zweck zu erreichen (Rn. 21). Es dürfen keine anderen, gleich wirksamen Mittel zur Verfügung stehen, die das Persönlichkeitsrecht des Arbeitnehmers weniger einschränken. Eine Verhältnismäßigkeit sei gegeben, wenn die „Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht“[1067] (Rn. 21).

Es handle sich zwar um ein legitimes Anliegen des Arbeitgebers, eine unterschiedliche Belastungssituation der Arbeitnehmer und deren Ursachen in Erfahrung zu bringen, um steuernd eingreifen zu können und die Effizienz zu steigern (Rn. 25). Allerdings sei bereits zweifelhaft, ob das Mittel der „Belastungsstatistik“ auf dieses Ziel gerichtet sei. Durch die Belastungsstatistik würden ausschließlich Daten zur Erledigung von Arbeitsaufgaben erfasst, ohne Berücksichtigung der Komplexität der Aufgabe und der Qualität des Arbeitsergebnisses. Aus diesem Grund spreche bereits viel dafür, dass das eingesetzte Mittel untauglich sei, den erstrebten Zweck zu fördern.

Zwar könne man zugunsten der Arbeitgeberin davon ausgehen, dass die erhobenen Statistiken für den Zweck erforderlich seien. Dem stehe jedenfalls nicht entgegen, dass der jeweilige Gruppenleiter den „digitalen Arbeitskorb“ ebenfalls überwachen und steuern könne. Denn dies sei nur

1067 Ebenso BAG, Beschl. v. 15.04.2014 – 1 ABR 2/13 (B), NZA 2014, 551 (555) = BAGE 148, 26 = AP BetrVG 1972 § 29 Nr. 9 Rn. 41 unter Verweis auf BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, BVerfGE 115, 320 (1941 f.) = NJW 2006, 1939 – Rasterfahndung II Rn. 88.

„tagesaktuell" möglich, die Statistik hingegen solle eine Einschätzung über einen längeren Zeitraum ermöglichen.

Im Ergebnis seien die Eingriffe durch die Belastungsstatistik allerdings unverhältnismäßig im engeren Sinne (unangemessen), da sie einen schwerwiegenden Eingriff in das Persönlichkeitsrecht des betroffenen Arbeitnehmers darstellten, der durch schützenswerte Interessen des Arbeitgebers nicht zu rechtfertigen sei:

Durch die Gesamtbetriebsvereinbarung werde eine lückenlose, dauerhafte und sehr detaillierte Erfassung des wesentlichen Arbeitsspektrums der Sachbearbeiter geregelt (Rn. 29), sodass der einzelne Arbeitnehmer während der gesamten Dauer seiner Arbeitszeit in der Schadenaußenstelle davon ausgehen müsse, dass sein „wesentliches Arbeitsspektrum auf elektronischem Wege anhand einer Vielzahl von quantitativen Kriterien (Haupt- und Analysekennzahlen) im Rahmen der einzelnen ‚Arbeitsauslöser' durchgehend detailliert erfasst und einer Auswertung auf den Ebenen einer 1-Wochen-, 4-Wochen- und 26-Wochen-Sicht zugeführt würden. Sämtliche Auswertungen würden wochenweise fortgeschrieben und stünden jeweils am Ende der Arbeitswoche zur Verfügung. Dies führe zu einem ständigen Überwachungs- und daran anknüpfenden Anpassungs- und Leistungsdruck in allen wesentlichen Arbeitsbereichen." (Rn. 30). Arbeitnehmer würden dazu gedrängt, möglichst in allen maßgebenden Arbeitsbereichen in Bezug auf die Kennzahlen unauffällig zu arbeiten, um nicht aufgrund „erheblicher Abweichungen" in Personalgespräche zitiert zu werden oder personellen Maßnahmen ausgesetzt zu sein (Rn. 32).[1068]

Erschwerend komme hinzu, dass der einzelne Sachbearbeiter nur bei erheblichen Abweichungen seine Werte sehen könne und dann nur retrospektiv am Ende der jeweiligen Woche; die „erhebliche Auswertung" sei ferner nicht von einem fest bestimmten Wert abhängig, sondern von der jeweiligen Zusammensetzung der Gruppe und deren Ergebnisse, auf die der einzelne Arbeitnehmer keinen Einfluss habe (Rn. 33). Dazu komme, dass nur die Abweichungen ausgewiesen würden, nicht aber alle Werte, sodass der Sachbearbeiter in einzelnen Kennzahlen auch überdurchschnitt-

1068 Das BVerfG spricht hierbei von Freiheitsbeschränkung durch „Einschüchterungseffekten" aufgrund des Gefühls des „Überwachtwerdens", vgl. BVerfG, Urt. v. 11.03.2008 – 1 BvR 2074/05, 1 BvR 1254/07, BVerfGE 120, 378 (402) = NJW 2008, 1505 – Automatische Kennzeichenerfassung Rn. 78 m.w.N.; unter Verweis auf das Urteil des BVerfG ebenso BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (Rn. 1191) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54 Rn. 29.

lich sein könnte, was dann dem Gruppenleiter und ihm selbst nicht zugänglich wäre (Rn. 34).

(b) Bewertung

Die Entscheidung verdeutlicht, dass Überwachungsmaßnahmen nicht per se unverhältnismäßig sind, sondern es auf die konkrete Ausgestaltung ankommt. Arbeitgeber haben ein anerkanntes Interesse daran, Leistungs- und Verhaltenskontrollen im Rahmen der Durchführung vorzunehmen.[1069] Dabei ist „weniger nicht immer mehr": Ein entscheidender Punkt in der Verhältnismäßigkeit im engeren Sinn war, dass die Arbeitnehmer unter der Woche keinen Zugriff auf die aktuellen Daten hatten, sondern nur bei Überschreiten bestimmter Grenzwerte die Überschreitungen angezeigt bekommen haben (ebenso die Gruppenleiter). Die Anzeige anderer Daten hätte mitunter die Überdurchschnittlichkeit in anderen Bereichen aufzeigen und somit die Transparenz erhöhen können, mit dem Ergebnis eines geringeren Eingriffs in das Persönlichkeitsrecht. Im Kern der Entscheidung stand allerdings, dass die lückenlose Überwachung der Primärleistungspflicht zu einem Überwachungsdruck führt, die die Arbeitnehmer an der Wahrnehmung ihrer Freiheitsrechte hindern könnte, da aus dem „Überwachtwerden" ein Anpassungsdruck folgen könnte. Ausschlaggebende Kriterien nach eingangs dargestelltem Maßstab waren daher die Dauer der Überwachung sowie die (nicht hinreichende) Anlassbezogenheit.

In einem früheren Fall hat das BAG 1996 für sog. „Bedienerplatzreports" von Call-Center-Mitarbeitern hingegen die datenschutzrechtliche Zulässigkeit solcher Auswertungen angenommen.[1070] In diesen Reports konnten jeweils die Länge der Anrufe, die Verteilung der Anrufe auf die einzelnen Bedienplätze und nicht angenommene Anrufe dargestellt werden. Hintergrund der Entscheidung dürfte sein, dass sich die Erfassung lediglich auf den Arbeitsbereich und auf schlichte Zahlen und Fakten beschränkt, sodass nur eine fernliegende Gefahr eines allumfassenden Persönlichkeitsprofils bestand. Die Persönlichkeitsrelevanz war im Vergleich zur Belastungsstatistik daher geringer. Hinzu kommt das Kriterium der

1069 So auch *Schürmann*, Auswertung von Mitarbeiterdaten - (Any)/(No)thing possible?, in: Taeger, Smart world - smart law?, S. 503 m.w.N.

1070 BAG, Beschl. v. 30.08.1995 – 1 ABR 4/95, NZA 1996, 218.

Anlassbezogenheit: In Call-Centern ist eine Steuerung der Arbeitsplätze und Telefonate unabdingbar.[1071]

Wendet man die Schlüsse aus diesen Entscheidungen in Bezug auf die eingangs genannten Kriterien auf *Advanced People Analytics*-Maßnahmen an, so folgt daraus, dass die Analytics über die Primärleistungspflicht mit dem Zweck der Verbesserung der Arbeitssituation/Effizienzsteigerung, aber auch Leistungsüberwachung im Ausgangspunkt als legitim beachtet werden können, da sie einen bestimmten und berechtigten Anlass haben. Arbeitgeber verfolgen bei ersteren nicht nur selbstgelagerte Interessen, sondern auch solche seiner Arbeitnehmer. Für diese kann sich eine solche Überwachung zu ihren Gunsten auswirken, falls hierdurch eine Verringerung der Belastung stattfindet bzw. Überbelastungen erkannt und vermieden werden.

Voraussetzung ist aber in jedem Fall, dass die erhobenen Daten auch tatsächlich geeignet sind, das erstrebte Ziel zu fördern. Wird hierzu eine unzureichende oder falsche Datenbasis verwendet, so sind die Analytics bereits nicht tauglich. Zwar haben sich die Arbeitgeber am Grundsatz der Datenminimierung zu orientieren; dieser darf aber nicht derart ad absurdum geführt werden, dass die Daten ihre Aussagekraft verlieren und somit erst hierdurch ein unverhältnismäßiger Eingriff in das Persönlichkeitsrecht erfolgt. Bei IT-Nutzungsdaten muss daher genau überprüft werden, ob diese Daten im Hinblick auf das erstrebte Ziel aussagekräftig sind.

Beispiel: Die Erfassung der täglichen Bildschirmarbeitszeit (am PC angemeldet und nicht ausgeloggt) wäre kein taugliches Mittel zur Erfassung der Arbeitsbelastung oder Arbeitszeit, da es Zeiten geben kann, in welchen ein Arbeitnehmer zwar arbeitet, aber gerade telefoniert oder nicht am PC sitzt. Umgekehrt kann es Zeiten geben, in welchen der Arbeitnehmer zwar am PC angemeldet ist, jedoch nicht aktiv einer Arbeit nachgeht. Hingegen kann bei einem Call-Center-Mitarbeiter die Überwachung der Bildschirmarbeitszeit, zusammen mit der Auswertung von Anruflisten und dem Terminkalender des einzelnen Arbeitnehmers durchaus ein mögliches Mittel sein, etwaigen Arbeitszeitenbetrug aufzudecken oder zumindest Anhaltspunkte für die Leistungsfähigkeit des Arbeitnehmers zu geben (die Verhältnismäßigkeit nun außer Acht gelassen).

Abseits der Primärleistungspflichten, im Bereich der arbeitsvertraglichen Fürsorgepflicht nach § 241 Abs. 2 BGB, können Analytics anhand der gezeigten Maßstäbe jedoch in weiterem Maße durchgeführt werden,

1071 *Schürmann*, Auswertung von Mitarbeiterdaten - (Any)/(No)thing possible?, in: Taeger, Smart world - smart law?, S. 506.

sofern der Persönlichkeitsbezug möglichst geringgehalten wird. Hier ist der durch die Überwachung von bestimmten Daten erzeugte „Anpassungsdruck" deutlich geringer; personelle Maßnahmen sind in aller Regel nicht zu befürchten. Solche Auswertungen sind vor allem im Bereich der Personalentwicklung und der Gesundheitsvorsorge bzw. des Arbeitsschutzes auf Individualebene denkbar.

Beispiel: Anhand der ausgewerteten Bildschirmarbeitszeit könnte analysiert werden, wieviel Zeit der einzelne Arbeitnehmer vor dem Bildschirm verbringt. Nach § 5 der Bildschirmarbeitsverordnung (BildSchArbV) hat der Arbeitgeber die Tätigkeit der Beschäftigten so zu organisieren, dass die tägliche Arbeit an Bildschirmgeräten regelmäßig durch andere Tätigkeiten oder durch Pausen unterbrochen wird, die jeweils die Belastung durch die Arbeit am Bildschirmgerät verringern. Durch eine Analyse der Screen-Time (nicht des Bildschirminhalts!) kann der Arbeitgeber seiner arbeitsvertraglichen Fürsorgepflicht nachkommen und – sollte er feststellen, dass entsprechende Unterbrechungen nicht stattfinden – dem Arbeitnehmer entsprechend andere Zwischen-Tätigkeiten zugewiesen / angeboten werden oder beispielsweise durch eine eigene Software[1072] Pausen vorgeschlagen werden. Ebenso könnte die Screen-Time als Indikator genutzt werden, ob ein Arbeitnehmer viel sitzt (z.B., wenn keine höhenverstellbaren Schreibtische vorhanden sind) und diesem entsprechende Bewegungsangebote angeboten werden. Alternativ könnte der Arbeitgeber auch durch diese Kennzahl ermitteln, für welche Arbeitnehmer höhenverstellbare Schreibtische sinnvoll sind, um Haltungsschäden vorzubeugen und Bewegung anzuregen.

Zu beachten ist, dass die für die Ausübung der Fürsorgepflichten gesammelten Daten auch ausschließlich für diese Zwecke genutzt und nicht für Leistungskontrollen missbraucht werden dürfen. Hier müssen technisch-organisatorische Maßnahmen vorgesehen werden. Diese sollten dem Arbeitnehmer möglichst transparent und verständlich erklärt werden, um eventuelle „Überwachungsängste" zu vermeiden.[1073]

1072 Hierfür gibt es bereits unzählige, kostenlose Tools. Als Beispiele können EyeLoveU, Workrave (das darüber hinaus auch vor schlechter Haltung warnen soll), Time Out oder Eye Saver genannt werden.

1073 Eine Gefahr des Überwachungsdrucks bei der Nutzung von Sensordaten sehen auch *Brecht/Steinbrück/Wagner*, PinG 2018, 10 (11).

b) Die Nutzung von IT-Daten für Advanced People Analytics

Für die Nutzung von IT-Daten für *Advanced People Analytics* gilt derselbe Maßstab wie für die Erhebung. Dennoch muss eine Unterscheidung getroffen werden zwischen Daten, die der Arbeitgeber speziell für diese Zwecke aktiv erhebt und solchen, die aus anderen Gründen erhoben wurden, beispielsweise zum Zwecke der Gewährleistung der Funktionsfähigkeit und Integrität von IT-Systemen. Bei ersteren wurde die erforderliche Abwägung bereits vor der Erhebung der Daten getroffen und es ändert sich daher durch den weiteren Verarbeitungsvorgang für diesen Zweck grundsätzlich nichts an der Abwägung.

Bei letzteren hingegen wurden die Daten auf Basis einer anderen Legitimationsgrundlage und zu einem anderen Zweck erhoben, sodass einerseits die weiteren Voraussetzungen der Zweckänderung (sog. Kompatibilitätstest) nach Art. 6 Abs. 4 DSGVO[1074] und andererseits das Vorliegen der Voraussetzungen der neuen Legitimationsgrundlage (insbesondere die Erforderlichkeit für die Durchführung des Beschäftigungsverhältnisses nach § 26 Abs. 1 S. 1 BDSG bzw. zur Wahrnehmung berechtigter Interessen des Arbeitgebers nach Art. 6 Abs. 1 lit. f DSGVO)[1075] geprüft werden müssen.

aa) Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO

Sofern APA auf aggregierter und somit anonymer Basis stattfinden, d.h. die Ergebnisse nicht personenbezogen und ferner nicht auf Einzelpersonen angewandt werden, greift die unwiderlegliche Vermutung der Zweckvereinbarkeit gem. Art. 5 Abs. 1 lit. b i.V.m. Erwägungsgrund 152 und 162 DSGVO („Statistik-Ausnahme“).[1076] Dies ist insbesondere dann der Fall, wenn der Arbeitgeber Unternehmens-/Betriebs- oder Abteilungskennzahlen durch *Advanced People Analytics* berechnet und diese nicht für weitergehende Einzelmaßnahmen einsetzt. Hier stehen also die mittel- und langfristige Planung statt kurzfristiger Maßnahmen im Mittelpunkt.

Für alle anderen Auswertungen, also solche, die auf individualisierter Basis vorgenommen werden oder deren Ergebnisse auf Einzelpersonen angewandt werden, ist ein Kompatibilitätstest vorzunehmen. Aufgrund

---

1074 Ausführlich hierzu **E. § 1 I. 2.**

1075 Zum Streitstand bezüglich der Erforderlichkeit einer Legitimationsgrundlage bei einer zweckkompatiblen Weiterverarbeitung, siehe **E. § 1 I. 2. a**).

1076 Siehe bereits **E. § 1 I. 2. c**).

der strikteren Erlaubnistatbestände einer Zweckänderung im Vergleich zu Art. 6 Abs. 1 DSGVO bzw. § 26 Abs. 1 BDSG unterliegt die Weiterverarbeitung besonderen Hürden.[1077]

So muss geprüft werden, ob die Weiterverarbeitung mit den ursprünglichen Erhebungszwecken vereinbar ist, wobei unter anderem die Verbindung zwischen den Verarbeitungszwecken, der Zusammenhang zwischen Erhebung und Weiterverarbeitung, die Art der personenbezogenen Daten, die möglichen Folgen sowie das Vorhandensein vorhandener Garantien im Rahmen des Kompatibilitätstests untersucht werden müssen.[1078]

(1) Kriterien der Zweckvereinbarkeit

Bei der Verwendung von Log-Dateien ist zu beachten, dass der Zusammenhang zwischen Erhebung und Weiterverarbeitung grundsätzlich ein komplett verschiedener ist, die Zwecke also mithin nicht sehr eng verbunden sind (z.B. wie im Falle, wenn bereits erhobene Arbeitnehmerdaten für die Durchführung des Beschäftigungsverhältnisses für Analytics weiterverwendet werden sollen). Der Erhebungszweck von IT-Systemdaten dient – wie bereits erläutert – der Sicherstellung der Funktionsfähigkeit und Integrität von Informationssystemen und nicht primär dem Arbeitsverhältnis. Wenn man berücksichtigt, dass der Betroffene bei den IT-Systemdaten, sofern er zuvor nicht darauf aufmerksam gemacht wurde, nicht mit einer Verarbeitung für APA-Zwecke rechnet, so ist dies bereits ein Anhaltspunkt gegen eine Zweckvereinbarkeit.[1079] Hinzu kommt, dass nach Art. 6 Abs. 4 lit. b DSGVO auch die gegenseitige Abhängigkeit beachtet werden muss, da in dieser Konstellation möglicherweise kein „Gleichgewicht der Entscheidungsfreiheit" besteht:[1080] Der Arbeitnehmer ist zur Erfüllung seiner Leistungspflicht aus dem Arbeitsvertrag gezwungen, die IT-Systeme des Arbeitgebers zu nutzen und ist daher davon abhängig. Umgekehrt ist auch der Arbeitgeber verpflichtet, gewisse Systemdateien zu sammeln; damit muss ein Arbeitnehmer rechnen. Nicht hingegen muss er, sofern er bei Erhebung nicht darauf aufmerksam gemacht wurde, damit rechnen,

1077 EuArbRK/*Franzen*, Art. 6 DSGVO Rn. 13.

1078 Zu den Kriterien im Einzelnen, siehe die Ausführungen unter **E. § 1 I. 2. d**).

1079 Vgl. *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 187; siehe hierzu bereits **E. § 1 I. 2. d**) **aa**) m.w.N.

1080 *Monreal*, ZD 2016, 507 (510).

dass diese Daten später für die Beurteilung seiner persönlichen Leistung genutzt werden, also für Zwecke außerhalb des technischen Kontextes.

Gegen eine Zweckkompatibilität sprechen ferner die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen (Art. 6 Abs. 4 lit. d DSGVO). Zwar sind in diesem Zusammenhang nicht nur negative, sondern auch positive Folgen zu beachten. Eine Rolle spielen hierbei aber nicht nur rechtliche, sondern auch emotionale Folgen, wie beispielsweise die Angst, die Kontrolle über die eigenen Daten zu verlieren oder überwacht zu werden.[1081] Gerade, wenn notwendige IT-Systemdaten später für People Analytics und einer damit verbundenen Leistungsbeurteilung eingesetzt werden sollen, könnte dies die Angst der Arbeitnehmer vor unkontrollierbarer Überwachung schüren. Dies wären bereits negative Folgen, die berücksichtigt werden müssen. Dazu kommt, dass auch personelle Einzelmaßnahmen abgeleitet werden könnten, wenn in den Auswertungen festgestellt wird, dass gegen arbeitsvertragliche Pflichten oder das Gesetz verstoßen wird.

(2) Vertragliches Verarbeitungsverbot als geeignete Garantie zur Herstellung von Zweckkompatibilität?

Um eine Verarbeitung dennoch zu ermöglichen, ist daher die Frage aufzuwerfen, ob eine solche Zweckkompatibilität auf Basis von Art. 6 Abs. 4 lit. e DSGVO auch durch geeignete *juristische* Garantien wie beispielsweise einem vertraglich oder in einer Betriebsvereinbarung niedergelegten Verarbeitungsverbot hergestellt werden könnte. Wie bereits herausgearbeitet[1082], siedelt die DSGVO die Verarbeitungs-Garantien im Rahmen der Zweckkompatibilitätsprüfung vor allem auf der technischen Seite, bei den technisch-organisatorischen Maßnahmen an. Diese Garantien (außer eine Anonymisierung, die im Rahmen von People Analytics bereits Zweckkompatibilität herstellen würde[1083]) können die aufgeworfenen Probleme allerdings nicht beseitigen.

Fraglich ist daher, ob auch juristische Garantien wie beispielsweise eine Betriebsvereinbarung, die ein Beweisverwertungsverbot statuiert oder eine Gesamtzusage des Arbeitgebers, aus den hieraus gewonnenen Erkenntnis-

1081 *Article 29 Data Protection Working Party,* WP 203, S. 25 f.; vgl. auch im Detail **E. § 1 I. 2. d) dd)**.
1082 Vgl. oben **E. § 1 I. 2. d) ee)**.
1083 Siehe **E. § 1 I. 2. c)**.

sen keine negativen Folgen für den Arbeitnehmer herzuleiten, die Zweckkomptabilität herstellen können. Grundsätzlich werden in der Literatur rechtliche Vorkehrungen als mögliche Garantien erachtet.[1084] Allerdings beschränken sich die Vorschläge vor allem auf Geheimhaltungs- und Löschpflichten.[1085]

In Art. 46 DSGVO, der Regelung von Datenübermittlungen vorbehaltlich geeigneter Garantien, kommt ebenfalls derselbe Terminus vor, wobei dort in Abs. 2 lit. a auch rechtliche Garantien explizit genannt werden, z.B. ein rechtlich bindendes und durchsetzbares Dokument zwischen öffentlichen Stellen. Aus Erwägungsgrund 108 geht hervor, dass die Garantien im Rahmen von Art. 46 DSGVO dazu dienen sollen, dass die Datenschutzvorschriften und Rechte der betroffenen Personen auf eine der Verarbeitung innerhalb der Union angemessene Art und Weise beachtet werden sollen.

Aus der Systematik der DSGVO lässt sich nicht viel für die Beantwortung dieser Frage herleiten. Wenn man jedoch berücksichtigt, dass die Garantien im Zusammenhang mit dem Kriterium der möglichen Folgen für den Betroffenen zu sehen ist und der Datenschutzansatz risikobasiert ist,[1086] so müssen in dieser Folge auch Verarbeitungsverbote grundsätzlich eine taugliche Garantie darstellen. Dieser Ansatz wird durch den Wortlaut des Art. 35 Abs. 1 DSGVO bekräftigt, der von einem „hohen Risiko für die Rechte und Freiheiten natürlicher Personen spricht". Es kommt dabei nicht nur auf das Risiko eines Datenverlustes oder einer unbefugten Nutzung von Daten an, sondern insbesondere darauf, ob natürliche Personen (Betroffene) Rechts- und Freiheitseinbußen befürchten müssen, wenn der Verarbeiter die vorhandenen Daten über die Kompatibilitätsklausel des Art. 6 Abs. 4 DSGVO weiterverarbeitet. Als Risiko kann man allgemein „das Bestehen der Möglichkeit eines Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder das zu einem

1084 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 60; *Sander/Schumacher/Kühne*, ZD 2017, 105 (109); dagegen wohl *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 209.

1085 Sydow/*Reimer*, Art. 6 DSGVO Rn. 60; *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 60; wohl auch *Sander/Schumacher/Kühne*, ZD 2017, 105 (109).

1086 Vgl. hierzu bereits **E. § 1 I. 2. d) ee)**.

weiteren Schaden für eine oder mehrere natürliche Personen führen kann" bezeichnen.[1087]

Dies entspricht auch dem in Art. 1 Abs. 2 DSGVO ausdrücklich festgelegten Ziel: Der Schwerpunkt der DSGVO liegt zwar auf dem Schutz der personenbezogenen Daten, ferner aber auch auf dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen.

Aus diesem Grund kann ein Verarbeitungsverbot im Rahmen einer Zusicherung durch den Arbeitgeber durchaus eine geeignete Garantie im Rahmen von Art. 6 Abs. 4 DSGVO darstellen.

(3) Keine Zweckkompatibilität von IT-Systemdaten mit People Analytics

Zwar können Verarbeitungsverbote grundsätzlich eine geeignete Garantie darstellen, für den Fall der People Analytics stellt sich allerdings die Frage, ob eine Zusage des Arbeitgebers, keine nachteiligen Folgen aus den für Analytics verwendeten IT-Systemdaten für Arbeitnehmer zu generieren, den bereits genannten Gefahren hinreichend begegnen kann, um zu einer Zweckkompatibilität zwischen Erhebungszweck und Weiterverarbeitungszweck zu kommen.

Dies ist zu verneinen: Einerseits wäre es dann Arbeitgebern möglich, auch rückwirkend Daten zu Analyticszwecken heranzuziehen, bei denen die Arbeitnehmer noch keine Kenntnis davon hatten, dass diese Daten für weitere Zwecke genutzt werden könnten. Andererseits ist dem Arbeitgeber auch bei späterer Einführung von (Advanced) People Analytics zuzumuten, die Daten erst ab diesem Zeitpunkt zu erheben (z.B. indem eine bestimmte Datenaufzeichnung erst dann aktiviert wird) und in diesem Rahmen der Erhebung den weitergehenden Verarbeitungszweck für IT-Systemdaten festzulegen, sodass es einer zweckkompatiblen Weiterverarbeitung nicht bedarf. Eine vertragliche Zusicherung kann die hieraus resultierenden Überwachungsängste der Betroffenen nicht verhindern.

Hingegen wäre es auch möglich, die retrospektiven Daten auf anonymer Basis auszuwerten (in diesem Fall wird die Zweckkompatibilität unwiderleglich vermutet), um festzustellen, ob die Auswertungen hilfreiche Erkenntnisse für das Personalwesen erzeugen können. Bei einer solchen Auswertung haben Arbeitnehmer keine Folgen zu befürchten, da Rück-

1087 *DSK*, Kurzpapier Nr. 18 - Risiko für die Rechte und Freiheiten natürlicher Personen, <www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf> , S. 1 unter Rückgriff auf die Erwägungsgründe 75 und 94 S. 2.

schlüsse auf die einzelne Person nicht möglich sind. Für Datenpunkte, bei denen relevante Korrelationen feststellbar sind, können Verarbeiter, respektive Arbeitgeber, im Anschluss an die Feststellung für die weitere zukünftige Erhebung festlegen, dass diese auch für die Zwecke von People Analytics in personenbezogener Form genutzt werden (die weiteren Rechtmäßigkeitsvoraussetzungen aus § 26 Abs. 1 BDSG müssen selbstverständlich vorliegen). Somit sind zwar keine personenbezogenen rückblickenden Analytics (bezogen auf IT-Daten vor dem Zeitpunkt der Zweckerweiterung des jeweiligen Datenpunkts) möglich, hingegen aber für die Zukunft. Dies erfordert aber auch der Schutz der Rechte und Freiheiten des Arbeitnehmers, der zumindest im Rahmen der Erhebung bereits damit rechnen können muss (Stichwort: „*Missing Link*"), dass diese Daten auch für das Personalwesen von Bedeutung sein können bzw. im Rahmen des Human Ressource Managements verarbeitet werden.

Bei der Einführung von APA sollten Arbeitgeber daher möglichst mit Hilfe anonymisierter Daten mögliche relevante Zusammenhänge, die sich aus einer Verarbeitung von IT-Systemdaten ergeben können, erkennen, bevor eine Zweckerweiterung bei der Datenerhebung vorgenommen wird. Erst nach erfolgter Zweckerweiterung vor der zukünftigen Erhebung der jeweiligen Datenpunkte stellen solche Daten eine geeignete Grundlage für Advanced People Analytics dar. Somit ist die Geeignetheit der Datenverarbeitung sichergestellt und kann durch den Arbeitgeber im Rahmen seiner Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO auch nachgewiesen werden.

bb) Zulässigkeit der Nutzung von IT-Daten für Advanced People Analytics

Ist eine Zweckerweiterung im Rahmen der Datenerhebung vorgenommen worden (und der Arbeitnehmer nach Art. 13 f. DSGVO darüber informiert worden), muss die Nutzung der Daten am Maßstab des § 26 Abs. 1 BDSG gemessen werden, wenn die Daten für APA genutzt werden sollen. Hierbei gilt derselbe Maßstab wie bei der Erhebung von IT-Systemdaten (siehe **E. § 1 III. 2. a) cc) (4)**).

(1) Legitimation für den Vorgang der Anonymisierung erforderlich

Für die Daten, die für die Nutzung anonymisiert werden, ist nach der Anonymisierung kein Datenschutzrecht mehr anwendbar, sodass die Verarbeiter diese Daten frei verarbeiten können, sofern durch die Verknüpfung unterschiedlicher anonymer Datensätze keine personenbezogenen Daten entstehen.[1088] Der Vorgang der Anonymisierung selbst muss jedoch legitimiert sein, da hierfür (zunächst) personenbezogene Daten als Grundlage für einen Verarbeitungsvorgang dienen. Hier darf analog der Anonymisierung bei Simple People Analytics mangels entgegenstehender Interessen des Arbeitnehmers (keine Rückführbarkeit mehr möglich, somit keine Beeinträchtigung von Freiheiten und Rechte) von einer Zulässigkeit des Verarbeitungsvorgangs ausgegangen werden.[1089] Legitimationsgrundlage dürfte in aller Regel mangels Bezugs der Auswertungen zu einem konkreten Beschäftigungsverhältnis Art. 6 Abs. 1 lit. f DSGVO sein, andernfalls § 26 Abs. 1 S. 1 BDSG.

(2) Besonderheiten bei der Nutzung von TK- und Standortdaten

Nach der hier vertretenen Auffassung stellt auch das Telekommunikationsrecht keine weiteren Grenzen bei der Nutzung von IT-Systemdaten für People Analytics, da der Arbeitgeber in jenem Bereich, wo etwaige nützliche Daten erhoben würden (Arbeitsrechner des Beschäftigten) nicht als Diensteanbieter im Sinne des TKG anzusehen ist.[1090] Da jedoch insbesondere die Datenschutzbehörden der Auffassung sind, dass die §§ 88 ff. TKG bei erlaubter Privatnutzung anwendbar sind, sollten sich Arbeitgeber der Risiken (insbesondere in strafrechtlicher Hinsicht, § 206 StGB) bewusst sein, wenn sie Telekommunikationsdaten für APA auswerten. Von § 88 Abs. 1 TKG sind nicht nur der Inhalt der Telekommunikation, sondern auch die näheren Umstände wie Telekommunikationsteilnehmer (E-Mail-Absender und Empfänger) sowie alle sonstigen Daten erfasst, die nicht schon als Inhalt erfasst werden; es besteht ein umfassender Schutz.[1091] § 88 Abs. 3 TKG regelt genau, für welche Zwecke die Daten genutzt werden dürfen: Grundsätzlich dürfen solche Daten nur für das für die geschäftsmä-

1088 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 256.
1089 Vgl. **E. § 1 III. 1. a) aa)**.
1090 Zum Streitstand siehe bereits **D. § 3 I.**
1091 *Bock*, in: Geppert/Schütz, Beck'scher TKG-Kommentar, § 88 TKG Rn. 14.

ßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß verwendet werden. Dies inkludiert beispielsweise die Fehlerbehebung, elektronische Erfassung von Telefonaten für die Abrechnung oder die Erkennung der missbräuchlichen Nutzung solcher Systeme.[1092]

Ebenfalls von Bedeutung ist dieser Streit für die Nutzung von Standortdaten, wenn das GPS-Modul[1093] des Mobiltelefons dafür genutzt werden soll, diese zu erfassen und auszuwerten. Ist der Arbeitgeber als Diensteanbieter im Sinne des TKG anzusehen, so könnte für die Verarbeitung von Standortdaten § 98 TKG Anwendung finden, mit der Folge, dass eine Einwilligung zum Abruf dieser Daten beim Arbeitnehmer eingeholt werden müsste. Standortdaten sind nach § 3 Nr. 19 TKG solche Daten, die in einem Telekommunikations-Netz erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines TK-Dienstes für die Öffentlichkeit angeben. Unter den Begriff des TK-Netzes (vgl. § 3 Nr. 27 TKG) ist jedoch nicht das Sattelitennetz, über welches GPS funktioniert, zu fassen.[1094] Hintergrund hierfür ist, dass keine Datenübermittlung im Satellitennetz stattfindet, sondern das Mobiltelefon lediglich die Standortdaten von bestimmten Satelliten zu bestimmten Zeiten erfasst und die Positionsbestimmung ausschließlich im Endgerät stattfindet; es werden also keine Nachrichten über das Satellitennetz übermittelt.[1095]

Da jedoch die Ortung bei modernen Mobiltelefonen nicht mehr ausschließlich satellitenbasiert, sondern auch über nahegelegene drahtlose Netzwerke (WLAN)[1096] sowie Mobilfunknetze stattfindet,[1097] ist die obige

---

1092 Beispiele aus *Bock*, in: Geppert/Schütz, Beck'scher TKG-Kommentar, § 88 TKG Rn. 27; für das letzte Beispiel ergibt sich die Legitimation nicht bereits aus § 88 Abs. 3 S. 1, sondern aus S. 2 i.V.m. § 100 Abs. 3 TKG.

1093 Von dem Begriff „GPS" werden für die Zwecke dieser Arbeit nicht nur Ortungen über das GPS-System, sondern über sämtliche satellitenbasierte Systeme erfasst (so also auch Ortungen über GLONASS/GALILEO).

1094 Plath/*Jenny*, § 98 TKG Rn. 10; a.A. *Steidle*, MMR 2009, 167 (168); *Eckhardt*, in: Spindler/Schuster, Recht der elektronischen Medien, § 98 TKG Rn. 9, der seine Auffassung mit der Gegenauffassung belegt und nicht weiter begründet.

1095 Plath/*Jenny*, § 98 TKG Rn. 10; *Maier/Ossoinig*, VuR 2015, 330 (333 f.).

1096 Sogenanntes Wi-Fi Positioning System (WPS); dies funktioniert so, dass in einer Geo-Datenbank die Lokalisationsdaten der einzelnen Zugangspunkte gespeichert werden und das Mobiltelefon die sich in der Nähe befindlichen Access-Points mit der Datenbank abgleicht, wodurch der Standort ziemlich genau ermittelt werden kann, vgl. *Maier/Ossoinig*, VuR 2015, 330 (334) Eine solche Datenbank ist beispielsweise www.wigle.net.

1097 Siehe hierzu https://www.heise.de/ct/hotline/FAQ-Ortung-auf-dem-Smartphone-2450476.html (letzter Abruf am: 07.02.2020).

Diskussion weitgehend obsolet, da in der Regel die Software nicht darauf programmiert ist, ausschließlich das integrierte GPS-Modul zu nutzen. Sobald Mobilfunk-Stationsdaten verwendet werden, ist § 98 TKG anwendbar, mit der Folge, dass diese Daten entweder anonymisiert erfasst werden müssen oder die Einwilligung des Teilnehmers eingeholt werden muss.

Bei der Inanspruchnahme von Dienstleistern für Location Based Services (LBS), wie beispielsweise der Ortung von Diensthandys des Arbeitgebers durch den Mobilfunkanbieter, ist Teilnehmer der Arbeitgeber, der die Dienste in Anspruch nimmt.[1098] Dieser muss dann allerdings seine Arbeitnehmer als Nutzer nach § 98 Abs. 1 S. 7 TKG über die erteilte Einwilligung zur Standorterfassung informieren.[1099] Sofern auf Standortdaten aufgrund einer Einwilligung des Teilnehmers zugegriffen wird, ist bei jedem Standortzugriff eine Textmitteilung (SMS) an das Endgerät zu senden, § 98 Abs. 1 S. 2 TKG.

Werden LBS hingegen durch den Arbeitgeber selbst durchgeführt, findet § 98 TKG keine Anwendung, da nach allgemeiner Meinung der Arbeitgeber bei rein dienstlicher Kommunikation kein Diensteanbieter im Sinne des TKG ist.[1100]

Unabhängig der Anwendbarkeit des Telekommunikationsrechts ist es in jedem Fall erforderlich, die Verarbeitung solcher Daten an § 26 Abs. 1 S. 1 BDSG zu messen. Die Standort-Überwachung von Arbeitnehmern unterliegt aufgrund des gravierenden Eingriffs in die Persönlichkeitsrechte hohen Voraussetzungen, die im Einzelfall anhand der dargestellten Kriterien zur Erforderlichkeit zu prüfen sind. Es sind allerdings keine Fälle denkbar, in denen solche – außerhalb der Zwecke des § 26 Abs. 2 S. 2 BDSG – heimlich erfolgen könnte.[1101] Zudem muss ausgeschlossen sein, dass der private Bereich des Beschäftigten mitüberwacht wird, z.B. wenn dieser das Dienst-Telefon auch mit nach Hause nehmen darf oder eine Pause macht. In Frage kommt eine Standorterfassung vor allem dann, wenn diese für die Sicherheit des Beschäftigten oder für den Schutz äußerst wertvoller Gegenstände des Arbeitgebers erforderlich ist.[1102] Abweichendes kann dann

1098 *Steidle*, MMR 2009, 167 (169).

1099 *Gola*, ZD 2012, 308 (309); *Seifert*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 88 DSGVO Rn. 142.

1100 Siehe **D. § 3 I. 1**; unklar *Seifert*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 88 DSGVO Rn. 142, der die Notwendigkeit einer Einwilligung und der Information des Beschäftigten ohne nähere Differenzierung annimmt.

1101 So auch WHWS/*Byers*, B. VII. GPS-Ortung, Rn. 27.

1102 *Seifert*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 88 DSGVO Rn. 142.

gelten, wenn diese anonymisiert werden. Hier muss jedoch in aller Regel an der Wirksamkeit der Anonymisierung gezweifelt werden: Standortdaten in Verbindung mit den Schichtplänen der jeweiligen Arbeitnehmer führen in aller Regel wieder zu einer Identifizierbarkeit. Der praktische Anwendungsbereich ist daher allenfalls marginal.

Etwas anderes gilt für die Ortung selbstverständlich dann, wenn diese auf Basis eines Gesetzes erfolgt, beispielsweise im Rahmen der digitalen Tachographen.[1103] In diesem Fall besteht eine Legitimation für die Verarbeitung nach Art. 6 Abs. 1 lit. c DSGVO, soweit diese zur Erfüllung der Pflicht erfolgt. Teilweise wird eine Fahrzeug-Ortung zur Optimierung der Ressourcennutzung im Rahmen des Flottenmanagements als zulässig erachtet, wenn sie offen und ausschließlich während der Arbeitszeit mit genauer Zweckfestlegung erfolgt.[1104] Darüberhinausgehende Auswertungen beispielsweise für People Analytics sind hiervon aber nicht gedeckt.

Da ein sinnvoller Anwendungsbereich für eine zulässige Ortung mittels LBS für People Analytics nicht ersichtlich ist, bleibt dieses Feld in dieser Arbeit außer Betracht.

c) Profiling und Scoring im Rahmen von Advanced People Analytics

Sollen die zulässigerweise erhobenen IT-Daten für Profiling genutzt werden, so handelt es sich hierbei um einen gesonderten Verarbeitungsvorgang[1105], der eigens an den Maßstäben des § 26 Abs. 1 BDSG gemessen werden muss. Dieser Vorgang des Profilings ist bei Advanced People Analytics von besonderer Bedeutung, da die erhobenen Daten nicht bloß menschenlesbar dargestellt, sondern durch eine inhaltliche Bewertung der Daten auch ein Mehrwert generiert werden soll. Hierzu ist es in aller Regel erforderlich, diese ins Verhältnis zu anderen Beschäftigten zu setzen, um eine Vergleichbarkeit herzustellen (hierzu bereits **E. § 1 II. 3** und **4**).

1103 *Kort*, RdA 2018, 24 (28); HdbIT-DSR/*Conrad/Treeger*, § 34 Recht des Datenschutzes, Rn. 301.

1104 WHWS/*Byers*, B. VII. GPS-Ortung, Rn. Rn. 29, 36 f.

1105 Siehe **E. § 1 II. 2**.

aa) Zweckbestimmung der Daten

Da die Verarbeitung zum Zwecke des Profilings ein eigener Verarbeitungsvorgang ist, muss dieser bereits bei der Erhebung der Daten vom Zweck umfasst sein, andernfalls ist eine Kompatibilitätsprüfung nach Art. 6 Abs. 4 DSGVO vorzunehmen. Bei der Zweckfestlegung ist darauf zu achten, dass dieser eindeutig und klar verständlich bestimmt ist.

(1) Spezifität der Zweckbestimmung

Sofern die Verarbeitung nicht auf den gesetzlichen Erlaubnistatbestand des § 26 Abs. 1 S. 1 BDSG gestützt wird, sondern aufgrund einer Einwilligung oder Betriebsvereinbarung erfolgen soll, müssen die Vorgaben zur Zweckbestimmung bei der Erhebung beachtet werden.[1106] Da feststellbar sein muss, welche Verarbeitungsvorgänge vom Zweck erfasst sind,[1107] dürfen auch im Rahmen einer Betriebsvereinbarung nicht zu vage Zwecke festgelegt werden. Aus diesem Grund wird es nicht ausreichend sein, wenn in einer Betriebsvereinbarung lediglich geregelt wird, dass die Daten zum Zwecke der *People Analytics* oder *Advanced People Analytics* verarbeitet werden, da diese ein sehr breites Feld darstellen und wie sich bereits aus den bisherigen Ausführungen zeigt, eine Vielzahl von Verarbeitungsvorgängen erfasst werden können.

Geboten ist daher eine Angabe, welche Analysen mit den Daten (insbesondere bei personenbezogenen Daten) angestrebt werden und ob Profiling-Maßnahmen stattfinden. Nur so kann überprüft werden, ob die Vorgänge auch vom in der Betriebsvereinbarung statuierten Zweck erfasst sind. Andernfalls müsste eine Definition des Begriffs „People Analytics" stattfinden, der die Zweckbestimmung weiter konkretisiert und die Verarbeitungsvorgänge so konkret wie möglich nennt, ohne zur Unverständlichkeit der Zweckbestimmung zu führen.

Beispielsweise könnte eine zulässige Zweckbestimmung lauten: „*Die Erfassung des Werts der Bildschirmzeit erfolgt zum Zwecke der Gesundheitsförderung des Arbeitnehmers durch Verhinderung von unergonomischen Bildschirm-*

1106 In aller Regel ist der Zweck der People Analytics für das konkrete Beschäftigungsverhältnis bereits durch die gesetzliche Zweckbestimmung in § 26 Abs. 1 S. 1 BDSG erfasst; hierzu bereits **E. § 1 I. 1. a**).

1107 *Article 29 Data Protection Working Party*, WP 203, S. 15; ebenso wohl EuArbRK/*Franzen*, Art. 5 DSGVO Rn. 5.

zeiten im Rahmen der durchgeführten People Analytics. Hierbei wird im Vergleich zu anderen Arbeitnehmern ein Vergleichswert generiert, der signifikante Abweichungen (mehr als 20 % über der durchschnittlichen Bildschirmzeit) erfasst und bewertet."

(2) Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO

Wurden die Daten bereits zum Zwecke der Durchführung des Arbeitsverhältnisses erhoben und sind weitergehende Analytics nicht mehr rechtssicher durch § 26 Abs. 1 S. 1 BDSG erfasst, sollte für die weitere Verarbeitung (das Profiling) eine Betriebsvereinbarung abgeschlossen werden. In diesen Fällen ist ein Kompatibilitätstest vorzunehmen. Etwas anderes gilt bei der (erneuten) Einwilligung zur Verarbeitung, da eine solche eine Legitimation zur Zweckänderung darstellen kann (Art. 6 Abs. 4 S. 1 DSGVO). Diese Privilegierung gilt allerdings nicht für Kollektivvereinbarungen, da Art. 6 Abs. 4 S. 1 DSGVO explizit eine Rechtsvorschrift der Union oder der Mitgliedsstaaten, die den Zielen des Art. 23 DSGVO dient, erfordert.

Anders als bei der Nutzung von IT-Systemdaten für People Analytics-Zwecke sind die Erhebungs- und Verarbeitungszwecke, wenn die Daten bereits zur Durchführung des Beschäftigungsverhältnisses erhoben wurden, sehr ähnlich und stehen in enger Verbindung, wenn die weiterführenden *People Analytics* zur Optimierung des Beschäftigungsverhältnisses oder der Arbeitsbedingungen genutzt werden sollen.

Mangels differenzierter höchstrichterlicher Rechtsprechung zum Themenkomplex *People Analytics* könnten Arbeitgeber Zweifel daran haben, ob ein Gericht im Streitfall die weitere Datenverarbeitung als „erforderlich" im Rahmen von § 26 Abs. 1 S. 1 BDSG erachten würde. Aus diesem Grund wird in der Praxis vielfach das Mittel der Betriebsvereinbarung gewählt und versucht, eine diesbezügliche Einigung mit dem Betriebsrat zu erzielen. Auch hier müssen die Betriebspartner aufgrund § 75 Abs. 2 BetrVG eine dem § 26 Abs. 1 S. 1 BDSG entsprechende Abwägung vorzunehmen; bei der Gewichtung der einzelnen Interessen steht ihnen jedoch ein (gerichtlich nur begrenzt überprüfbarer) Einschätzungsspielraum zu,[1108] sodass keine identische Erforderlichkeits- bzw. Verhältnismäßig-

1108 BAG, Beschl. v. 29.06.2004 – 1 ABR 21/03, NZA 2004, 1278 (1280) = BAGE 111, 173 = AP BetrVG § 87 1972 Überwachung Nr. 41 (m. Anm. Ehmann) im Hinblick auf die Erforderlichkeit der Datenverarbeitung im Rahmen der Abwägung nach § 75 Abs. 2 BetrVG.

keitsprüfung durch die Gerichte stattfindet, in welcher die gegenseitigen Interessen vom Gericht abschließend gewichtet werden. In gewissem Maß kann eine Parallele zur „Richtigkeitsgewähr des Tarifvertrags" durch den Schutz des Kollektivs gezogen werden.[1109]

Prüfungsgegenstand der gerichtlichen Kontrolle ist dann insbesondere das Überschreiten des eigenen Ermessensspielraums bei der Beurteilung, wodurch ein höheres Maß an rechtlicher Sicherheit geschaffen werden kann. Ebenfalls können weitere Zwecke außerhalb der Durchführung des Beschäftigungsverhältnisses durch eine Betriebsvereinbarung legitimiert werden. Da diese in der Regel eng mit dem Erhebungszweck zusammenhängen, ist eine Zweckvereinbarkeit – anders als bei IT-Systemdaten – nicht von vornherein ausgeschlossen, sondern in aller Regel gegeben.

Im Vergleich zum zuvor bei den Systemdaten vorgenommenen Kompatibilitätstest liegt gerade kein „*Missing Link*" vor, denn die Arbeitnehmer müssen damit rechnen, dass ihre personenbezogenen Daten auch für Zwecke der Optimierung der Geschäftsabläufe und Effektivierung der Arbeit durch Arbeitgeber genutzt werden.

Um allerdings den potenziellen negativen Folgen, die ein solches Profiling mit sich bringt, Rechnung zu tragen, müssen Arbeitnehmer bei zweckkompatibel verarbeiteten Daten – soweit es der konkrete Verarbeitungszweck zulässt – vor negativen Folgen geschützt werden. Grund hierfür ist, dass die Arbeitnehmer bei dieser Form der Verarbeitung – anders als wenn bereits die Daten auf Grundlage einer „weiten" Betriebsvereinbarung erhoben werden – bei der Erhebung noch nicht informiert wurden, dass ein Profiling mit ihren Daten stattfinden wird. Hierzu können in der Betriebsvereinbarung juristische Garantien für die Arbeitnehmer vorgesehen werden (**E. § 1 III. 2. b**) (**2**)).

bb) Rechtliche Vorgaben für das Profiling: Anwendbarkeit des § 31 Abs. 1 BDSG

Die DSGVO bestimmt für den in Art. 4 Nr. 4 definierten Begriff des *Profilings* keine weiteren Rechtmäßigkeitsvoraussetzungen, wie beispielsweise der nationale Gesetzgeber in § 31 BDSG für das Scoring. Nach § 31 Abs. 1 ist die „*Verwendung eines Wahrscheinlichkeitswerts über ein bestimmtes zukünftiges Verhalten einer natürlichen Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses*

1109 BeckOK DatenSR/*Riesenhuber*, Art. 88 DSGVO Rn. 68.

mit dieser Person (Scoring) nur zulässig, wenn […] 2. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit erheblich sind".

Scoring beruht auf der Grundhypothese, dass der Eintritt eines ähnlichen Verhaltens umso wahrscheinlicher ist, je mehr Faktoren einer Vergleichsgruppe in einer Person vereint sind.[1110] Score-Werte stellen Auffassung des BGH Meinungsäußerungen dar.[1111]

Ausweislich der Gesetzesbegründung[1112] und der Überschrift „Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften" hatte der Gesetzgeber nur das Kredit-Scoring im Blick, obwohl der Wortlaut des § 31 Abs. 1 BDSG jegliches Scoring bzw. Profiling erfasst.[1113] Es stellt sich also die Frage, ob die strengen Vorgaben zum Scoring auch für Maßnahmen im Rahmen von *People Analytics* anzuwenden sind.[1114] § 31 Abs. 2 BDSG kann hierbei außer Betracht bleiben, da sich diese Vorschrift auch materiell ausschließlich auf die Zahlungsfähig- und Zahlungswilligkeit einer Person bezieht.

(1) Europarechtswidrigkeit der Vorschrift

Überwiegend wird vorgebracht, dass die Vorschrift mangels entsprechender Öffnungsklausel in der DSGVO europarechtswidrig sei.[1115] § 31 Abs. 1

1110 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 105.

1111 Zum Bonitätsscore BGH, Urt. v. 22.02.2011 – VI ZR 120/10, NJW 2011, 2204; zu Score-Werten allgemein *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 105.

1112 BT-Drs. 18/11325, S. 101 f.

1113 Gegen eine Anwendbarkeit daher *Rudkowski*, NZA 2019, 72 (75); so wohl auch *Kainer/Weber*, BB 2017, 2740 (2747); für eine Anwendbarkeit (von § 28b BDSG a.F.) wohl *Diercks*, PinG 2016, 30 (31); aufgrund des Wortlauts von § 28b BDSG a.F. ebenso im Grundsatz *Eschholz*, DuD 2017, 180.

1114 Für eine solche Interpretation *Hoeren*, MMR 2016, 8 (10).

1115 *Ehmann*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Anh. 2 zu Art. 6 DSGVO Rn. 17; wohl ebenso *Lapp*, in: Gola/Heckmann, BDSG, § 31 BDSG Rn. 4; unklar *Schulz*, zfm 2017, 91 (95 f.); im Ergebnis ebenso *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 166; *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, § 31 BDSG Rn. 4 f.; kritisch hierzu auch *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 110: Allenfalls als verbraucherschützende Vorschrift in unionsrechtskonformer Auslegung; a.A. *von Lewin-*

BDSG spezifiziert die Vorgaben für Scoring als einen Sonderfall des Profiling über die Vorgaben der Art. 6 und 22 DSGVO hinaus, ohne dass die jeweiligen Normen eine entsprechende Öffnungsklausel enthalten; auch Art. 22 Abs. 2 S. 1 lit. b DSGVO sei nicht anwendbar, da dies nur Fälle betreffe, in denen das Scoring Grundlage einer automatisierten Einzelfallentscheidung sei, während die Regelung des § 31 BDSG auch Profiling-Vorgänge ohne Entscheidung erfasse.[1116] Dagegen wird argumentiert, dass es auch „implizite Öffnungsklauseln" bei nicht abschließenden oder unvollständigen Regelungen in der DSGVO gebe und der deutsche Gesetzgeber einen solchen Gestaltungsspielraum in Anspruch genommen habe.[1117] In der Gesetzesbegründung nennt der Gesetzgeber jedenfalls keine Öffnungsklausel, auf die er sich stützt.[1118] Teilweise wird erwogen, § 31 Abs. 1 BDSG auf die Öffnungsklausel des Art. 6 Abs. 4 S. 1 i.V.m. Art. 23 Abs. 1 lit. i DSGVO zu stützen.[1119] Hiernach wäre eine Zweckänderung zulässig, wenn dies eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme darstellt, um den Schutz der betroffenen Personen oder der Rechte und Freiheiten anderer Personen sicherzustellen. Anwendbar wäre dann die Vorschrift jedoch nur, wenn das vorgenommene Scoring nicht bereits Erhebungszweck ist; § 31 Abs. 1 BDSG geht jedoch darüber hinaus und stellt allgemeine Regelungen für das Scoring auf, nicht nur für die Zweckänderung, sodass die Norm von dieser Öffnungsklausel nicht mehr erfasst ist. Auch das Argument der Unterkomplexität der DSGVO und der hierdurch geschaffenen „impliziten Öffnungsklauseln" überzeugt nicht: Gesetzlich vorweggenommene und abschließende Wertungen nationaler Gesetzgeber sind in Bezug auf abstrakte Formulierungen des europäischen Gesetzgebers unzulässig.[1120]

---

ski/Pohl, ZD 2018, 17 (19): § 31 BDSG beruhe auf einer impliziten Öffnungsklausel.

1116 *Ehmann*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Anh. 2 zu Art. 6 DSGVO Rn. 20; *Abel*, ZD 2018, 103 (105); Plath/*Kamlah*, Art. 22 DSGVO Rn. 9; a.A. HK DSGVO/BDSG/*Atzert*, Art. 22 DSGVO Rn. 93 ohne weitere Begründung.

1117 *von Lewinski/Pohl*, ZD 2018, 17 (19).

1118 BT-Drs. 18/11325, S. 101 f.

1119 *Schulz*, zfm 2017, 91 (94); *Hoeren/Niehoff*, RW 2018, 47 (64) stellen auf lit. e ab; ebenso *Taeger*, RDV 2017, 3 (7).

1120 So sogar zu einer Richtlinie: EuGH, Urt. v. 19.10.2016 – C-582/14, NJW, 2016, 3579 (3582) – Breyer Rn. 62 ff.; vgl. *Ehmann*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Anh. 2 zu Art. 6 DSGVO Rn. 21 m.w.N. aus der Rechtsprechung.

Selbst wenn man § 31 BDSG als Diskriminierungsschutz anstatt als datenschutzrechtliche Vorschrift sieht,[1121] bestehen aufgrund der Verortung im BDSG und dem Vereinheitlichungsgedanken der DSGVO erhebliche Bedenken: Die DSGVO soll ein (weitgehend) einheitliches Datenschutzniveau schaffen und § 31 BDSG würde etwaig vorgesehene Interessensabwägungen im Rahmen der DSGVO gesetzlich vorwegnehmen.[1122]

Einen anderen Ansatz bietet *Maamar*, der verdeutlicht, dass der Anknüpfungspunkt von § 31 BDSG im Vergleich zu § 28b BDSG a.F. ein anderer ist: § 31 BDSG stelle keine Legitimationsgrundlage zur Verarbeitung der Daten zu einem Score dar, sondern knüpfe an die folgende Verwendung des Scores zur Entscheidungsfindung an, wie sich bereits aus dem Wortlaut der Norm „Verwendung eines Wahrscheinlichkeitswerts" ergebe. Zudem verdeutliche auch § 31 Abs. 1 Nr. 3 BDSG, der von den Daten, die zur Berechnung „genutzt" wurden, spricht, dass die Berechnung des Scores bereits abgeschlossen sei, wenn der Anwendungsbereich der Vorschrift eröffnet wird.[1123] Da § 31 BDSG selbst nicht die Zulässigkeit der Score-Ermittlung regle, sei sie dementsprechend auch nicht unionsrechtswidrig.[1124]

Dies überzeugt allerdings nicht, da der Score ebenfalls ein personenbezogenes Datum darstellt[1125] und nach der Definition des Begriffs „Verarbeitung" in Art. 4 Nr. 2 DSGVO auch die Verwendung erfasst ist; mithin regelt § 31 BDSG eine datenschutzrechtliche Frage, für die es in der DSGVO keine Öffnungsklausel gibt.

§ 31 Abs. 1 BDSG ist unionsrechtswidrig und daher unanwendbar. Es ist im Folgenden dennoch die Frage nach den Voraussetzungen und Rechtsfolgen des § 31 BDSG aufzuwerfen, um zu überprüfen, ob die durch § 31 BDSG zusätzlichen Erfordernisse bereits in den allgemeinen Regelungen der DSGVO enthalten sind und – falls nicht – es zweckmäßig wäre, eine vergleichbare Regelung für Scoring im Bereich der (Advanced) People Analytics in einer eventuellen Betriebsvereinbarung vorzusehen.

1121 So z.B. *Kühling*, NJW 2017, 1985 (1988), der eine unionsrechtskonforme Auslegung mangels Öffnungsklausel vornehmen will; ähnlich *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 110, aber ohne klarem Ergebnis.

1122 *Abel*, ZD 2018, 103 (105).

1123 *Maamar*, CR 2018, 820 (825 f.).

1124 So wohl *Maamar*, CR 2018, 820 (828), indem er darauf abstellt, das die Vorschrift andernfalls unionsrechtswidrig sei.

1125 *Helfrich*, Teil IX. Kapitel 3, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Rn. 7.

(2) Regelungsgehalt des § 31 Abs. 1 BDSG

Nach § 31 BDSG muss die Verwendung des Wahrscheinlichkeitswerts über das zukünftige Verhalten einer Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dieser Person erfolgen, wobei nicht vorausgesetzt wird, dass es sich hierbei um eine automatisierte Einzelfallentscheidung im Sinne des Art. 22 DSGVO handelt. Die Bildung von Wahrscheinlichkeitswerten für Marketing-Maßnahmen (beispielsweise für gezielte Werbung oder zur Marktsegmentierung) unterliegt daher mangels Vertragsbezug nicht dem § 31 Abs. 1 BDSG.[1126] Auch bloße statistische Korrelationen sind nicht als Wahrscheinlichkeitswert zu verstehen, da solche Korrelationen, insbesondere mangels Ursache-Wirkungs-Beziehung keine Aussagekraft haben.[1127]

Zu beachten ist, dass der Gesetzgeber zwar nur das Kredit-Scoring bei der Schaffung der Vorschrift im Blick hatte, dem Wortlaut nach aber eine solche materielle Beschränkung für Abs. 1 nicht gilt, sodass auch andere Wahrscheinlichkeitswerte, die im Rahmen von Vertragsverhältnissen zur Anwendung kommen, erfasst werden.[1128] So ist § 31 Abs. 1 BDSG demnach anwendbar auf (Vor-)Auswahlentscheidungen im Bereich der Mitarbeitergewinnung.[1129] Nicht hingegen wird eine reine Potentialanalyse im Rahmen des Beschäftigungsverhältnisses erfasst, wenn diese nicht Grundlage einer Entscheidung wird oder werden soll.[1130]

Da sich der Wortlaut auf die „Verwendung des Wahrscheinlichkeitswerts“ beschränkt, finden die Voraussetzungen des § 31 Abs. 1 BDSG nicht bereits auf die Erhebung und Berechnung des Wertes Anwendung, sondern lediglich auf die Nutzung für die genannten Zwecke; für diese

1126 *Ehmann*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Anh. 2 zu Art. 6 DSGVO Rn. 31.

1127 *Ehmann*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Anh. 2 zu Art. 6 DSGVO Rn. 31.

1128 *Helfrich*, Teil IX. Kapitel 3, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Rn. 27, wo als Beispiele "Matchingwerte" im Rahmen von Partnervermittlungen oder Wahrscheinlichkeiten eines bestimmten Produkterwerbs durch einen bestimmten Kunden genannt werden; letzteres Beispiel ist jedoch im Hinblick auf den Vertragsbezug zweifelhaft.

1129 Plath/*Kamlah*, § 31 BDSG Rn. 18; *Klar*, BB 2019, 2243 (2251); a.A. *Kainer/Weber*, BB 2017, 2740 (2747).

1130 Plath/*Kamlah*, § 31 BDSG Rn. 20.

müssen die Daten den weiteren Voraussetzungen des § 31 Abs. 1 Nrn. 2 - 4 BDSG genügen.[1131]

So müssen nach § 31 Abs. 1 Nr. 2 BDSG die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sein.[1132] Diesbezüglich ist der Wortlaut deckungsgleich mit § 28b Nr. 1 BDSG a.F. Der Gesetzgeber zielte darauf ab, den materiellen Schutzstandard der Vorgängerregelung beizubehalten.[1133]

Die Voraussetzung, dass die Daten nachweisbar erheblich sein müssen, ergibt sich bereits aus dem in Art. 5 Abs. 1 lit. c DSGVO normierten Grundsatz der Datenminimierung. Da Ziel der Vorschrift ist, einen möglichst genauen Wahrscheinlichkeitswert zu erreichen, ist der Begriff der Erheblichkeit in einem statistisch-fachlichen Sinn zu verstehen, sodass alle Daten erheblich sind, die das Rechenergebnis beeinflussen.[1134] § 31 Abs. 1 Nr. 2 BDSG stellt somit keine zusätzlichen Erfordernisse in Bezug auf die Erheblichkeit der Daten auf.

Darüber hinaus ist die Vorschrift methodenneutral, da kein bestimmtes mathematisch-statistisches Verfahren vorgeschrieben wird. Es muss allerdings wissenschaftlich anerkannt sein.[1135] Nicht erforderlich ist, dass das Verfahren durch Prüfsiegel oder Zertifikate nachgewiesen wird, es muss aber Gegenstand wissenschaftlicher Untersuchungen gewesen sein und allgemein als zutreffende Bewertung der Wahrscheinlichkeitswerte für zukünftiges Verhalten eingestuft werden.[1136] Dies ist jedoch keine allzu hohe Anforderung: Rechtswidrig sind nur solche Verfahren, die auf reinem Zufall, auf nicht rationalisierbaren Intuitionen des Scorers oder fehlerhaften statistischen Verfahren beruhen. Somit wird keine bestimmte

1131 So auch *Helfrich*, Teil IX. Kapitel 3, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Rn. 79.

1132 *Ehmann*, in: Simitis, Bundesdatenschutzgesetz, § 28b BDSG Rn. 24, 27.

1133 BT-Drs. 18/11325, S. 101.

1134 *Ehmann*, in: Simitis, Bundesdatenschutzgesetz, § 28b BDSG Rn. 34 ff.; *Ehmann*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Anh. 2 zu Art. 6 DSGVO Rn. 46.

1135 Zur Kritik hierzu siehe ausführlich *Ehmann*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Anh. 2 zu Art. 6 DSGVO Rn. 39 ff.

1136 *Lapp*, in: Gola/Heckmann, BDSG, § 31 BDSG Rn. 29; in Bezug auf die Wissenschaftlichkeit des Verfahrens ebenso *Ehmann*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Anh. 2 zu Art. 6 DSGVO Rn. 42; *Klar*, BB 2019, 2243 (2251): Ein Algorithmus muss zumindest ursprünglich auf hinreichenden fachlichen bzw. wissenschaftlichen Standards beruhen.

Ergebnisgüte vorgeschrieben, ebenso wenig müssen die Verfahren auf dem „Stand der Technik" sein, wie manch andere Vorschrift das fordert.[1137] Es wird also nur eine gewisse „Basisrationalität" des Verfahrens gefordert,[1138] indem das Gesetz ein wissenschaftliches Verfahren verlangt, aber hierzu keine weiteren Vorgaben trifft, außer dass die Daten nachweislich für die Berechnung erheblich sein müssen, also in die Formel miteinfließen. An die Ergebnisgüte selbst werden keine Anforderungen gestellt. Diese Voraussetzung dürfte für zu generierende Scores in der Praxis nur von geringer Bedeutung sein, da Arbeitgeber ohnehin ein hohes Eigeninteresse haben, aussagekräftige Algorithmen zu verwenden, die eine hohe „Trefferquote" bzw. Genauigkeit besitzen.[1139]

Letztlich muss das Verfahren auch der Prognose zukünftigen Verhaltens dienen; insofern findet sich hier eine Einschränkung zum allgemeinen Profiling gem. Art. 4 Nr. 4 DSGVO für welches es ausreicht, dass bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, bewertet werden. Aufgrund der geforderten Prospektivität wird teilweise vertreten, dass § 31 BDSG keine Anwendung auf Auswahlentscheidungen im Arbeitsverhältnis finde, da hier in der Vergangenheit erworbene Kenntnisse und Fähigkeiten evaluiert werden sollen und weniger das zukünftige Verhalten.[1140] Dies überzeugt allerdings nicht, da Arbeitgeber gerade in Auswahlverfahren zwar ausschließlich auf Basis retrospektiver Daten entscheiden können, diese aber inhaltlich ausschließlich zukunftsgerichtet sind.[1141] Etwas anderes könnte allenfalls dann gelten, wenn im Falle von Mitarbeiterbeurteilungen im laufenden Arbeitsverhältnis die Leistung oder das Verhalten des vergangenen Jahres bewertet werden soll (z.B. zur Bemessung des Bonus oder zur (manuellen) Festlegung von Zielen).

Insofern würde § 31 Abs. 1 BDSG auf die untersuchten People Analytics-Verfahren Anwendung finden, ließe man die Europarechtswidrigkeit außer Betracht.

1137 *Gerberding/Wagner*, ZRP 2019, 116 (118), die sich insgesamt kritisch zur gesetzlich geforderten Qualität der Algorithmen äußern.

1138 *Gerberding/Wagner*, ZRP 2019, 116 (119).

1139 So auch *Schürmann*, Auswertung von Mitarbeiterdaten - (Any)/(No)thing possible?, in: Taeger, Smart world - smart law?, S. 513.

1140 *Sommer*, CuA 2014, 4; Plath/*Kamlah*, § 31 BDSG Rn. 26.

1141 So auch *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, S. 255.

(3) Vergleich mit den Vorgaben der DSGVO

Bereits aus dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) in Verbindung mit der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) ergibt sich, dass nur solche Daten für Scoring-Verfahren genutzt werden dürfen, die nachweisbar für das Ergebnis erheblich sind. Eine Regelung zur Wissenschaftlichkeit der genutzten Verfahren besteht nicht. Diese Anforderung könnte sich aus dem Grundsatz der Transparenz nach Art. 5 Abs. 1 lit. a DSGVO in Verbindung mit dem Grundsatz der Richtigkeit (Art. 5 Abs. 1 lit. d DSGVO) ergeben.

Der nicht-normative Teil der DSGVO enthält in Erwägungsgrund 71 S. 6 eine dem § 31 Abs. 1 Nr. 2 BDSG vergleichbare Regelung: So soll der Verantwortliche, um der betroffenen Person eine faire und transparente Verarbeitung zu gewährleisten, *geeignete mathematische oder statistische Verfahren für das Profiling verwenden* sowie technische und organisatorische Maßnahmen treffen, mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen Ergebnissen führen, korrigiert werden und das Risiko von Fehlern minimiert wird.

Der Grundsatz der Transparenz erfordert, dass es dem Betroffenen möglich sein muss, die Datenverarbeitung Schritt für Schritt nachvollziehen zu können; dies betrifft sowohl den Prozess der Verarbeitung selbst als auch den Zusammenhang zwischen den verschiedenen Elementen der Datenverarbeitung (was, wann, warum und wofür).[1142] Ausfluss des Prinzips sind die Rechte der Betroffenen auf Auskunft, Berichtung und Löschung (Art. 12 ff. DSGVO).[1143] So bestimmt beispielsweise Art. 13 Abs. 2 lit. f DSGVO, dass *zumindest* in Fällen der automatisierten Entscheidungsfindung einschließlich Profiling aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung im Rahmen einer Auskunft zur Verfügung werden müssen.

Unklar ist die Reichweite der Informationspflicht in Bezug auf den Inhalt. Aus dem Zusatz „zumindest" ist davon auszugehen, dass die Pflicht nur in den Fällen des Art. 22 DSGVO besteht, in anderen Fällen jedoch freiwillig möglich ist.[1144]

Eine inhaltliche „Basisrationalität" des Verfahrens wird jedoch vom Grundsatz der Transparenz nicht umfasst, sondern allenfalls die Transpa-

1142 Paal/Pauly/*Frenzel*, Art. 5 DSGVO Rn. 21.
1143 EuArbRK/*Franzen*, Art. 5 DSGVO Rn. 4.
1144 So BeckOK DatenSR/*Schmidt-Wudy*, Art. 15 DSGVO Rn. 77.

renz in Bezug auf die verwendeten Verfahren, die nicht notwendigerweise zu einem zumindest im Ansatz treffenden Ergebnis führen müssen. Selbst eine inhaltliche Transparenz in Bezug auf die konkret verwendeten Formeln dürfte in Anbetracht der BGH-Rechtsprechung zur Score-Formel der SCHUFA[1145] sehr geringen Anforderungen unterliegen. Diese ist zwar noch zum alten BDSG ergangen, wird aber von einem Teil der Literatur aus Gründen des Geschäftsgeheimnisschutzes weiterhin für anwendbar erachtet.[1146] Zwar hat der europäische Gerichtshof die abschließende Auslegungskompetenz für Normen der DSGVO, inhaltlich dürfte aber zumindest die Rechtsprechung weiter Geltung beanspruchen, da auf Seiten des Verantwortlichen ein gewichtiges Interesse besteht, die genaue Formel geheim zu halten und zu schützen und dieses Interesse auch im Wege von Auskunftsbegehren zu berücksichtigen ist, wie Erwägungsgrund 63 S. 5 verdeutlicht. Zudem wäre dem Betroffenen mit der Mitteilung des genauen Algorithmus aufgrund der hohen Komplexität nur wenig geholfen.

Aus dem Grundsatz der Richtigkeit könnte sich jedoch die Notwendigkeit eines wissenschaftlich-anerkannten Verfahrens ergeben. Diesem Grundsatz wird zwar – leider – datenschutzrechtlich eher geringe Aufmerksamkeit geschenkt,[1147] hat jedoch mit der DSGVO aufgrund der Bewehrung mit Bußgeld eine andere Qualität gewonnen.[1148] Dieser Grundsatz erfordert nicht nur die Richtigkeit der zugrundeliegenden Daten, sondern auch der Prognosen und Korrelationen.[1149] Schwierig ist es jedoch festzulegen, ab wann ein Verfahren und dessen Ergebnisse als „richtig" zu beurteilen sind. Hier hilft die englische Sprachfassung der DSGVO weiter, die nicht von „correct", sondern von „*accurate*" spricht und somit vielschichtiger ist; gemeint ist daher die Zielgerichtetheit, Genauigkeit und Exaktheit des Verfahrens im Sinne der Mathematik.[1150] Gleiches lässt

1145 BGH, Urt. v. 28.01.2014 – VI ZR 156/13, ZD 2014, 306.

1146 *Klar*, BB 2019, 2243 (2251); *von Lewinski/Pohl*, ZD 2018, 17 (23); kritisch BeckOK DatenSR/*Schmidt-Wudy*, Art. 15 DSGVO Rn. 78.3.

1147 Ausführlich zur Anforderung der Datenqualität im Datenschutzrecht, *Hoeren*, ZD 2016, 459.

1148 Auch wenn dieser Grundsatz nach Maßgabe des Art. 103 Abs. 2 GG inhaltlich zu unbestimmt sein dürfte, um Strafen oder Bußgelder unter Maßgabe zu verhängen, vgl. *Hoeren*, ZD 2016, 459 (461 f.).

1149 BeckOK DatenSR/*Schantz*, Art. 5 DSGVO Rn. 27; unklar *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 5 DSGVO Rn. 140: nur auf Tatsachenangaben anwendbar; Werturteile können nicht richtig oder falsch sein; ebenso *Herbst*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 5 DSGVO Rn. 60.

1150 *Hoeren*, ZD 2016, 459 (462).

sich aus der spanischen („*exactos*“) und französischen Fassung („*exactes*“) herleiten, die von „exakt“ und nicht „korrekt“ oder „richtig“ sprechen.[1151]

Hieraus ergibt sich, dass das Verfahren zumindest – analog den Anforderungen des § 31 Abs. 1 Nr. 2 BDSG – eine gewisse „Basisrationalität“ besitzen muss, um zielgerichtet und genau im Sinne der (sachlichen) Richtigkeit gem. Art. 5 Abs. 1 lit. d DSGVO zu sein. Insofern stellt das nationale Datenschutzrecht an das Scoring im Rahmen von People Analytics keine höheren Anforderungen als die DSGVO. § 31 Abs. 1 BDSG führt letztlich „nur“ zu einer Beweislastumkehr betreffend die Anwendung geeigneter mathematischer und statistischer Verfahren,[1152] nicht aber zu einer Änderung inhaltlicher Vorgaben.

(4) Zwischenergebnis

Obwohl § 31 BDSG aufgrund der Unionsrechtswidrigkeit und des zweifelhaften Anwendungsbereiches außerhalb des Kreditscorings nicht unmittelbar auf People Analytics-Verfahren anwendbar ist, sind die inhaltlichen Vorgaben des § 31 Abs. 1 Nr. 2 BDSG der Sache nach auch nach dem Unionsrecht zu beachten. Diese Anforderungen ergeben sich unmittelbar aus den Datenschutzgrundsätzen der Datenminimierung und Richtigkeit, sind jedoch im nationalen Recht genauer umschrieben. Ohnehin werden Arbeitgeber ein Interesse daran haben, bei den eingesetzten Verfahren korrekte Ergebnisse zu erzielen.[1153] Dieselbe Verpflichtung dürfte sich auch aus den arbeitsvertraglichen Pflichten in Verbindung mit dem Grundsatz aus Treu und Glauben (§ 242 BGB) ergeben. Letztendlich müssen Arbeitgeber darauf achten, nur solche Verfahren einzusetzen, die zumindest im Ansatz nachweisbar zum gewünschten Ergebnis führen und dabei nur solche Daten in den Algorithmus einfließen zu lassen, die für die Berechnung und das Ergebnis von Relevanz sind. Es versteht sich von selbst, dass diskriminierende oder willkürliche Algorithmen bereits aufgrund § 7 AGG bzw. des arbeitsrechtlichen Gleichbehandlungsgrundsatzes nicht eingesetzt werden dürfen und daher darauf geachtet werden muss, dass es auch nicht

1151 Anders aber beispielsweise wieder die polnische Fassung, die von „*prawidłowe*“ spricht, das übersetzt wiederum „korrekt“ bedeutet.

1152 Hierzu *Hoeren/Niehoff*, RW 2018, 47 (63).

1153 So auch *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, S. 256.

zu versteckten Diskriminierungen kommt und der Algorithmus plausible Ergebnisse erzeugt.[1154]

cc) Einsatz künstlicher Intelligenz möglich?

Eine Frage, die sich in diesem Zusammenhang stellt, ist, ob der Einsatz künstlicher Intelligenz für Scoringmaßnahmen möglich ist. Hiergegen könnte, wie bereits oben unter **C. § 3 II** dargestellt, die mangelnde Nachvollziehbarkeit der Entscheidungen unter dem Aspekt der Transparenz der Datenverarbeitung sprechen.

Durch den Einsatz von neuronalen Netzen stellt die involvierte Logik für den Menschen eine Art „Black Box" dar, die nur schwer bis gar nicht nachvollziehen lässt, weshalb ein solches System zu einer bestimmten Entscheidung kommt bzw. warum welche Kriterien welche Gewichtung erhalten sind.[1155]

Gefordert wird von der DSGVO für Scoring-Verfahren allerdings nur eine gewisse „Basisrationalität" sowie eine Zielgerichtetheit und Genauigkeit des mathematischen Verfahrens, keine vollständige Transparenz aller einzelnen Schritte. Dies wird außerhalb des Kontextes von automatisierten Einzelfallentscheidungen auch durch die beschränkten Informationspflichten nach Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO bestätigt, die dort gerade *keine* Informationspflicht über die involvierte Logik statuieren. So müssen die anwandte Formel und letztendlich ausschlaggebenden Kriterien und deren Gewichtung dem Betroffenen auch nicht mitgeteilt werden. Obwohl die deutsche SCHUFA-Rechtsprechung nicht einfach auf die europäische Ebene übertragen werden kann (teilweise – jedenfalls im Rahmen von § 31 BDSG – weiterhin für anwendbar erklärt wird[1156]), dürfte, die Abwägung auf der europäischen Ebene identisch sein.[1157]

1154 Siehe auch Erwägungsgrund 71 S. 6 a.E. DSGVO.

1155 Zur Funktionsweise von Künstlicher Intelligenz bereits oben, **C. § 2 II. 2.** Erste Ansätze für erklärbare KI-Systeme sind bereits vorhanden, hierzu *Körner*, 2.4 Nachvollziehbarkeit von KI-basierten Entscheidungen, in: Kaulartz/Ammann/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, Rn. 24.

1156 *Klar*, BB 2019, 2243 (2251); *von Lewinski/Pohl*, ZD 2018, 17 (23); a.A. wohl BeckOK DatenSR/*Schmidt-Wudy*, Art. 15 DSGVO Rn. 78.3.

1157 Siehe oben **E. § 1 III. 2. c) bb) (3)**.

Zu beachten ist, dass Verfahren der künstlichen Intelligenz nicht auf personenbezogene Daten angewandt werden, sondern auf anonymisierte Trainingssätze, aus denen Korrelationen erkannt werden sollen.[1158] Für letztere gilt ohnehin kein Datenschutzrecht (mehr). Die Frage ist hier lediglich, ob die Ergebnisse und Gewichtungen, die durch ein Training des Systems mit *Machine Learning* und KI entstanden sind, für Scoring für Personalentscheidungen verwendet werden dürfen.

Dies ist grundsätzlich zu bejahen, weil die personenbezogenen Daten mit Hilfe der durch KI errechneten Kriterien klar und nachvollziehbar gewichtet werden, letztendlich also nur noch die Ergebnisse des KI-Prozesses angewandt werden.

Beispiel: Für die Vorhersage der Zuverlässigkeit eines Bewerbers wurde bisher als maßgeblicher Faktor die Durchschnittsnote aus bisherigen Arbeitszeugnissen herangezogen (Gewichtung von allen Kriterien 0,6). Durch den Einsatz eines KI-Systems, das auf anonymisierter Basis die Daten aller vorhandenen Arbeitnehmer ausgewertet hat, wurde festgestellt, dass die Note aus dem Arbeitszeugnis gar keine so große Vorhersagekraft für die zukünftige Zuverlässigkeit hat. Festgestellt und berechnet wurde ein Faktor von 0,443. Dieser Faktor wird nun auf zukünftige Bewerbungen angewandt.

Bei der Anwendung der Ergebnisse handelt es sich vielmals um einen simplen Rechenvorgang (wie im obigen Beispiel die Multiplikation des Faktors mit der Durchschnittsnote), der auch nachvollziehbar ist. Weshalb das System diese Gewichtung als korrekt ermittelt hat, muss im Rahmen von Rechenschaft und Transparenz nicht genau feststehen. Ausreichend ist eine „Basisrationalität". Auch bei menschlichen Entscheidungen kann die Entscheidung nicht mit 100 %iger Genauigkeit an bestimmten Faktoren festgemacht werden; insofern darf hier von einer Maschine auch nicht mehr gefordert werden als von einem Menschen. Das Scoring mit KI bietet im Vergleich zur menschlichen Entscheidung sogar ein „Mehr" an Transparenz, weil es die Entscheidung an bestimmten Faktoren und Gewichtungen klar festmachen kann, auch wenn dies dem Betroffenen nicht offengelegt werden muss.

1158 Kritisch hierzu *Götz*, Big Data im Personalmanagement, S. 152 f. mit rein folgenbezogenen Erwägungen.

dd) Legitimation des Profilings im Rahmen von Advanced People Analytics

Als neuer Verarbeitungsvorgang muss das Profiling bzw. Scoring ebenfalls unter eine Legitimationsgrundlage subsumiert werden können. Hier kommen drei praxisrelevante Legitimationsgrundlagen in Betracht: (1) Einwilligung durch den Arbeitnehmer, (2) Erforderlichkeit nach § 26 Abs. 1 BDSG bzw. Art. 6 Abs. 1 lit. f DSGVO und (3) Legitimation durch eine Betriebsvereinbarung. Diese sollen im Folgenden untersucht werden.

(1) Legitimation des Profilings durch eine Einwilligung des Arbeitnehmers

Während die Einwilligung für Profiling im Rahmen von Online-Diensten[1159] die gängige Legitimationsform der Datenverarbeitung ist, sind die Anforderungen an eine wirksame Einwilligung im Arbeitsverhältnis faktisch deutlich höher, da das bestehende Abhängigkeitsverhältnis zwischen Arbeitnehmer und Arbeitgeber besondere Berücksichtigung findet.[1160] Anders als bei der Einwilligung im Rahmen von Simple People Analytics[1161] ist die Eingriffsintensität durch die erfolgende Bewertung von Persönlichkeitsaspekten deutlich höher. Zudem kann die Transparenz geringer ausfallen, wenn beispielsweise die konkrete Formel und Gewichtung der einzelnen maßgeblichen Faktoren nicht mitgeteilt wird.

Einwilligungen in solche Verfahren sind daher unter dem Aspekt der Rechtssicherheit als höchst kritisch zu betrachten, zumal Arbeitnehmer Ihre Einwilligung jederzeit widerrufen können (Art. 7 Abs. 3 DSGVO, § 26 Abs. 2 S. 4 BDSG) und somit für zukünftige Auswertungen die personenbezogenen Daten des betroffenen Arbeitnehmers nicht mehr genutzt werden dürfen. Dies stellt mitunter einen enormen administrativen Aufwand dar, wenn Daten in eine Vielzahl von Auswertungsvorgängen einfließen bzw. eingeflossen sind (bei retrospektiver Betrachtung). Zwar gilt der Widerruf nur für die Zukunft und berührt daher die bisher auf der Einwilli-

1159 Bspw. bei Facebook, Instagram, WhatsApp oder sonstigen Netzwerken, auch wenn diese mitunter in den seitenlangen Datenschutzerklärungen von den Benutzern nicht wirklich wahrgenommen werden.

1160 Zu den Anforderungen an eine wirksame Einwilligung siehe bereits **D. § 1 III. 2. a**).

1161 Hierzu **E. § 1 III. 1. a**).

gung durchgeführten Datenverarbeitungsvorgänge nicht (Art. 7 Abs. 3 S. 2 DSGVO), dennoch dürfen die durchgeführten Auswertungen, sofern diese nicht anonymisiert sind und somit nicht mehr dem Datenschutzrecht unterliegen, zukünftig nicht mehr für weitere Verarbeitungsvorgänge genutzt werden, da hierfür keine Legitimationsgrundlage mehr besteht.[1162]

Ob eine Einwilligung zulässig ist, ist jeweils im Einzelfall zu entscheiden; sie sollte jedoch auch für solche Verfahren nur als allerletzte Option in Betracht gezogen werden (siehe aber **E. § 1 III. 2. c) dd) (2) (c)**).

(2) Erforderlichkeit nach § 26 Abs. 1 BDSG

Eine weitere Legitimationsgrundlage könnte die Erlaubnisnorm für Datenverarbeitungen im Arbeitsverhältnis, § 26 Abs. 1 S. 1 BDSG, darstellen, wenn personenbezogene Daten eines Arbeitnehmers für Profiling und Scoring genutzt werden sollen. Zu beachten ist, dass für die weitere Beurteilung davon ausgegangen werden muss, dass die Daten bereits rechtmäßig erhoben wurden (hierzu siehe bereits **E. § 1 III. 2. a) cc)**). Eine Zweckkompatibilitätsprüfung muss in diesem Fall nicht mehr stattfinden, da für APA-Profiling erforderlich ist, dass die Daten für den Zweck der Durchführung des Beschäftigungsverhältnisses erhoben wurden und eine zweckkompatible Verarbeitung anderweitig erhobener Daten (z.B. Sensor-/Systemdaten) ausscheidet.[1163]

Für die im Rahmen von § 26 Abs. 1 S. 1 BDSG vorzunehmende Abwägung kommt es daher ausschließlich auf den Vorgang des Profilings oder Scorings unter Zugrundelegung der erhobenen personenbezogenen Daten an. Es muss also mit anderen Worten geprüft werden, ob die erhobenen personenbezogenen Daten nicht nur zum Zwecke der Durchführung des Beschäftigungsverhältnisses (ggf. zweckändernd), sondern auch zum Zwecke der Erstellung eines Persönlichkeitsprofils genutzt werden dürfen.

Anders als bei Simple People Analytics handelt es sich nicht mehr um eine reine Fortschreibung bereits vorliegender Daten mit einfachen mathematischen Verfahren, sondern um die inhaltliche Bewertung von

---

1162 So wohl auch EuArbRK/*Franzen*, Art. 7 DSGVO Rn. 6 m.w.N.: Ein in der Vergangenheit erstellter Werbefilm, in welchem der Arbeitnehmer kurz im Rahmen eines Gruppenbildes gezeigt wird, darf entgegen bisheriger Rechtsprechung (BAG, Urt. v. 11.12.2014 – 8 AZR 1010/13, NZA 2015, 604) zum BDSG a.F. wohl nicht mehr weiterverwendet werden.

1163 Siehe ausführlich **E. § 1 III. 2. b) (3)**.

Persönlichkeitsmerkmalen wie beispielsweise Verhalten und Leistung und somit die Generierung von grundsätzlich neuen[1164] personenbezogenen Daten mit hoher Persönlichkeitsrelevanz. Die Anforderungen an einen solchen Verarbeitungsvorgang müssen daher deutlich höher gesetzt werden als bei der simplen Fortschreibung bestehender Werte durch einfache statistische Methoden. Zudem können sich solche Aussagen und Prognosen als individuell falsch, ungerecht bzw. willkürlich oder diskriminierend erweisen, sodass die Persönlichkeitsrechte erheblich beeinträchtigt werden können.[1165]

Maßgeblich ist vor allem die Eingriffsintensität beim Betroffenen.[1166] Durch die Profilbildung können Risiken des Kontextverlustes sowie der Unrichtigkeit entstehen, wenn aus dem Vorliegen bestimmter Eigenschaften auf das Vorhandensein anderer Eigenschaften geschlossen wird. Diese Gefahr besteht insbesondere, wenn die zugrundeliegenden Daten nicht mehr aktuell sind oder falsch erfasst wurden. Zudem können einzelne spezifische Datensätze sehr einfach zu einem Gesamtprofil zusammengefasst werden, was zu persönlichem Überwachungsdruck führen könnte,[1167] weil hierdurch mitunter neue Daten generiert werden, die aussagekräftigte Vorhersagen zum Verhalten der betroffenen Person treffen können. Hierdurch entsteht eine enorme Eingriffsintensität. Bereits das Erstellen eines Teilabbilds der Persönlichkeit gegen den Willen des Betroffenen ist daher, wie das Bundesverfassungsgericht in der *Volkszählungs*-Entscheidung herausgearbeitet hat, in der Regel verfassungswidrig.[1168] Werden aber auf Basis einer Einwilligung, z.B. im Rahmen des Online-Marketings oder bei sozialen Netzwerken Persönlichkeitsprofile erstellt, so sind diese nicht *per* se als verfassungswidrig zu bezeichnen.[1169] Die Abgabe der Einwilligung auch die Eingriffsintensität, zumal nicht ein staatlicher Akteur auf der anderen Seite handelt, sondern ein privater Konzern. Etwas anderes kann etwa gelten, wenn der Konzern weltweit tätig ist und aufgrund Gesetze

1164 So auch *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 4 DSGVO Rn. 6.
1165 *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 4 DSGVO Rn. 9.
1166 *Brecht/Steinbrück/Wagner*, PinG 2018, 10 (11 f.).
1167 *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 117.
1168 BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1 (53 f.) – Volkszählungsurteil Tz. 178.
1169 *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 118 m.w.N.

in anderen Ländern dem Staat einen Zugriff auf die Daten gewähren muss.[1170]

Zur Feststellung der Eingriffsintensität ist zu unterscheiden, ob ein Überwachungsdruck für eine Gruppe von Arbeitnehmern oder für einen einzelnen Arbeitnehmer entsteht. Bei ersterem kommt es im Weiteren maßgeblich darauf an, ob sich eine Identifizierbarkeit im Nachhinein ergeben kann.[1171] Ist dies nicht der Fall, liegen keine personenbezogenen Daten und somit auch kein Eingriff in das Persönlichkeitsrecht vor; das Datenschutzrecht ist nicht anwendbar. Anonymes Profiling und Scoring von Gruppen sind somit datenschutz- und verfassungsrechtlich möglich.

Steht – wie hier beim personenbezogenen Profiling – allerdings der einzelne Arbeitnehmer im Fokus, so müssen die unternehmerischen Interessen (Art. 12, 14 GG im Lichte der Art. 16 f. EU-GRC) mit dem Recht auf Privatheit des Arbeitnehmers (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG im Lichte der Art. 7 f. EU-GRC) abgewogen und in praktische Konkordanz gebracht werden,[1172] wobei die Rahmenbedingungen ebenfalls von besonderer Bedeutung sind. Insbesondere der erzeugte Überwachungsdruck bei Bewertung und Prognose des Verhaltens und der Arbeitsleistung kann einem Profiling bzw. Scoring entgegenstehen.[1173]

(a) Scoring von Bewerbern

Hohe Relevanz hat diese Diskussion im Bereich des Bewerber-Managements, insbesondere bei begehrten Stellen, wo sich viele Menschen bewerben und eine Flut an Bewerbungen eingeht. In diesen Fällen ist es für die Personalverantwortlichen kaum möglich, diese Bewerbungen alle einzeln zu sichten, sodass gewisse Vorauswahlen bzw. Einstufungen getroffen werden müssen. Eine sehr effektive Methode kann das Profiling / Scoring der Bewerber anhand der in einer Online-Maske eingetragenen oder einem CV-Parser ausgelesenen Daten sein. Das Personalmanagement gibt die Anforderungen für die Stelle an die gewünschte Person in eine Maske im

1170 Vgl. hierzu das aktuelle Urteil des EuGH zum „Privacy Shield", EuGH, Urt. v. 16.07.2020 – C-311/18, ECLI:EU:C:2020:559 – Schrems II.

1171 *Brecht/Steinbrück/Wagner*, PinG 2018, 10 (11 f.).

1172 *Brecht/Steinbrück/Wagner*, PinG 2018, 10 (12), die allerdings nur die nationalen Grundrechte in den Fokus stellen.

1173 Siehe hierzu bereits **E. § 1 III. 2. a) cc) (4)**.

System ein und das System ermittelt den Match-Wert in Form eines Scores des einzelnen Bewerbers mit den Anforderungen des Unternehmens.

Selbstverständlich muss in diesem Rahmen darauf geachtet werden, dass nur solche Daten erhoben werden, die vom Fragerecht des Arbeitgebers erfasst sind.[1174] Die zulässigerweise erhobenen Daten durchlaufen im Anschluss einen Auswahlalgorithmus, der die Bewerber nach der Eignung auf die passende Stelle reiht und jeweils mit einer Punkteanzahl oder Note versieht.[1175] Eine automatische Vorauswahl findet an dieser Stelle noch nicht statt (siehe hierzu **D. § 1 V. 3. c) aa)**).

Da eine wirksame Einwilligung in diesem Stadium des (erwünschten oder angebahnten) Beschäftigungsverhältnisses aufgrund mangelnder Freiwilligkeit ausscheidet,[1176] muss die Legimitation über § 26 Abs. 1 S. 1 BDSG erfolgen; die Datenerhebung also zum Zweck der Entscheidung über die Begründung des Beschäftigungsverhältnisses[1177] erforderlich sein. Art. 22 DSGVO, welcher die Zulässigkeit automatisierter Einzelfallentscheidungen regelt, ist bei einem reinen Ranking (noch) nicht anwendbar, sofern ein menschlicher Entscheider die Letztentscheidung auf Basis der Datengrundlage trifft.[1178]

Hierbei sind die berechtigten Interessen des Arbeitgebers an einem Scoring der Bewerber im Rahmen der Entscheidung über die Begründung des Beschäftigungsverhältnisses gegenüber entgegenstehenden Interessen der Bewerber abzuwägen. Die Arbeitgeberinteressen liegen in einer Effektivierung des Bewerbermanagements sowie (was ebenfalls im Interesse der Bewerber ist) an einer möglichst passenden und gerechten Auswahl des besten Bewerbers für die ausgeschriebene Stelle. Auf der Bewerberseite lauten die Interessen grundsätzlich dahingehend, möglichst wenig private Daten offenbaren zu müssen und insbesondere selbst entscheiden zu können, welche Daten der Arbeitgeber für die Bewertung erhält bzw. verarbeitet. Darüber hinaus hat auch der Bewerber ein Interesse daran, eine faire Chance zu bekommen und bei der Auswahl berücksichtigt zu werden.[1179]

1174 Vgl. hierzu die ausführliche Kommentierung von *Seifert*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 88 DSGVO Rn. 75 ff. m.w.N.; zur Problematik des Preisgebens von Daten, um eine bessere Chance zu erhalten, *Däubler*, Gläserne Belegschaften, S. 182 Rn. 250c.

1175 Ein Beispiel hierzu wurde bereits oben bei **C. § 3 I** genannt.

1176 Siehe hierzu bereits **D. § 1 III. 2. a) bb) (2)**; ferner *Kainer/Weber*, BB 2017, 2740 (2742).

1177 Zu dieser Zweckbestimmung siehe **E. § 1 I. 1. b) aa)**.

1178 So bereits *Blum/Kainer*, PERSONALquarterly 2019, 22 (26).

1179 Zum Interessenkonflikt im Arbeitsverhältnis, siehe **A. § 2**.

Größtes Risiko neben Persönlichkeitsdurchleuchtungen dürften in diesem Zusammenhang (versteckte) Diskriminierungen durch Algorithmen sein,[1180] auch wenn Algorithmen mitunter auch mit dem Ziel eingesetzt werden, gerade solche zu verhindern. Grundlage für solche Diskriminierungen können eine fehlerhafte Datenbasis für den Algorithmus oder Modellfehler sein, aber auch diskriminierende Entscheidungen in der Vergangenheit, aus die der Algorithmus „lernt".[1181] Hier muss nicht nur im Diskriminierungskontext darauf geachtet werden, sondern auch im datenschutzrechtlichen, denn auch diese Gefahr stellt eine mögliche negative Folge für den Betroffenen dar, die im Rahmen der Interessensabwägung zu berücksichtigen ist. Wird der Auswahlalgorithmus hingegen nur für bestimmte fachliche Kriterien verwendet und bleiben andere Merkmale außer Betracht (z.B. Auswertung des Fotos auf „Sympathie" oder Einbeziehung des Geschlechts in ein Ranking), so dürfte eine diskriminierende Entscheidung eher fern liegen. Je mehr Daten der Algorithmus jedoch als Grundlage verwendet, die nicht im rein fachlichen Bereich liegen, desto höher wird das Risiko einer unzulässigen Diskriminierung. Arbeitgeber müssen in solchen Fällen Vorkehrungen schaffen, indem die Systeme beispielsweise statistisch auf eine Voreingenommenheit getestet werden oder Quotierungen festgelegt werden (z.B. eine bestimmte Frauenquote in den Top-10-Ergebnissen der Ranking-Vorschläge).[1182]

Die Tendenz im Rahmen von People-Analytics geht allerdings dazu, statt „harten" Kriterien eher weiche Kriterien aus dem Persönlichkeitsbereich der Arbeitnehmer für Auswahlentscheidungen heranzuziehen: So könnte beispielsweise ein Unternehmen solche Softwareentwickler bevorzugt einstellen, die in ihrer Freizeit einem bestimmten Hobby nachgehen, da durch interne Auswertungen mit Hilfe von KI herausgefunden wurde, dass hier eine Korrelation besteht.[1183] Die Grenzen werden durch die (inzwischen) feingliedrige Rechtsprechung zum Fragerecht des Arbeitgebers gesetzt. In keinem Falle darf es zu Totalabbildungen der Persönlichkeit des Bewerbers kommen.

Teilweise wird in diesem Rahmen vertreten, dass allein der Wunsch nach einer besseren Personalplanung nicht von den in § 26 Abs. 1 BDSG

1180 Zu den Diskriminierungsrisiken speziell in Bezug auf das AGG beim Einsatz von Algorithmen im Bewerbungsverfahren, siehe *Dzida/Groh*, NZA 2018, 1917.

1181 *Dzida/Groh*, NZA 2018, 1917; ebenso bereits **C. § 3 III**; ferner *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, S. 81 ff.

1182 Vgl. *Dzida/Groh*, NZA 2018, 1917 (1922).

1183 Beispiel aus *Dzida*, NZA 2017, 541 (542).

genannten Zwecken erfasst ist, insbesondere, wenn als Grundlage (anonymisierte) Daten von Beschäftigten als Vergleichsbasis herangezogen werden.[1184] Diese Auffassung geht von einem zu engen Erforderlichkeitsbegriff aus. § 26 Abs. 1 BDSG setzt die Erforderlichkeit für die „Entscheidung über die Begründung" voraus; welche Daten der Arbeitgeber für die Entscheidung benötigt, liegt zwar nicht vollständig in seinem Ermessen, aber sofern ein berechtigtes Interesse für die Kenntnis besteht und die Interessen des Bewerbers an der Geheimhaltung nicht überwiegen, ist eine Verarbeitung zulässig.[1185]

Das Scoring auf Basis „harter Fakten" und anschließende Ranking von Bewerbern ist – jedenfalls bei einer hohen Anzahl an Bewerbungen auf eine Stelle[1186] – „erforderlich" im Sinne von § 26 Abs. 1 S. 1 BDSG, wenn Arbeitgeber ein entsprechendes System einsetzen. So müssen einerseits Bewerber damit rechnen, dass ihre Daten verarbeitet und in Relation zu den Stellenvoraussetzungen gesetzt, andererseits auch, dass sie inhaltlich bewertet werden. Es ist nahezu selbstverständlich, dass kein Personalverantwortlicher eine sehr hohe Anzahl an Bewerbungen sichten kann, zumal dies auch unwirtschaftlich wäre. Arbeitgeber sind daher bereits jetzt gezwungen, bei Bewerbungsfluten ein effektives Selektionssystem zu etablieren.

So wäre ein Aussortierungssystem, das nach dem Prinzip verfährt, dass jede zweite Bewerbung ungesichtet im Müll landet, weder nach datenschutzrechtlichen noch diskriminierungsrechtlichen Gesichtspunkten unzulässig, auch wenn es in hohem Maße unfair ist und hierdurch möglicherweise der am besten geeignete Bewerber aussortiert wird. Andererseits könnten auch Bewerbungen aussortiert werden, die beispielsweise nicht in einem PDF-Gesamtdokument gesendet wurden, sondern in unzähligen Einzeldokumenten bei einer E-Mail-Bewerbung; auch hierdurch würde man allenfalls solche Bewerber effektiv aussortieren, die keine ausreichenden PC-Kenntnisse besitzen, die Anforderungen der Stellenbeschreibung nicht korrekt lesen (oder eine entsprechende Software nicht besitzen). Zwar vermindert man hiermit ebenfalls den Aufwand in der Personalabteilung, alle Dokumente entsprechend einzeln zu sichten bzw.

1184 Noch zu § 32 BDSG a.F.: *Bissels/Mayer-Michaelis/Schiller*, DB 2016, 3042.

1185 Zum Erhebungszweck „Erforderlichkeit für die Entscheidung über die Begründung" vgl. bereits **E. § 1 I. 1. b) aa)**.

1186 Aufgrund des geringeren Eingriffs in die Rechte der Arbeitnehmer gelten geringere Anforderungen als im Rahmen der automatisierten Einzelfallentscheidung; zum Begriff der Erfordertlichkeit dort vgl. **D. § 1 V. 3. d) aa)**.

auszudrucken, die Effizienz dieses Verfahrens hängt jedoch stark von der ausgeschriebenen Stelle ab. Für eine Sekretariatsstelle könnte dies unter Umständen ein taugliches Kriterium sein, sofern dies in den Anforderungen an die Bewerbung explizit verlangt wurde.

Ein computerbasiertes System, das den Inhalt der Bewerbungen abgleicht und mit dem konkreten Stellenprofil vergleicht, ist jedenfalls effektiver als – teilweise eingesetzte – Verfahren, die dem Zufall unterliegen. Der Bewerber hat ebenfalls ein Interesse daran, keinem Zufallssystem „zum Opfer zu fallen". Ein solches System lässt eine schnelle Erstauswahl der Bewerber treffen, wobei grundsätzlich die Gefahr besteht, dass aufgrund von Eingabefehlern bzw. Auswertungsfehlern falsche Scores generiert werden und geeignete Bewerber im Ranking weit unten landen. Zu beachten ist an dieser Stelle allerdings, dass noch keine automatisierte Einzelfallentscheidung getroffen wird, sondern ein menschlicher Entscheider die „Vorauswahl" des Computers noch inhaltlich auf Basis der Datengrundlage (nicht allein des Scores) nochmals überprüfen und bestätigen muss. Ansonsten läge ein Fall des Art. 22 DSGVO vor.

Generiert die Software im obigen Beispiel also den „Scorewert 0" für solche Bewerber, so müsste der Sachbearbeiter überprüfen, ob mehrere Dateien eingegangen sind oder nur ein Gesamt-PDF vorliegt. In letzterem Fall wäre der erstellte Scorewert falsch und der Sachbearbeiter müsste manuell eine Neubewertung vornehmen.

Werden hingegen „weiche Daten" aus dem Persönlichkeitsbereich gescort, so ist zunächst erforderlich, dass der Arbeitgeber diese Daten rechtmäßig erheben durfte. Das o.g. Beispiel des Vergleichs der Hobbys des Bewerbers mit solchen von Angestellten ist in der Praxis datenschutzrechtlich unzulässig, da ein Hobby ausschließlich dem Privatleben zuzuordnen ist und für die Beschäftigung grundsätzlich[1187] ohne Relevanz.[1188] Eine Einwilligung scheidet mangels Freiwilligkeit aus, ebenso eine Legitimation durch Betriebsvereinbarung, da der Betriebsrat für die Bewerber persönlich nicht zuständig ist[1189] und eine etwaige Betriebsvereinbarung im Übrigen auch nach § 75 Abs. 2 BetrVG aufgrund des unzulässigen Eingriffs in das Persönlichkeitsrecht des Arbeitnehmers rechtswidrig wäre.

1187 Kein Grundsatz ohne Ausnahmen: Wenn ein Hobby eine Verbindung zu der Tätigkeit aufweist, dann kann eine solche Frage zulässig sein, z.B. jemand soll die Öffentlichkeitsarbeit in einem Ruderverein wahrnehmen; die Frage, ob jemand selbst in seiner Freizeit rudert, wäre also legitim.

1188 Vgl. *Kort*, NZA-Beilage 2016, 62 (67).

1189 *Bausewein*, DuD 2016, 139 (140).

Psychologische Eignungstests, z.B. im Rahmen von Assessment-Centern wurden in der höchstrichterlichen Rechtsprechung kaum behandelt,[1190] sind jedoch im Grundsatz zulässig, wenn sie solche Daten über den Bewerber generieren, die auch konkreten Bezug zur Stelle haben (so z.B. Belastbarkeit, Durchsetzungsfähigkeit, wenn ein vorheriger Stelleninhaber an diesen Merkmalen gescheitert ist[1191]),[1192] also für die Entscheidung über die Begründung erforderlich sind. Obwohl oft von den Bewerbern eine Einwilligung eingeholt wird, ist diese mangels Freiwilligkeit in den wenigsten Fällen wirksam.[1193] Man wird wohl davon ausgehen müssen, dass ein bloßes Interesse des Arbeitgebers, einen charakterlich besser passenden Bewerber einzustellen nicht ausreichen mag, wenn der Charakterzug keinen konkreten Bezug zur Arbeit hat, weil der Arbeitnehmer überwiegend nur mit der Bedienung von Maschinen beschäftigt ist und nicht im Team arbeitet.[1194] Je höher der Bewerber in der Hierarchie eingesetzt werden soll und desto mehr Personal- und Unternehmensverantwortung er letztlich hat, desto wichtiger sind seine persönlichen (Führungs-)Eigenschaften, sodass bei einem Manager ein Assessment-Center mit (weitgehenden) Persönlichkeitsanalysen eher in Betracht kommt als bei einem „einfachen Arbeitnehmer" am unteren Ende der Hierarchie.

Da bereits recht hohe Anforderungen an eine Datenerhebung bzgl. „weicher Kriterien" bestehen und dies ohnehin erst bei Bewerbern mit einem hohen Verantwortungsspektrum in Betracht kommt, darf aufgrund des nur geringfügigen weiteren Eingriffs in das Persönlichkeitsrecht im Vergleich zur Ersterhebung auch ein weitergehendes Scoring durchgeführt werden, um die erhobenen Daten entsprechend in einen Vergleich einbeziehen zu können. Ohne eine entsprechende Visualisierung der Ergebnisse der psychologischen Tests besitzen diese wenig Aussagekraft für die Entscheidung über die Begründung des Arbeitsverhältnisses. Es ist daher sogar von einer (zwingenden) Erforderlichkeit des Scorings im Anschluss an die Tests auszugehen, um die gewünschte Entscheidung als Personalverantwortlicher oder Manager (der nicht Psychologe o.ä. ist) treffen zu können.

1190 So auch *Franzen*, NZA 2013, 1 (2).
1191 Beispiel von *Bausewein*, DuD 2016, 139 (142).
1192 *Franzen*, NZA 2013, 1 (2).
1193 *Kort*, NZA-Beilage 2016, 62 (71); unklar *Bausewein*, DuD 2016, 139 (141 f.); siehe bereits **D. § 1 III. 2. a) bb) (2)**.
1194 *Bausewein*, DuD 2016, 139 (143).

Nota bene: Sofern als Daten- und Vergleichsbasis personenbezogene Daten von (erfolgreichen) und bereits angestellten Arbeitnehmern genutzt werden sollen, ist zu beachten, dass die Verarbeitung der personenbezogenen Daten der bereits angestellten Arbeitnehmer nicht mehr von der Ermächtigungsgrundlage § 26 Abs. 1 BDSG erfasst ist; die Zwecke des § 26 Abs. 1 BDSG sind nicht einschlägig, da die Daten weder zur Entscheidung über die Begründung ihres konkreten Anstellungsverhältnisses, noch für die Durchführung genutzt werden, sondern für die Optimierung des Bewerbungsverfahrens für neue potentielle Arbeitnehmer. § 26 Abs. 1 BDSG sperrt allerdings nicht den Rückgriff auf Art. 6 Abs. 1 lit. f DSGVO.[1195] Dem Arbeitgeber ist ein berechtigtes Interesse anzuerkennen, solche Daten – zumindest für die Anonymisierung zum Zwecke der Nutzung im Bewerbungsprozess – zu nutzen.[1196] Alternativ käme auch eine Einwilligung des zu vergleichenden Arbeitnehmers nach Art. 7 DSGVO in Betracht, da dieser als Positivbild zur Bewertungsgrundlage herangezogen werden soll und daher keine Nachteile aus der Datenverarbeitung zu befürchten hat, zumal die Daten auch anonymisiert werden können; Zweifel an der Freiwilligkeit bestehen daher nur in geringem Maße.

(b) Scoring der Arbeitsleistung

Nach erfolgreicher Begründung des Arbeitsverhältnisses haben Arbeitgeber ein weitergehendes Interesse auch die Arbeitsleistung der Beschäftigten zu überwachen, um eventuellen Fehlentwicklungen mit weiteren Maßnahmen gegensteuern zu können. Dem Arbeitgeber ist grundsätzlich ein Recht einzuräumen, zu kontrollieren, ob die Beschäftigten die vertraglich vereinbarte Arbeitsleistung erbringen und somit ihren Pflichten nachkommen.[1197] Hierfür ist der Einsatz technischer Hilfsmittel zulässig.[1198] Allerdings kann das Erstellen von Scores über die Leistung von Arbeitnehmern und das folgende Vergleichen der Scores mit anderen Arbeitnehmern zu einem enormen Leistungs- und Anpassungsdruck führen. So könnten beispielsweise Low-Performer schnell durch solche Maßnahmen

1195 Paal/Pauly/*Gräber/Nolden*, § 26 BDSG Rn. 10 ff.
1196 So wohl auch unter Rückgriff auf § 28 Abs. 1 S. 1 Nr. 2 BDSG a.F., *Dzida*, NZA 2017, 541 (542 f.).
1197 *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 105.
1198 *Däubler*, Gläserne Belegschaften, S. 190 Rn. 260a.

individualisiert und gekündigt werden.[1199] Dies gilt umso mehr, wenn das Scoring-Verfahren dem Arbeitnehmer nicht im Detail bekannt ist[1200] oder individualisierte Daten gar in Dashboards (dazu im Folgenden **E. § 3**) auf Gruppen-/ oder Abteilungsebene (bei Vergleichbarkeit) dargestellt werden und zu einer Mehrleistung motivieren sollen, m.a.W. schwache Mitarbeiter an den Pranger gestellt werden. Jedenfalls ausgeschlossen sind daher in diesem Zusammenhang solche Scores, die darauf beruhen, dass die Primärleistungspflicht lückenlos überwacht wird.[1201]

Etwas anderes kann aber für Profiling-Maßnahmen oder Scores ohne (dauerhafte) Überwachung der Primärleistungspflicht gelten, beispielsweise, wenn unterjährige Mitarbeitergespräche stattfinden und Zielvereinbarungen getroffenen werden und die Daten aus diesen Maßnahmen in das HRM-System eingetragen werden oder lediglich (gezielte) stichprobenartige Kontrollen durchgeführt[1202] werden.

In einem solchen Fall kommt es im Rahmen der Datenerhebung zu keiner (technischen) Überwachung; Zielvereinbarungen und Mitarbeitergespräche sind allgemein üblich und werfen keine spezifisch datenschutzrechtlichen Fragen im Rahmen von People Analytics auf.

Datenschutzrechtliche Relevanz erlangen Zielvereinbarungen und Mitarbeitergespräche im Rahmen der hier untersuchten People Analytics dann, wenn die Daten aus solchen Gesprächen bzw. Beurteilungen genutzt werden sollen, um mit Hilfe intelligenter Algorithmen neue personenbezogene Daten wie beispielsweise einen Score zu generieren, die dann ins Verhältnis zu anderen (vergleichbaren) Arbeitnehmern gesetzt werden können. Anders als bei einem automatischen Scoring durch (technische) Überwachung der Primärleistungspflicht kommt es nicht zu einem vergleichbaren Überwachungs- und Anpassungsdruck, da Grundlage des Scores (für den Beschäftigten) nachvollziehbare Daten aus den genannten Maßnahmen sind. Dennoch kann die Bildung eines Scores (und somit

---

1199 Vgl. zu diesem Problem *Kraus*, DB 2018, 701; für eine Unzulässigkeit einer solchen Aussortiertung durch technische Überwachung *Däubler*, Gläserne Belegschaften, S. 190 Rn. 260a.

1200 Vgl. hierzu bereits die *Belastungsstatistik*-Entscheidung des BAG (Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205), dargestellt und analysiert unter **E. § 1 III. 2. a) cc) (4)**.

1201 BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205 (1211) Rn. 30; etwas anderes gilt, wenn nur bestimmte Daten aus dem Bereich der täglichen Arbeit in Auswertungen einfließen, vgl. BAG, Beschl. v. 30.08.1995 – 1 ABR 4/95, NZA 1996, 218.

1202 *Lunk*, NZA 2009, 457 (461) m.w.N.

Vergleichswertes) dazu führen, dass ein gewisser Druck entsteht, höchstmögliche Score-Zahlen zu erreichen. Der Leistungsdruck besteht allerdings schon aus der Zielvereinbarung selbst, da die dort vereinbarten bzw. vorgegebenen Ziele erreicht werden sollen / müssen. Der Unterschied ist, dass sich der Druck aus dem direkten Vergleich mit anderen Arbeitnehmern durch Generierung spezifischer Punktezahlen durch Scoring erhöhen kann.

Beispiel: Der Arbeitnehmer erreicht die vereinbarten Ziele voll, andere vergleichbare Arbeitnehmer überschreiten diese erheblich. Im Vergleich erreicht ein Arbeitnehmer daher nicht (mehr) 100 %, sondern lediglich 60 %. Zu beachten ist aber, dass in einem gut funktionierenden HR-Management solche Unterschiede auch ohne ein Scoring-Verfahren aufgedeckt und die Zielvereinbarungen entsprechend angepasst werden sollten, mit der Folge, dass eine höhere Leistung erwartet wird und der Leistungsdruck sich daher nicht aus dem Scoring, sondern der Zielvereinbarung selbst ergibt.

Selbst wenn aber durch technische Maßnahmen (Überwachungs-)Daten erhoben werden, beispielsweise in Fällen, in denen aus Gründen der Prozesssteuerung sehr detaillierte Daten erhoben werden müssen, kann es zulässig sein, diese für die konkrete Beurteilung von Mitarbeitern zu aggregieren.[1203] Dies bedeutet, dass der Arbeitgeber für die Leistungsbeurteilung keine konkreten Einblicke in die einzelnen Prozessschritte erhält, sondern beispielsweise am Monatsende eine vergleichende Darstellung der Leistung der einzelnen Mitarbeitern, aggregiert über einen Zeitverlauf. Somit ist es dem Arbeitgeber unmöglich, ein Bewegungsprofil des Arbeitnehmers zu erstellen und ihn konkret zu überwachen. Darstellbar ist ein Gesamtbild der Arbeitsleistung auf Monatsbasis, das mit anderen Arbeitnehmern in den Vergleich gestellt und hieraus entsprechende Scores generiert werden können.

Bei einer entsprechenden Transparenz des Scoring-Verfahrens überwiegen die Arbeitgeber-Interessen an einer Effektivierung des Personalmanagements dem Recht auf Privatheit und informationelle Selbstbestimmung des Beschäftigten, zumal die Eingriffsintensität bei der Verwendung transparenter und mathematisch-korrekter Verfahren im Vergleich zur Mitarbeiterbeurteilung ohne Scoring allenfalls geringfügig höher ist. Letztlich kommt es aber darauf an, wer Zugriff auf diese Daten erhält, um eine endgültige Bewertung der Zulässigkeit vorzunehmen (siehe **E. § 3**). Dem

1203 *Schürmann*, Auswertung von Mitarbeiterdaten - (Any)/(No)thing possible?, in: Taeger, Smart world - smart law?, S. 508.

Grunde nach ist ein Scoring der Primärleistungspflicht folglich möglich, wie auch der Wortlaut des Art. 4 Nr. 4 DSGVO nahe legt.

(c) Scoring des betrieblichen Verhaltens (z.B. Kommunikationsverhalten)

Als weitere denkbare Scoring-Situation ist im Rahmen von Advanced People Analytics die Bewertung von nicht leistungsrelevanten Daten denkbar. Als Beispiel kann die Auswertung des betriebliche Kommunikationsverhaltens zum Zwecke der „Selbstoptimierung" (Softwarebeispiel: IBM Social Dashboard[1204] oder Microsoft MyAnalytics[1205]) genannt werden. Ebenfalls gibt es inzwischen Tools (z.B. Office 365 Workplace Analytics[1206]), die die Daten auch auf Unternehmensebene darstellen. So kann dort eingesehen werden, wer wie lange an einem Dokument gearbeitet hat oder welche Kontakte mit welchen Betreffzeilen miteinander kommuniziert haben.[1207] Da hier nicht notwendigerweise Aussagen zum Primärleistungsverhalten getroffen werden und somit kein Leistungsdruck erzeugt wird, sind die Interessen der Parteien in solchen Fällen anders zu bewerten.

In diesem Zusammenhang ist zunächst die Frage aufzuwerfen, ob das Scoring nicht direkt leistungsrelevanter Daten (beispielsweise zum Zwecke der Selbstoptimierung) überhaupt von § 26 Abs. 1 BDSG erfasst werden kann, also die Datenverarbeitung als „erforderlich für die Durchführung des Arbeitsverhältnisses" ist. Andernfalls muss ggf. auf eine andere Legitimationsgrundlage wie Art. 6 Abs. 1 lit. f DSGVO oder eine Einwilligung zurückgegriffen werden.

1204 Eine mögliche Darstellungsform zeigt der Screenshot unter **C. § 4 V.**

1205 Siehe die Produktbeschreibung auf der Website: https://products.office.com/de-de/business/myanalytics-personal-analytics (letzter Abruf am: 28.02.2020).

1206 Vgl. die Beschreibung auf der Website: https://products.office.com/de-de/business/workplace-analytics (letzter Abruf am: 28.02.2020).

1207 *DGB*, Darum ist Microsoft Office 365 ein Fall für den Betriebsrat, 24.07.2017, abrufbar unter: https://www.dgb.de/themen/++co++0342f31e-6c85-11e7-b8f9-525400e5a74a (letzter Abruf am: 28.02.2020); ferner *Kraus*, DB 2018, 701 (703); zu beachten ist allerdings, dass Microsoft damit wirbt, dass sie die Vorgaben der DSGVO einhalten und personenbezogene Daten nur dem einzelnen Arbeitnehmer zur Verfügung stellen, während die Unternehmensansicht lediglich aggregierte, anonyme Daten sind, vgl. https://docs.microsoft.com/de-DE/workplace-analytics/myanalytics/overview/privacy-guide (letzter Abruf am: 28.02.2020).

§ 26 Abs. 1 BDSG erfordert, dass der Arbeitgeber die Daten zur Erfüllung seiner vertraglichen oder gesetzlichen Pflichten oder Wahrnehmung seiner Rechte benötigt, wobei auch die Erforderlichkeit der Daten zur Wahrnehmung berechtigter Interessen des Arbeitgebers davon umfasst sind.[1208] Unter diesem Aspekt ist es auf den ersten Blick zweifelhaft, die Datenerfassung und -verarbeitung bezüglich des betrieblichen Verhaltens unter § 26 Abs. 1 BDSG zu subsumieren. Es könnte aber eine Wahrnehmung berechtigter Interessen vorliegen, wenn die Auswertung des betrieblichen Verhaltens und die Selbstoptimierung zum Zwecke der Effizienzsteigerung der Arbeitskraft erfolgen. Arbeitgeber haben ein berechtigtes Interesse daran, das Unternehmen möglichst wirtschaftlich zu führen und Arbeitnehmer in höchstem Maße gewinnbringend einzusetzen.[1209]

Die Verarbeitung müsste hierfür nicht nur „erforderlich" sein, d.h. kein milderes, gleich effektives Mittel zur Erreichung des Zwecks geben, sondern die Maßnahme ist auch auf ihre Geeignetheit zu überprüfen. Geeignet ist eine Maßnahme dann, wenn sie tauglich ist, den gewünschten Zweck zu fördern. In der *Belastungsstatistik*-Entscheidung hatten sich die Erfurter Richter mit diesem Begriff in einem ähnlichen Kontext auseinanderzusetzen.[1210] Dort sahen die Richter erhebliche Zweifel bei einer Belastungsstatistik, die in der konkreten Ausgestaltung nicht die Belastungssituation einzelner Ebenen erfasste und rein quantitative Erhebungen traf, ohne auf die Komplexität der einzelnen zugewiesenen Aufgabe einzugehen.[1211]

Die gleiche Gefahr besteht bei der Auswertung des betrieblichen Verhaltens, insbesondere des Kommunikationsverhaltens, wenn die eingesetzten Algorithmen nicht die individuelle Position und Situation der Arbeitnehmer berücksichtigen, sondern schlichtweg einen Vergleich zur gesamten Abteilung oder Unternehmen darstellen. Dann verliert der Score aufgrund des Kontextverlusts seinen Aussagewert.

Beispiel: Ein Abteilungsleiter, der eine Führungsverantwortung für 40 Arbeitnehmer in der Abteilung hat, bekommt einen schlechten Score, da er einen hohen Zeitanteil seines Arbeitstages in Meetings und mit dem Verfassen und Beantworten von E-Mails verbringt, während die restlichen

---

1208 Zum Zweck „Erforderlichkeit für die Durchführung des Beschäftigungsverhältnisses", siehe **E. § 1 I. 1. b) bb)**.

1209 BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205 (1212) Rn. 36 zu einer "Belastungsstatistik".

1210 Zum Inhalt der Entscheidung, siehe bereits **E. § 1 III. 2. a) cc) (4)**.

1211 Vgl. BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205 (1210) Rn. 26.

40 Arbeitnehmer im Verhältnis nur wenige E-Mails schreiben, sich einmal wöchentlich zu einem kurzen „Jour-Fixe" treffen und den Rest der Arbeitszeit mit ihrer Kernarbeit verbringen.

Dieses Beispiel zeigt eigentlich eine sehr effektiv funktionierende Abteilung, bei der ein einzelner Abteilungsleiter sich um die Organisation der Arbeit kümmert und die anstehenden Arbeiten im „Jour-Fixe" verteilt, sodass die restlichen Arbeitnehmer der Abteilung effizient arbeiten können. Der niedrige Score beruht dann darauf, dass ihm ein ganz anderer Aufgabenbereich zugewiesen ist als Abteilungsleiter, der im Algorithmus nicht ausreichend Berücksichtigung gefunden hat.

Ohne Aussagewert sind solche Scores nicht geeignet, den gewünschten Zweck („*Effizienzsteigerung des Unternehmens und Gewinnmaximierung*") zu fördern, sondern sogar eher hinderlich. Der Abteilungsleiter im o.g. Beispiel könnte aufgrund des Scores nun Anreize bekommen, seine Organisationstätigkeit zurückzufahren, um eine bessere Bewertung zu erhalten. Dies führt dazu, dass die sehr effizient arbeitenden 40 Abteilungsmitarbeiter nunmehr mehr Organisatorisches erledigen müssen und die Effizienz sinkt, da weniger produktive Arbeit geleistet werden kann.

Der Einsatz solcher Software setzt also voraus, dass im Vorhinein ausreichend Analysearbeit geleistet wird, um „korrekte" Vergleichsgruppen für das Scoring bilden zu können. Selbst in solchen Fällen kann jedoch die individuelle Situation von Arbeitnehmern nur gering berücksichtigt werden, sodass solche Vergleichsscorings kaum Aussagewert besitzen. Etwas anderes kann dann gelten, wenn nicht verschiedene Arbeitnehmer verglichen werden, sondern das Verhalten einzelner Arbeitnehmer im Zeitverlauf isoliert gescort wird.

Beispiel: Max Mustermann stellt fest, dass er kaum noch Arbeitszeit für seine Kerntätigkeit (die Software-Programmierung) zur Verfügung hat. Er kann jedoch nicht konkret ausmachen, was die Gründe hierfür sind; er merkt lediglich, dass er viel mehr Zeit mit dem Verfassen von E-Mails verbringt. Hier könnte eine solche Software zunächst aufdecken, welchen Anteil der Arbeitszeit das Beantworten von E-Mails im Zeitverlauf in Anspruch genommen hat. Werden weitere Kommunikationsparameter ausgewertet,[1212] könnte Max feststellen, dass nur ein Bruchteil seiner E-Mails gelesen, beantwortet oder weitergeleitet werden, er mithin seine Arbeitszeit effektivieren könnte, wenn er auf das Verfassen von E-Mails weitgehend verzichtet.

1212 Vgl. Beispiele in *Höller/Wedde*, Die Vermessung der Belegschaft, S. 26 f.

Solche Scorings könnten mit Schwellenwert-Trigger versehen werden, die den Arbeitnehmer per E-Mail informieren, wenn bestimmte Grenzen überschritten wurden und ihm in weiterer Folge Handlungsempfehlungen zugeleitet werden. Da der einzelne Arbeitnehmer seine individuelle Situation kennt, ist die Gefahr „fehlerhafter" Scorings gering. Eventuell entstehende Abweichungen zu früheren Werten kann er nachvollziehen und dadurch informiert entscheiden, ob Handlungsbedarf vorhanden ist.

Für den Fall, dass die Analyseergebnisse jedoch nur für den Arbeitnehmer selbst angezeigt werden, ist die Frage nach der Geeignetheit der Maßnahme aufzuwerfen, wenn Dashboards Arbeitnehmern aufgezwungen werden können:

Hintergrund hierfür ist, dass ein Arbeitnehmer möglicherweise die E-Mails nicht liest oder auch das Dashboard als Startseite sofort schließt, wenn er kein Interesse an einer solchen Auswertung hat.

Es stellt sich auch ein weiteres Problem: Eine solche Verarbeitung ist nicht erforderlich, da es ein milderes Mittel für die daran interessierten Arbeitnehmer gibt, das gleich effektiv ist. Nämlich: Die Einholung von Einwilligungen bei Nutzung eines solchen Dienstes als originärer Ausfluss der Selbstbestimmung. Da niemand sonst Zugriff auf die Daten des Scorings hat, ist von einer Freiwilligkeit auszugehen, da lediglich Vorteile für den Arbeitnehmer entstehen (§ 26 Abs. 2 S. 2 BDSG).

§ 26 Abs. 1 S. 1 BDSG scheidet daher unter den genannten Umständen als Legitimationsgrundlage aus.

Im Ergebnis sind die Anwendungsfelder für betriebliches Verhaltensscoring auf Basis von § 26 Abs. 1 S. 1 BDSG sehr eingeschränkt; bei der Auswertung von Kommunikationsverläufen bzw. des Kommunikationsverhaltens ist zudem die Rechtsentwicklung im Bereich der Anwendbarkeit des TKG auf Arbeitgeber bei erlaubter Privatnutzung im Auge zu behalten; nach hier vertretener Auffassung spricht bei entsprechender technischer Implementation nichts dagegen, die Kommunikationsparameter betrieblicher Kommunikation im Rahmen von People Analytics auszuwerten.[1213]

Dennoch ist Scoring des betrieblichen Verhaltens ist datenschutzrechtlich nicht grundsätzlich ausgeschlossen. Sollen die personenbezogenen Daten eines Arbeitnehmers nicht nur für ihn selbst erhoben und ausgewertet werden, ist die Legitimationsgrundlage ist § 26 Abs. 1 S. 1 BDSG, wenn die Verarbeitung auch zur Durchführung seines Beschäftigungsverhältnisses dient. Auf Art. 6 Abs. 1 lit. f DSGVO hingegen muss zurückgegriffen

1213 Vgl. **D. § 3 I. 2. b) bb)**.

werden, wenn die Verarbeitung der personenbezogenen Daten des Arbeitnehmers keinen Bezug mehr zu seinem Beschäftigungsverhältnis aufweist.

Beispiel: Die personenbezogenen Daten von Arbeitnehmern eines besonders effizient arbeitenden Teams werden erhoben, um Probleme in vergleichbaren Teams zu erkennen. Aufgrund der verschiedenen Aufgabenzuweisungen innerhalb des Teams ist es erforderlich, dass die jeweilige Zuweisung bekannt ist, um die Daten sinnvoll miteinander zu vergleichen können. Obwohl keine Namen genutzt werden, ist eine Identifizierbarkeit anhand der Daten gegeben. Hier dient die Verarbeitung der personenbezogenen Daten des einen Teams nicht zur Durchführung der Beschäftigungsverhältnisse dieser Arbeitnehmer, sondern zur Optimierung anderer Teams, sodass die Datenverarbeitung nicht auf § 26 Abs. 1 S. 1 BDSG gestützt werden kann, sondern auf Art. 6 Abs. 1 lit. f DSGVO basieren muss. Der Abwägungsmaßstab ist aber inhaltlich derselbe, sodass sich hieraus keine Unterschiede ergeben.

(d) Scoring von Gesundheitsdaten

Letztlich stellt sich in diesem Zusammenhang noch die Frage, ob auch ein Scoring von Gesundheitsdaten als sensitive Daten im Sinne von Art. 9 DSGVO zulässig sein kann, wenn dies im Rahmen des betrieblichen Gesundheitsmanagements oder zur Gefahrenprävention stattfindet. Auch hier sollte kurz vorweg klargestellt werden, dass das Scoring an sich noch kein Fall des Art. 22 DSGVO darstellt und daher grundsätzlich Gesundheitsdaten als Grundlage dienen können; eine solche Verarbeitung nicht bereits aufgrund Art. 22 Abs. 4 DSGVO verboten.

Wie bereits im Rahmen der Bewertung von Simple People Analytics-Maßnahmen dargestellt (**E. § 1 III. 1. b) bb) (2)**), unterliegen solche Daten gem. § 26 Abs. 3 S. 1 BDSG einem erhöhten Schutz. So ist es nicht mehr ausreichend, wenn der Arbeitgeber ein berechtigtes Interesse an der Verarbeitung der Daten im Rahmen des Beschäftigungsverhältnisses hat, sondern vielmehr entscheidend, dass die Verarbeitung der Daten zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist.

Für die rechtliche Bewertung gilt, dass an dieser Stelle nicht die Erhebung und Verarbeitung der Daten selbst im Vordergrund steht, sondern ein darauf beruhendes Profiling / Scoring, d.h. beispielsweise die Erstellung eines Gesundheitsprofils oder Gesundheitsscores des Arbeitnehmers.

Von einer rechtmäßigen Erhebung der Gesundheitsdaten für Zwecke der People Analytics unter den bereits im Rahmen von SPA genannten Voraussetzungen wird daher im weiteren Verlauf ausgegangen.

Da die hier untersuchte Grundlage der Verarbeitung nicht etwa eine Betriebsvereinbarung oder Einwilligung ist, muss geprüft werden, ob die Bewertung der Gesundheit für die Erfüllung gesetzlicher Pflichten insbesondere aus dem Arbeitsrecht erforderlich ist.

Ist die Verarbeitung nicht für die Durchführung des Beschäftigungsverhältnisses erforderlich, so beispielsweise im Rahmen der Gesundheitsvorsoge, so sind andere Rechtsgrundlagen der Verarbeitung nicht ausgeschlossen. Letzteres könnte auf § 22 Abs. 1 Nr. 1 lit. b BDSG gestützt werden,[1214] wobei dort erforderlich ist, dass die Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden. Zur Gesundheitsvorsorge gehört insbesondere auch die Arbeitsmedizin im Sinne einer arbeitsmedizinischen Fürsorge.[1215] In diesem Fall schreibt das Gesetz explizit vor, dass der Datenbestand unter Verantwortung des Arbeitsmediziners verarbeitet wird, d.h. diese Daten dürfen zwar – sofern die weiteren Voraussetzungen vorliegen – für arbeitsmedizinische Zwecke unter Umständen einem Profiling oder Scoring unterzogen werden, nicht hingegen für beschäftigungspolitische Zwecke durch die HR-Abteilung. Beschäftigten kann somit u.U. eine Gesundheitsapp auf dem Smartphone zur Verfügung gestellt werden, dabei muss aber darauf geachtet werden, dass der Arbeitgeber auf den Datenbestand keinen Zugriff hat, um den Anforderungen des § 22 Abs. 1 Nr. 1 lit. b BDSG zu entsprechen.

Für Advanced People Analytics bleiben daher nur noch solche sensitiven Daten, die für die Erfüllung gesetzlicher Pflichten, insbesondere aus dem Arbeitsrecht erforderlich sind. Die Einschränkung aus dem Wortlaut des § 26 Abs. 3 S. 1 BDSG ist freilich zu beachten, aus dem sich ergibt, dass die Daten *ausschließlich* für die Erfüllung der gesetzlichen Pflicht verarbeitet werden dürfen. Weitergehende Analytics sind nicht statthaft. Die Wertung des Art. 9 Abs. 1 DSGVO, wonach grundsätzlich ein Verarbeitungsverbot für solche Daten gilt, ist bei der Bewertung zu berücksichtigen, sodass ein Scoring / Profiling zwingend erforderlich sein müsste, um die gesetzlichen Pflichten zu erfüllen; das gesetzlich festgelegte Regel-Ausnahmeverhältnis darf nicht ins Gegenteil umgekehrt werden.

1214 So ausdrücklich die Gesetzesbegründung zu § 26 BDSG, BT-Drs. 18/11325, S. 98.

1215 BT-Drs. 18/11325, S. 95.

Während für Simple People Analytics eine Fortschreibung bisheriger gesundheitsrelevanter Daten für prospektive Sicherheitsbewertungen noch erforderlich sein kann, ist dies beim Profiling / Scoring von Gesundheitsdaten grundsätzlich zu verneinen. Es sind keine Gründe ersichtlich, weshalb über die prospektive Betrachtung im Rahmen von SPA hinausgehend, ein Scoring zwingend erforderlich sein sollte. Etwas anderes gilt natürlich, wenn ein Gesetz (in der Zukunft) bestimmte Profiling-/Scoring-Maßnahmen vorschreiben sollte. Dann ist allerdings Rechtsgrundlage nicht mehr § 26 Abs. 1 S. 1 BDSG, sondern Art. 6 Abs. 1 lit. c DSGVO.

(e) Zwischenergebnis

Schon im Bewerbungsverfahren unterliegt das Bewerten von „weichen" Kriterien der Bewerber hohen Maßstäben an die Datenerhebung; die Grenzen des Fragerechts des Arbeitgebers sind (auch bei weitergehenden Scoring-Maßnahmen) einzuhalten. Sind die Daten zulässigerweise erhoben, so ist auch eine daran anknüpfende Bewertung in Form eines Profilings, Scorings oder Rankings, das die Persönlichkeitsrechte der Arbeitnehmer wahrt, in aller Regel vom Zweck der Erforderlichkeit für die Begründung des Beschäftigungsverhältnisses nach § 26 Abs. 1 S. 1 BDSG erfasst, wie sich aus den beispielshaften Fällen zeigt. Vorsicht ist geboten, wenn Daten von bereits im Unternehmen beschäftigten Arbeitnehmern als Vergleichsgrundlage herangezogen werden sollen; für diese Datenerhebung ist nicht § 26 BDSG einschlägig, sondern Art. 6 Abs. 1 lit. f DSGVO. Möglich ist auch eine Verarbeitung auf Basis einer Betriebsvereinbarung sowie – mangels nachteiliger Folgen für den Arbeitnehmer bei strenger Zweckbindung der Daten – die Einholung einer Einwilligung.

Nach Begründung des Beschäftigungsverhältnisses scheidet ein Scoring der Hauptleistungspflicht aus, wenn das Leistungsverhalten des Arbeitnehmers lückenlos überwacht und hierdurch ein Überwachungs- und Anpassungsdruck erzeugt wird. Etwas anderes gilt dann, wenn die Daten, die im Rahmen von Mitarbeitergesprächen oder Zielvereinbarungen getroffen wurden, in ein Personalmanagementsystem eingepflegt werden, welches eine Gesamtbewertung in Form eines Scores generiert. Letztere Verarbeitung ist von § 26 Abs. 1 S. 1 BDSG gedeckt, da der Arbeitgeber ein berechtigtes Interesse daran hat, einen schnellen Überblick über die Leistung seiner Arbeitnehmer zu bekommen und hiergegen kein wesentliches Interesse des Arbeitnehmers am Unterbleiben eines solchen Scorings spricht,

sofern die zugrunde gelegten Daten korrekt sind und rationale Verfahren eingesetzt werden.

Bei der Bewertung des betrieblichen Verhaltens muss ebenfalls darauf geachtet werden, dass kein „Gefühl des Überwachtwerdens" erzeugt wird. Einsatzbeispiel könnte eine Auswertung des innerbetrieblichen Kommunikationsverhaltens für Zwecke der Selbstoptimierung des Arbeitnehmers sein, um die Effizienz der Arbeit zu steigern. Eine solche müsste allerdings mangels Geeignetheit bei Zwang auf einer Einwilligung nach § 26 Abs. 2 BDSG basieren. Lediglich Auswertungen zur Optimierung von Teams oder Abteilungen auf personenbezogener Basis zur Unterstützung von Entscheidungen von Vorgesetzten können unter gewissen Voraussetzungen auf § 26 Abs. 1 S. 1 BDSG gestützt werden.

Ein Scoring von sensitiven Daten (wie beispielsweise Gesundheitsdaten) ist in aller Regel unzulässig. Etwas anderes kann gelten, wenn die Datenverarbeitung und das Scoring im Rahmen der Gesundheitsvorsorge durch den innerbetrieblichen ärztlichen Dienst erfolgt. In Sonderfällen kann auch eine Verarbeitung auf Grundlage einer Einwilligung zulässig sein, beispielsweise dann, wenn Gesundheitsdaten von Profisportlern zur Team- und individuellen Leistungsoptimierung genutzt werden sollen. Legitimationsgrundlage ist dann § 22 Abs. 1 Nr. 1 lit. b BDSG. Zu beachten ist, dass der Arbeitgeber keinen Zugriff auf diese Daten erhalten darf und somit ein Einsatz für People Analytics im Bereich von HR-Maßnahmen ausscheidet.

(3) Legitimation durch eine Betriebsvereinbarung

Um Rechtsunsicherheiten bei der Anwendung des § 26 Abs. 1 BDSG oder Einholung einer Einwilligung zu umgehen, kann in bestimmten Fällen auch eine Betriebsvereinbarung abgeschlossen werden, um die Datenverarbeitung zu legitimieren. Hierdurch kann auch eine Verarbeitung von sensitiven Daten erfolgen, wie sich aus der Rechtsgrundlage des nach § 26 Abs. 4 S. 1 BDSG ergibt.

Art. 88 DSGVO bzw. § 26 Abs. 4 S. 1 BDSG spezifizieren als Legitimationsgrundlage nicht nur die Betriebsvereinbarung, sondern auch die Gesamtbetriebsvereinbarung, Konzernbetriebsvereinbarung sowie die zwischen Arbeitgeber und Sprecherausschuss zustande gekommenen Spre-

cherausschussrichtlinien nach § 28 SprAuG[1216] sowie etwaige Dienstvereinbarungen im öffentlichen Dienst (§ 73 BPersVG).[1217] Nur schuldrechtlich zwischen dem Arbeitgeber und dem Betriebsrat wirkende Regelungsabreden hingegen fallen mangels normativem Charakter nicht unter den Begriff der „Kollektivvereinbarung" und stellen somit keine tauglichen Rechtsnormen dar.[1218]

Zu beachten ist, dass die Betriebsvereinbarung nur für den in § 5 BetrVG genannten Personenkreis eine normative Wirkung entfalten und somit Legitimationswirkung besitzen kann; entsprechend scheiden Betriebsvereinbarungen über Scoring in Bewerbungssituationen aus.[1219]

In inhaltlicher Hinsicht dürfen die Vereinbarungen die Datenverarbeitung im Beschäftigtenkontext spezifizieren im Sinne einer Spezialregelung, aufgrund von Art. 88 Abs. 2 DSGVO jedoch nicht grundlegend vom Schutzstandard abweichen.[1220] Auch § 75 Abs. 2 BetrVG schreibt einen sehr ähnlichen Prüfungsmaßstab vor.[1221] Den Betriebspartnern sind aber gewisse (Einschätzungs-)Spielräume bei der Beurteilung der Eingriffsintensität einer einzuräumen (siehe bereits **E. § 1 III. 1. c) aa)**).

Über ein Scoring der Arbeitsleistung kann nach der *Belastungsstatistik*-Entscheidung des BAG[1222] grundsätzlich eine Betriebsvereinbarung abgeschlossen werden, die Auswertungen durch Überwachung der Primärleistungspflicht regelt. Zu beachten ist allerdings, dass die eingesetzte Datenverarbeitung insbesondere geeignet sein muss, die Arbeitsleistung für die Zwecke der Auswertungen auch korrekt zu erfassen und es nicht zu einer dauerhaften Überwachung der Primärleistungspflicht kommt. Zudem muss sie transparent gestaltet sein, sodass Beschäftigte einerseits im Vorfeld durch eine entsprechende Information nach Art. 13 f. DSGVO über die Vorgänge der Verarbeitung aufgeklärt werden und andererseits

1216 Vgl. *Dzida/Grau*, DB 2018, 189 (191): Sprecherausschussvereinbarungen sind ebenfalls als Kollektivvereinbarungen im Sinne von Art. 88 Abs. 1 DSGVO sowie § 26 Abs. 4 BDSG anzusehen.

1217 *Seifert*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 88 DSGVO Rn. 27.

1218 Vgl. *Seifert*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 88 DSGVO Rn. 28.

1219 Siehe bereits im Detail **E. § 1 III. 1. c) bb)**; ferner *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 252.

1220 Vgl. **D. § 1 V. 2** sowie **E. § 1 III. 1. c) aa)**.

1221 A.A. wohl *Wybitul*, ZD 2016, 203: Die Anforderungen des Art. 88 Abs. 2 DSGVO gehen über die Beschränkungen nach § 75 Abs. 2 BetrVG hinaus (mit unklarem Nachweis).

1222 BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205.

Kenntnis darüber erhalten können, welche personenbezogene Daten für das Scoring herangezogen werden und welche Folgen dies haben kann.

Eine pauschale Aussage zur Zulässigkeit solcher Regelungen verbietet sich, da dies jeweils anhand des konkreten Systems, dem gewünschten Auswertungsziel und der daran anknüpfenden Maßnahmen im Einzelfall zu bewerten ist. In **Kapitel F** stellt diese Arbeit verschiedene Einsatzszenarien und Regelungsmöglichkeiten für eine rechtskonforme Regelung der Datenverarbeitung auf Basis einer Betriebsvereinbarung dar.

Beim Scoring des betrieblichen Verhaltens gelten dieselben Maßstäbe. Hier ist allerdings zu berücksichtigen, dass nur bedingt Rückschlüsse auf das Leistungsverhalten gezogen werden können, was grundsätzlich den entstehenden Druck für die betroffenen Arbeitnehmer verringert. Dennoch ist darauf zu achten, dass durch die Überwachung des Verhaltens keine Totalüberwachung statuiert wird. Eine solche wäre datenschutzrechtlich unzulässig, da sie die betroffenen Arbeitnehmer in rechtswidriger Weise in ihren Grundrechten beeinträchtigen würde.[1223] Die Erzeugung von Bewegungsprofilen mittels RFID- oder GPS-Technik kann auch per Betriebsvereinbarung aufgrund der extrem hohen Eingriffsintensität in die Rechte der Arbeitnehmer nur in sehr begrenztem Maße legitimiert werden: In keinem Fall dürfen heimliche Überwachungsmaßnahmen etabliert werden; solche sind allenfalls zur Aufdeckung von Straftaten nach § 26 Abs. 1 S. 2 BDSG zulässig.[1224] Unter dem Gesichtspunkt des Überwachungsdrucks scheiden permanente, anlasslose Überwachungsmaßnahmen aus, da diese zu tief in die Persönlichkeitsrechte der Betroffenen eingreifen würden und somit nach § 75 Abs. 2 BetrVG unzulässig wären.

Stichprobenartige, offene Überwachungsmaßnahmen können allerdings in Betriebsvereinbarungen als „erforderlich" erachtet werden, um eine grundsätzliche Leistungs- und Verhaltenskontrolle zu statuieren.

Da in den genannten Bereichen auch betriebsverfassungsrechtliche Mitspracherechte, insbesondere aus § 87 Abs. 1 Nr. 6 BetrVG, bestehen, kommt der Betriebsvereinbarung insofern eine Doppelfunktion zu.[1225]

1223 *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 108; vgl. BAG, Beschl. v. 29.06.2004 – 1 ABR 21/03, NZA 2004, 1278 (1283 f.) = BAGE 111, 173 = AP BetrVG § 87 1972 Überwachung Nr. 41 (m. Anm. Ehmann) zum Abwägungsmaßstab bei einer Videoüberachung im Betrieb.

1224 *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 131.

1225 *Wurzberger*, ZD 2017, 258 (260).

Bei der Auswertung der betrieblichen Kommunikation auf Basis einer Betriebsvereinbarung ist zudem die Rechtsprechung zur Anwendbarkeit des TKG bei erlaubter Privatnutzung im Auge zu behalten; Betriebsvereinbarungen können anders als im Beschäftigtendatenschutz nicht legitimierend für Eingriffe in das Fernmeldegeheimnis durch Arbeitgeber wirken.

Zu beachten ist ferner, dass in Betriebsvereinbarungen ausschließlich Sonderregelungen für die Zwecke des Beschäftigungsverhältnisses getroffen werden dürfen.[1226] Im unter (**d**) genannten Beispiel der „Gesundheitsapp" durch die Arbeitsmedizin schiede dementsprechend eine Betriebsvereinbarung aus.

Etwas anderes könnte gelten, wenn bestimmte Gesundheitsdaten für Zwecke des Arbeitsschutzes gescort werden sollen. Hierfür kann die Betriebsvereinbarung grundsätzlich eine taugliche Legitimationsgrundlage, insbesondere im Hinblick auf die sensitiven Daten, nach § 26 Abs. 4 S. 1 BDSG darstellen. Ausweislich der Gesetzesbegründung beruht die Befugnis zur Regelung der Verarbeitung von sensitiven Daten in Kollektivvereinbarungen auf Art. 9 Abs. 2 lit. b DSGVO.[1227] Nach dieser Norm ist die Verarbeitung besonderer Kategorien von personenbezogenen Daten zulässig, wenn die Verarbeitung erforderlich ist, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht […] erwachsenen Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach […] einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten […] zulässig ist. Erforderlich ist, dass geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorgesehen werden. Nach deutschem Recht regelt dies § 22 Abs. 2 BDSG, der somit auch auf die Verarbeitung auf Grundlage einer Kollektivvereinbarung anwendbar ist.

Nach § 26 Abs. 3 BDSG fehlt für ein Scoring von Gesundheitsdaten für diese Zwecke bzw. im Rahmen von Advanced People Analytics eine gesetzliche Basis (siehe (**d**)). Den Betriebspartnern steht es in diesem Kontext aber grundsätzlich offen, eine erweiterte Regelung für die Verarbeitung von sensitiven Daten zu treffen, wenn sie in der konkreten Betriebs-/Unternehmenssituation den Pflichten zum Arbeitsschutz durch ein Scoring besser bzw. effektiver nachgekommen werden kann. Voraussetzung: Die Rechte der Betroffenen müssen hinreichend berücksichtigt und geschützt werden.

1226 *Wybitul*, ZD 2016, 203 (207).
1227 BT-Drs. 18/11325, S. 98.

Letztlich können durch eine Betriebsvereinbarung auch nach Erwägungsgrund 155 der DSGVO spezifische Möglichkeiten der Einwilligung von Arbeitnehmern in besonderen Verarbeitungssituationen geregelt werden, indem beispielsweise der Begriff der Freiwilligkeit konkreter geregelt wird. So könnte beispielsweise festgelegt werden, dass für die Einwilligung des Arbeitnehmers in bestimmten Verarbeitungssituationen eine Freiwilligkeit vermutet wird. Eine unwiderlegliche Vermutung der Freiwilligkeit wäre hingegen wohl nicht mit Art. 88 Abs. 2 DSGVO vereinbar, da es den Grundsatz aushebeln würde. Möglich sind ferner auch abweichende Regelungen zur Form der Einwilligung des Arbeitnehmers. Während das deutsche Recht in § 26 Abs. 2 S. 3 BDSG vorschreibt, dass die Einwilligung grundsätzlich schriftlich oder elektronisch[1228] zu erfolgen hat, können in einer Betriebsvereinbarung auch mündliche Einwilligungen für bestimmte Verarbeitungen entsprechend Art. 4 Nr. 11 DSGVO als ausreichend bestimmt werden oder strengere Voraussetzungen wie die Schriftform für besonders intensive Verarbeitungssituationen statuiert werden.

3. Zwischenergebnis

Simple People Analytics werfen datenschutzrechtlich kaum Probleme auf. Es ist davon auszugehen, dass diese als klassische Personalmanagement-Maßnahmen in aller Regel „erforderlich" im Sinne von § 26 Abs. 1 S. 1 BDSG sind, da die Arbeitgebergeberinteressen an einem effektiven Personaleinsatz sowie -planung überwiegen. Das Themenfeld um Advanced People Analytics hingegen, das derzeit umgangssprachlich schlicht als „People Analytics" bezeichnet wird und mit einer Bewertung persönlicher Merkmale (*Profiling*) einhergeht, ist deutlich komplexer zu beurteilen. Einerseits ist bereits die begriffliche Definition unscharf,[1229] sodass sich pauschale Aussagen zur Zulässigkeit oder Unzulässigkeit von People Analytics verbieten.[1230] Das Feld von People Analytics reicht von einfachen computergestützten Skill-Abgleichen im Rahmen des Bewerbungsprozesses bis hin zur Erstellung detaillierter Persönlichkeitsprofile der Arbeitnehmer durch lückenlose Überwachung mittels Log-Dateien, Wearables und Sen-

1228 Die grundsätzliche Zulässigkeit der elektronischen Form wurde mit dem zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU) eingefügt, vgl. BT-Drs. 19/11181, S. 19.

1229 Zu dieser Problematik bereits **C. § 1**.

1230 So aber BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 118.3.

soren.[1231] Während ersteres unter dem Gesichtspunkt der Erforderlichkeit für die Entscheidung über die Begründung des Beschäftigungsverhältnisses gerechtfertigt sein kann (**E. § 1 III. 2. c) dd) (2) (a)**), scheidet letzteres auf jeden Fall aufgrund des gravierenden Eingriffs in die Persönlichkeitsrechte der Arbeitnehmer aus (**E. § 1 III. 2. c) dd) (2) (b)** und (**c**)).

Dazwischen besteht eine rechtliche „Grauzone",[1232] die in der Rechtsprechung noch nicht ausgeurteilt und auch in der Literatur allenfalls oberflächlich behandelt wurde, obwohl die betriebswirtschaftliche Bedeutung im Rahmen der Arbeit 4.0 immer größer wird. Für die Bewertung der Fälle, die in diesem Zwischenfeld liegen, müssen die Systeme genau analysiert und festgestellt werden, welche Daten für welchen Zweck erhoben werden, wie hoch die Arbeitgeberinteressen an der Verarbeitung solcher Daten sind und welche Arbeitnehmerinteressen entgegenstehen könnten. In vielen Fällen zulässig ist ein Profiling oder Scoring von Beschäftigtendaten zum Zwecke der Analytics, sofern es sich nicht um sensitive Daten im Sinne von Art. 9 DSGVO handelt. Obwohl die spezifische Regelung zum Scoring nach § 31 BDSG unionsrechtswidrig ist, sind die darin enthaltenen Grundsätze bereits in der DSGVO selbst enthalten und bieten gute Anhaltspunkte für Arbeitgeber, welche Mindestanforderungen an eine Bewertung von Arbeitnehmern durch Algorithmen zu stellen sind, um diese rechtskonform umzusetzen.

Auch der Einsatz künstlicher Intelligenz im Rahmen von Scoring- und Profilingverfahren scheidet nicht per se aus, sofern die Verfahren eine gewisse Basisrationalität wahren und somit hinreichend transparent ausgestaltet werden (**E. § 1 III. 2. c) cc)**).

Das Instrument der Betriebsvereinbarung kann die Datenverarbeitung in diesem spezifischen Kontext weitgehend rechtssicher legitimieren, sofern die Betriebspartner die Grundsätze der DSGVO und die berechtigten Interessen der Arbeitnehmer wahren. In Betriebsvereinbarungen können im Weiteren die Anforderungen an Einwilligungen von Arbeitnehmern für konkrete Verarbeitungsvorgänge spezifiziert werden, um Rechtssicherheit zu schaffen.

Außerhalb dieses Kontextes ist das Institut der Einwilligung im Rahmen für *People Analytics* im Beschäftigungsumfeld nur bedingt zur Legitimation von Verarbeitungen geeignet und unterliegt hohen Rechtsunsicherheiten. Ein mögliches Beispiel stellt das Scoring zum Selbstzweck dar (**E. § 1 III. 2. c) dd) (2) (c)**).

1231 Vgl. *Dzida/Groh*, ArbRB 2018, 179 (180).
1232 Ähnlich *Dzida*, NZA 2017, 541 (543).

IV. Mitbestimmungsrechte des Betriebsrats

Da die Betriebsvereinbarung datenschutzrechtlich „das Mittel der Wahl ist“[1233] und nach § 26 Abs. 6 BDSG die Beteiligungsrechte der Interessensvertretungen durch das Datenschutzrecht unberührt bleiben, stehen dem Betriebsrat weitgehende Mitbestimmungsrechte zu. Dies gilt insbesondere dann, wenn technische Überwachungssysteme eingesetzt werden oder die Erkenntnisse aus den Analytics unmittelbar in die Entscheidung bei Personalmaßnahmen einfließen sollen. Im Folgenden werden die einschlägigen Mitbestimmungsrechte des Betriebsrats aufgezeigt. Die in der folgenden Darstellung werden die Mitbestimmungsrechte für Simple People Analytics und Advanced People Analytics getrennt dargestellt.

Gerade in Bereichen, in denen ohnehin zwingende Mitbestimmungsrechte des Betriebsrats bestehen, empfiehlt es sich in jedem Fall, beim Entwerfen einer Betriebsvereinbarung entsprechende Regelungen zur Legitimation der Datenverarbeitung zu treffen, um Rechtsunsicherheiten bei der Auslegung des unbestimmten Rechtsbegriffs der Erforderlichkeit weitgehend zu vermeiden.[1234]

1. Simple People Analytics

Nach hiesiger Definition der Simple People Analytics handelt es sich um Maßnahmen, die aus bereits bestehenden Daten Fortschreibungen generieren, um prospektiv Personalplanung und -steuerung betreiben zu können. In diesem Zusammenhang werden keine neuen Daten durch technische Maßnahmen aktiv erhoben.

Simple People Analytics werden meist durch Personalmanagement-Software durchgeführt. Beim Einsatz solcher Software werden in aller Regel die Zugriffe durch die Personalverantwortlichen registriert und gespeichert (z.B. zum Zwecke der Missbrauchskontrolle). Da § 87 Abs. 1 Nr. 6 BetrVG bereits ausgelöst wird, wenn die Maßnahme geeignet ist, die Leistung von Arbeitnehmern zu erfassen (hier der HR-Mitarbeiter, deren Zugriffe auf das System protokolliert werden), hat der Betriebsrat ein zwin-

1233 So wohl auch *Körner*, NZA 2019, 1389 (1390).

1234 So wohl auch *Wybitul*, NZA 2017, 1488 (1494); *Klösel/Mahnhold*, NZA 2017, 1428 (1433).

gendes Mitbestimmungsrecht beim Einsatz solcher Software, auch wenn hierdurch die bewerteten Arbeitnehmer nicht überwacht werden.[1235]

Sollen die hierdurch gewonnen Vorhersagedaten als Grundlage herangezogen werden, um Lohnfestlegungen für das kommende Jahr zu treffen, so besteht auch ein Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 10 BetrVG, wenn es sich um konkret leistungsbezogene Entgelte handelt, wäre Nr. 11 einschlägig. Allerdings werden leistungsbezogene Entgelte in aller Regel retrospektiv bezahlt und sind daher nicht im Kernbereich der Simple People Analytics angesiedelt.

Da bei SPA – im Unterschied zu APA – nur ein simpler Abgleich des Bewerberprofils mit der Stellenanforderung und inhaltlich keine Bewertung von Bewerbermerkmalen stattfindet, handelt es sich bei dem Abgleich noch nicht um eine Auswahlrichtline nach § 95 BetrVG; Bewerber die nicht den Anforderungen entsprechen, werden vorab „aussortiert" und kommen daher gar nicht erst für die Stelle in Betracht, auch wenn beispielsweise nur eine Person sich bewirbt. Eine Auswahl zwischen Bewerbern findet daher nicht statt, da diese Maßnahme der Auswahl vorgelagert ist.[1236]

Nach § 92 BetrVG muss der Arbeitgeber den Betriebsrat über die Personalplanung und den gegenwärtigen und künftigen Personalbedarf […] umfassend unterrichten und mit ihm darüber beraten. Für die Berechnung und Beratung dieser Gegenstände werden SPA-Maßnahmen eingesetzt. Ebenso wird der Tatbestand erfüllt, wenn SPA im Betrieb eingeführt werden sollen, da auch dies eine Maßnahme der Personalplanung ist, über die frühzeitig zu informieren ist.[1237]

Letztlich handelt es sich bei der Einführung von People Analytics um die Planung einer technischen Anlage i.S.v. § 90 Abs. 1 Nr. 2 BetrVG, wenn diese über neue Softwarekomponenten erfolgen soll.[1238] Hiernach ist vor Einführung der Betriebsrat rechtzeitig zu unterrichten und mit ihm darüber zu beraten.

Mitbestimmungsrechte statuieren §§ 90 und 92 BetrVG allerdings keine, sondern lediglich Informations- und Beratungsrechte.

1235 Vgl. hierzu **D. § 2 II. 1. b) bb)**.
1236 Siehe grundlegend **D. § 2 II. 2. b)**.
1237 Siehe auch **D. § 2 II. 4**.
1238 Siehe die Ausführungen zu § 90 BetrVG unter **D. § 2 II. 5.**

2. Advanced People Analytics

Bei Advanced People Analytics werden nicht nur bestehende Daten mit einfachen statistischen Methoden fortgeschrieben, sondern Ziel dieser ist es, mit einer Vielzahl von neu zu erhebenden oder zweckändernd verarbeiteten Daten aussagekräftige Kennzahlen für ein evidenzbasiertes Personalmanagement zu erzeugen. Es erfolgt also auch eine inhaltliche Bewertung der Daten durch Profiling- oder Scoring-Maßnahmen. Automatisierte Entscheidungen erfolgen in diesem Stadium noch nicht, es steht zunächst die Datenerhebung und insbesondere -verarbeitung im Vordergrund.

Auf der Erhebungsebene wurden in diesem Rahmen insbesondere IT-Nutzungs- und Sensordaten (etwa von Wearables) untersucht. Da diese Maßnahmen aktiv Beschäftigtendaten aufzeichnen, hat der Betriebsrat nicht nur ein Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG in Bezug auf die Einführung eines APA-Systems, sondern bereits bei der Erhebung solcher Daten beim Arbeitnehmer, d.h. bei der Einführung von Wearables oder IT-Systemen, die eine solche Auswertung ermöglichen. Dies ist der Kernmitbestimmungstatbestand für Advanced People Analytics, da genau dieser dazu dient, die Persönlichkeitsrechte von Arbeitnehmern (die durch solche Maßnahmen besonders tangiert werden) zu schützen.[1239]

Schreibt der Arbeitgeber den Arbeitnehmern vor, „smart clothes" in besonders gefährlichen Bereichen zu tragen, um hierdurch die Arbeitssicherheit zu erhöhen, oder bestimmte Software zur Kommunikation mit Teamkollegen zu nutzen, handelt es sich um eine Regelung, die nicht das mitbestimmungsfreie Arbeitsverhalten selbst betrifft, sondern das Ordnungsverhalten im Betrieb, welches nach § 87 Abs. 1 Nr. 1 BetrVG der Mitbestimmung unterliegt.[1240] Weiterhin sind auch etwaige „Gesundheitswettbewerbe" z.B. durch die Ausgabe von Fitness-Trackern im Betrieb davon erfasst, wenn Arbeitgeber dadurch erreichen möchten, dass sich Arbeitnehmer im Betrieb aktiver verhalten, z.B. öfters vom PC-Arbeitsplatz aufstehen und ein paar Schritte gehen.[1241] Auch hierdurch bezweckt der Arbeitgeber, das Verhalten der Arbeitnehmer in Bezug auf die betriebliche Ordnung zu beeinflussen.[1242]

1239 Vgl. **D. § 2 II. 1. b**).

1240 BAG, Beschl. v. 17.01.2012 – 1 ABR 45/10, NZA 2012, 687 (689) Rn. 23 zur Anordnung einer Dienstkleidungspflicht.

1241 Vgl. BAG, Beschl. v. 24.03.1981 – 1 ABR 32/78, NJW 1982, 404 = AP BetrVG 1972 § 87 Arbeitssicherheit Nr. 2 zu einem „Sicherheitswettbewerb" im Betrieb.

1242 Siehe hierzu grundlegend **D. § 2 II. 1. a**).

Erst recht werden wie bei Simple People Analytics auch die Mitbestimmungstatbestände der § 87 Abs. 1 Nr. 10 und 11 BetrVG ausgelöst, wenn die Daten genutzt werden sollen, die Entlohnung der Arbeitnehmer zu bestimmen oder leistungsbezogene Entgelte, die auf Scores basieren, festzulegen. Das Mitstimmungsrecht erstreckt sich auf die Bezugsgrößen einschließlich des Geldfaktors.[1243]

Werden im laufenden Arbeitsverhältnis oder im Bewerbungsprozess standardisierte Fragebögen eingesetzt (auch in digitaler Form von Eingabemasken), so muss der Betriebsrat nach § 94 BetrVG der Einführung zustimmen. Dieses Mitbestimmungsrecht besteht auch hinsichtlich des Inhalts der Fragebögen sowie die Umstände der Verwendung (somit auch Zweckbestimmung und Rahmenbedingungen der Datenverarbeitung). Solch standardisierte Formulare sind beispielsweise notwendig, um ein Bewerberscoring durchzuführen, damit die erhobenen Daten vergleichbar sind und etwaigen Fehlern beim CV-Parsing[1244] oder automatisierten Auswerten sonstiger eingereichter Unterlagen (z.B. mittels OCR-Scans) vorzubeugen.

§ 94 BetrVG greift auch ein, wenn das Verhalten oder die Leistung von Arbeitnehmern mit Hilfe von Scoring oder Profiling bewertet werden soll, da hierfür eine Bewertungsmatrix erforderlich ist (so auch beim Bewerberscoring, sodass hier das Mitbestimmungsrecht „doppelt" greift).

Beispiel: Der Arbeitgeber möchte ein System implementieren, welches die Arbeitnehmer im Betrieb in verschiedene Leistungskategorien klassifiziert. Für die verschiedenen Tätigkeiten werden einzelne Bewertungsmatrizen erstellt, die ein Scoring der Arbeitnehmer in den jeweiligen Tätigkeiten in Bezug zu den Anforderungen ermöglichen. Jeder Arbeitnehmer erhält einen Score. Durch die Erstellung des Scores lassen sich die Arbeitnehmer bei vergleichbaren Anforderungen in den Bewertungsmatrizen auch tätigkeitsübergreifend miteinander vergleichen und somit eine „Performer-Liste" für den gesamten Betrieb etablieren (z.B. zur Darstellung in Dashboards, hierzu **E. § 3 II**).

Weitgehende Informations- und Beratungspflichten statuiert § 92 BetrVG, die bereits in der Planungsphase eines Analytics-Systems ansetzen, sofern die hierdurch gewonnen Daten als Grundlage für Personalentscheidungen dienen sollen.

1243 ErfK/*Kania*, § 87 BetrVG Rn. 117.

1244 Parsing ist ein Vorgang, bei welchem mit Hilfe eines Computeralgorithmus Daten aus einem nicht für die elektronische Verarbeitung optimierten Dokuments gezogen werden.

Letztlich könnte die Einführung von Advanced People Analytics auch eine Betriebsänderung nach § 111 S. 3 Nr. 5 BetrVG darstellen, insbesondere wenn ein Unternehmen gleichzeitig von „klassischem" Personalmanagement auf evidenzbasiertes Management umstellt. Insbesondere bei einem Unternehmen ohne eine technisierte Personalabteilung kann es zu weitgehenden Änderungen durch Einführung grundlegend neuer Arbeitsmethoden kommen. Dies ist jedoch im Einzelfall zu prüfen.[1245] Jedenfalls aber stellt es die Planung einer technischen Anlage nach § 90 Abs. 1 Nr. 2 BetrVG dar.

V. Zusammenfassung

Die Anwendungsfelder für People Analytics in Betrieben und Unternehmen sind mannigfaltig. Unterschieden werden muss zwischen simplen und fortgeschrittenen People Analytics.

Bei den simplen Analytics werden lediglich vorhandene Daten durch einfache mathematische und statistische Verfahren fortgeschrieben. Solche werden bereits seit Jahren in vorhandenen Personalmanagementsystemen eingesetzt, um beispielsweise Fluktuationsquoten und sonstige Veränderungen im Personal mit Hilfe einer retrospektiven Betrachtung fortzuschreiben und Anhaltspunkte für zukünftige Veränderungen zu geben.

Solche Maßnahmen sind datenschutzrechtlich als relativ unkritisch einzustufen, da lediglich bereits rechtmäßig für die Zwecke der Durchführung des Beschäftigungsverhältnisses erhobene Daten (§ 26 Abs. 1 S. 1 Var. 2 BDSG) genutzt werden und keine *grundlegend* neuen personenbezogenen Daten generiert werden. Insbesondere findet hier keine inhaltliche Bewertung einzelner Personen statt, die mit tieferen Eingriffen in die Rechte der Arbeitnehmer verbunden ist. Oftmals lassen sich solche Analysen auch anonym durchführen, sodass der Datenschutz nur marginal (für den Anonymisierungsvorgang) berührt ist. Ist eine Anonymisierung tunlich, dass muss eine solche als milderes, gleich effektives Mittel auch vorgenommen werden.

Dennoch hat der Betriebsrat– allein aufgrund der Nutzung von Software – Mitbestimmungsrechte, die dazu führen, dass eine Betriebsvereinbarung abgeschlossen werden sollte, um diese Verfahren inhaltlich rechtsicher zu regeln. Eine solche kann nach Art. 88 DSGVO, § 26 Abs. 4 BDSG auch Datenverarbeitungen im Beschäftigtenkontext legitimieren, sodass

1245 Hierzu **D. § 2 II. 6. b**).

auch auf datenschutzrechtlicher Ebene Rechtssicherheit geschaffen werden kann.

Deutlich spannender und absolut im Trend sind fortgeschrittene (Advanced) People Analytics, die nicht nur bereits vorhandene Daten fortschreiben, sondern einerseits durch die Erhebung weiterer „Live-Daten" aus digitalen Systemen Echtzeitauswertungen ermöglichen und andererseits inhaltliche Bewertungen vornehmen. Hierfür kommen Profiling- und Scoring-Techniken zum Einsatz, die in vielen Fällen auch mit künstlicher Intelligenz kombiniert werden.

Solche Techniken sind unter datenschutzrechtlichen Gesichtspunkten weitaus kritischer zu betrachten, da sie eingriffsintensiver sind. Dennoch sind diese neuen Verfahren, sofern sie datenschutzkonform ausgestaltet werden und die Rechte der betroffenen Arbeitnehmer wahren, durchaus zulässig. Als Legitimationsgrundlage dient in der Regel § 26 Abs. 1 S. 1 BDSG, sofern die Durchführung des konkreten Beschäftigungsverhältnisses im Mittelpunkt steht. Sollen Daten von Arbeitnehmern für andere betriebliche Zwecke genutzt werden, muss auf Art. 6 Abs. 1 lit. f DSGVO zurückgegriffen werden.

In Fällen, in denen Arbeitnehmer keine Nachteile zu befürchten haben, kann auch auf eine Einwilligung nach § 26 Abs. 2 BDSG zurückgegriffen werden, da eine Freiwilligkeit dann vermutet wird. Dieser Anwendungsbereich beschränkt sich aber auf eng begrenzte Ausnahmefälle und birgt das Risiko in sich, dass der Arbeitnehmer von seinem Recht, die Einwilligung jederzeit zu widerrufen (Art. 7 Abs. 3 S. 1 DSGVO), Gebrauch macht.

Aus diesem Grund ist in der überwiegenden Anzahl der Fälle die Betriebsvereinbarung das vorzugswürdige Mittel. Diese kann nicht nur aufgrund der bestehenden Unterkomplexität der Datenschutzgrundverordnung und des BDSG zum Beschäftigtendatenschutz Rechtssicherheit schaffen, sondern auch aufgrund der in der Regel bestehenden Mitspracherechte des Betriebsrates eine einfache Möglichkeit der Regelung dieses Themenbereiches gewähren. Verhandelt werden muss mit dem Betriebsrat über den Einsatz solcher Technologien und die Reichweite von Auswertungen (insbesondere aufgrund § 87 Abs. 1 Nr. 6 BetrVG) ohnehin. Wird eine Einigung erzielt, lassen sich hierdurch auch die Datenverarbeitung legitimieren und differenzierte Regelungen schaffen, die das Datenschutzniveau auf Betriebsebene sogar steigern, da die besondere Unternehmens- und Betriebssituation berücksichtigt wird.

Eine Ausnahme stellen Bewerbungssituationen dar, da der Betriebsrat nur für Arbeitnehmer (§ 5 BetrVG) zuständig ist; in diesem Bereich müssen zwar mitunter Betriebsvereinbarungen über Auswahlrichtlinien

geschlossen werden, datenschutzrechtlich legitimierend wirken sie mangels normativer Wirkung für diesen Personenkreis nicht. Arbeitgeber sind daher gehalten, die Anforderungen des § 26 Abs. 1 S. 1 Var. 1 BDSG genau einzuhalten.

§ 2 *Automatisierte Entscheidungen auf Basis von People Analytics*

Ziel von People Analytics ist nicht nur, weitgehende Informationen über die Personalstruktur und Arbeitnehmer zu erhalten, sondern auch Betriebsabläufe im Personalmanagement zu effektivieren. Hierzu kann auch zählen, dass bestimmte (standardisierte) oder besonders arbeitsintensive Aufgaben nicht mehr durch Menschen, sondern vollständig automatisiert durch ein modernes Personalmanagementsystem erledigt werden. Bereits jetzt gibt es Software auf dem Markt, die je nach Kategorisierung der Mitarbeiter bestimmte Logiken auslöst. So beispielsweise eine automatisierte Gehaltserhöhung zum Jahresende bei „High Performern", um diese an das Unternehmen zu binden.[1246] Auch im Bereich des Bewerbermanagements werden zuweilen (insbesondere im angloamerikanischen Raum) Software-Lösungen vorgeschlagen, die eine automatische Vor- bzw. sogar Endauswahl[1247] der Bewerber vornehmen, ohne dass ein menschlicher Entscheider zwischengeschaltet wird.

Im Anwendungsbereich der Datenschutzgrundverordnung sind automatisierte Einzelfallentscheidungen, die gegenüber den Betroffenen eine rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen, grundsätzlich verboten (Art. 22 Abs. 1 DSGVO).[1248]

Zu prüfen ist im Folgenden, welche Maßnahmen im Rahmen von People Analytics von diesem Verbot erfasst sind und in welchen Situationen sich Arbeitgeber auf die in Art. 22 Abs. 2 DSGVO normierten Ausnahmetatbestände berufen können.

I. Bewerbermanagement

Das Bewerbermanagement dürfte der wichtigste Anwendungsbereich automatisierter Einzelfallentscheidungen sein, insbesondere wenn aufgrund

1246 *Sommer*, CuA 2017, 8 (10).
1247 Vgl. *Peck*, The Atlantic 2013 (Dezember 2013).
1248 Die Grundlagen wurden bereits im Abschnitt **D. § 1 V. 3** erläutert.

hoher Bewerberflut es für menschliche Entscheider faktisch unmöglich ist, alle Bewerbungen zu sichten und somit eine gerechte Auswahl vorzunehmen. So erhalten Großunternehmen mit mind. 500 Mitarbeiter im Schnitt 2.000 Bewerbungen pro Jahr, bei Unternehmen mit einer Mitarbeiteranzahl von 100 bis 499 sind es 374, während es bei klein- und mittelständischen Unternehmen mit 50-99 Arbeitnehmern 182 sind. Die Personalabteilung besteht dabei im Schnitt aus 13 Mitarbeitern bei Großunternehmen, 3 bei Unternehmen mit bis zu 499 Mitarbeitern und 1,9 bei Unternehmen mit 50 – 99 Angestellten.[1249] Hierbei ist zu bedenken, dass die HR-Verantwortlichen auch laufende Aufgaben wie Personalmanagement, -entwicklung und -abrechnung vorzunehmen haben. Bei beliebten Arbeitgebern wie Audi oder Google sehen die Zahlen noch deutlich drastischer aus: Bei Audi in Ingolstadt geht im Schnitt alle 52 Sekunden eine neue Bewerbung ein, das sind mehr als 100.000 pro Jahr; bei Google sind es 75.000 pro *Woche* (!).[1250] Automatisierte Lösungen zum Bewerbermanagement sind für solche Unternehmen unumgänglich.

Für den Einsatz der zur Bewältigung erforderlichen Software sind mehrere Szenarien für automatisierte Entscheidungen denkbar: Das Aussortieren von bereits formal ungeeigneten Kandidaten, ein Ranking aller eingehenden Bewerbungen und eine Bestenauslese[1251] sowie ein vollständig automatisiertes Einstellungsmanagement, völlig ohne menschliche Interaktion, wobei letzteres in Deutschland nicht nur aus datenschutzrechtlichen Gründen zum aktuellen Zeitpunkt noch reine Science-Fiction darstellen dürfte.[1252] Die anderen beiden untersuchten Szenarien werden aber teilweise schon in der Praxis angewandt und sind in vielen größeren Softwarelösungen bereits implementiert.[1253]

1249 So eine gemeinsame Studie von *Bitkom Research GmbH/Personio GmbH*, Woran scheitern Einstellungen?

1250 *Kontio*, Wie Bewerber die Robo-Recruiter überlisten können, 04.09.2018, abrufbar unter: https://www.handelsblatt.com/unternehmen/beruf-und-buero/the_shift/jobsuche-wie-bewerber-die-robo-recruiter-ueberlisten-koennen/22991974.html?ticket=ST-3589804-FXMKTFgbNgF1zeM14jmT-ap2 (letzter Abruf am: 06.03.2020).

1251 Hierzu grundlegend *Blum/Kainer*, PERSONALquarterly 2019, 22 sowie noch zum altem Datenschutzrecht *Groß/Gressel*, NZA 2016, 990 (992 f.).

1252 So aber bereits teilweise in den USA angewandt, vgl. *Peck*, The Atlantic 2013 (Dezember 2013).

1253 Siehe hierzu beispielsweise *Kontio*, Wie Bewerber die Robo-Recruiter überlisten können, 04.09.2018, abrufbar unter: https://www.handelsblatt.com/unternehmen/beruf-und-buero/the_shift/jobsuche-wie-bewerber-die-robo-recruiter-ueberlisten-koennen/22991974.html?ticket=ST-3589804-FXMKTFgbNgF1

1. Vorauswahl und automatische Absage an ungeeignete Bewerber

Wenn man bedenkt, dass bei 97 % der Fälle die Bewerber noch nicht einmal die Kriterien der Stellenanzeigen erfüllen und mit gleicher Quote zu hohe Gehaltsvorstellungen angegeben werden,[1254] lässt sich durch eine automatische Vorauswahl solch formal ungeeigneter Bewerber bereits eine Vielzahl der Kandidaten aussortieren. Hierdurch könnten sich die Verantwortlichen im Unternehmen mehr Zeit für die in Frage kommenden Bewerber nehmen und folglich eine bessere Auswahl treffen.

Aus datenschutzrechtlicher sowie nachgelagert betriebsverfassungsrechtlicher Sicht ist die Frage aufzuwerfen, ob ein solches Vorselektionssystem in der Praxis umsetzbar ist. Für die rechtliche Bewertung steht insbesondere das Verbot automatisierter Einzelfallentscheidungen aus Art. 22 DSGVO im Fokus, während nachgelagert eventuelle Mitspracherechte des Betriebsrats nach § 99 BetrVG voll automatisierten Absagevorgängen entgegenstehen könnten.

a) Datenschutzrechtlicher Rahmen

Für eine Anwendbarkeit des Art. 22 DSGVO bedarf es einer vollautomatischen Entscheidung durch das Bewerbermanagementsystem. Nicht vom Verbot erfasst ist es, wenn der Algorithmus lediglich Vorschläge für eine letztlich vom Menschen zu treffende Entscheidung erstellt, indem beispielsweise alle Bewerber nach der Passgenauigkeit auf das Stellenprofil sortiert werden, letztlich aber ein Mensch die Entscheidung „Absage" nach inhaltlicher Prüfung trifft. Voraussetzung ist allerdings, dass der menschliche Entscheider nicht nur den Vorschlag des Computers übernimmt und sich (wie sich aus dem Einschub „einschließlich Profiling" ergibt) auf die Bewertung des Systems verlässt, sondern selbst unter Berücksichtigung der Datengrundlage, d.h. den vom Bewerber eingereichten Daten, eine wertende Entscheidung vornimmt.[1255] Nur dann kann das Schutzziel des Art. 22 DSGVO erreicht werden, keine vom Computer inhaltlich verant-

---

zeM14jmT-ap2 (letzter Abruf am: 06.03.2020); ein Softwarebeispiel stellt die Bewerbermanagement-Software von *Persis* dar, vgl. https://www.persis.de/bewerbermanagement/ (letzter Abruf am: 06.03.2020); ähnliche Funktionen dürfte Prescreen anbieten, vgl. https://prescreen.io/de/bewerberverwaltung/ (letzter Abruf am: 06.03.2020).

1254 *Bitkom Research GmbH/Personio GmbH*, Woran scheitern Einstellungen?, S. 8.

1255 Siehe bereits **D. § 1 V. 3. c) aa)**.

worteten Entscheidungen zuzulassen, bei denen der Mensch zum Objekt der Datenverarbeitung wird, sofern sich Verarbeiter nicht auf einen Ausnahmetatbestand stützen können.[1256]

Obwohl die Ablehnung eines Arbeitsvertragsschlusses noch keine rechtliche Wirkung im Sinne des Art. 22 Abs. 1 DSGVO erzeugt, stellt dies bei objektiver Betrachtung eine erhebliche Beeinträchtigung für den Bewerber dar,[1257] sodass derartige Anwendungen vom Verbot des Art. 22 Abs. 1 DSGVO erfasst sind und im Folgenden zu prüfen ist, ob ein Ausnahmetatbestand des Abs. 2 einschlägig ist.

Während die Einwilligung in eine automatisierte Entscheidung im Bewerbungsprozess aus denselben Gründen ausscheidet wie eine „normale" Datenverarbeitung auf dieser Basis[1258] und ebenso wenig eine Erlaubnisnorm nach Art. 22 Abs. 2 lit. b DSGVO besteht, kommt es darauf an, ob die automatisierte Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist. Obwohl von der Erforderlichkeit für den „Abschluss des Vertrages" gesprochen wird, können auch ablehnende Entscheidungen von Art. 22 Abs. 2 lit. a DSGVO gerechtfertigt werden.[1259]

Inwieweit eine automatisierte Entscheidung im Rahmen der Bewerbervorauswahl erforderlich ist, hängt davon ab, bis zu welchem Maße dem Arbeitgeber eine Sichtung der Bewerbungsunterlagen durch menschliche Entscheider zumutbar ist.[1260] Sicherlich ist es im genannten Bespiel von Audi unzumutbar, dass die Personalverantwortlichen jede Minute eine Bewerbung sichten und hierüber entscheiden; umso mehr gilt dies für Google. Auch bei Großunternehmen mit im Schnitt 2.000 Bewerbungen handelt es sich immer noch (bei im Schnitt 230 Arbeitstagen pro Jahr) um knapp 8,7 Bewerbungen, die täglich (von 13 Personalverantwortlichen) zu bearbeiten wären. Auch in solchen Fällen ist die Zumutbarkeitsgrenze

1256 *Klar*, BB 2019, 2243 (2249).

1257 Wie hier *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 22 DSGVO Rn. 36.

1258 Zum Kriterium der Freiwilligkeit: **D. § 1 III. 2. a) bb) (2)**; vgl. aber *Götz*, Big Data im Personalmanagement, S. 177 zu einer "optionalen Teilnahme an automatisierten Bewertungssystemen. *Götz* übergeht leider das Problem, dass Bewerber dennoch unfreiwillig an der Maßnahme teilnehmen werden, da sie Benachteiligungen befürchten, wenn sie die Option nicht auswählen.

1259 *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 22 DSGVO Rn. 29; *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 22 DSGVO Rn. 40.

1260 Zum Begriff der Erforderlichkeit im Detail: **D. § 1 V. 3. d) aa)**.

überschritten, wenn man bedenkt, dass die Personalakquise nur ein Bruchteil der Personalarbeit im Unternehmen darstellt. Selbst die Bearbeitung von 1,6 Bewerbungen (bei drei Personalverantwortlichen) bei mittleren Unternehmen oder 0,8 Bewerbungen (bei 1,9 Personalverantwortlichen) bei kleinen Unternehmen pro Tag dürfte die Zumutbarkeitsgrenze sprengen. Dies wäre im Schnitt über alle Unternehmensgrößen alle zwei Tage eine Bewerbung, die pro HR-Mitarbeiter zu bearbeiten ist, wobei nicht berücksichtigt wird, dass diese Zahlen nur Mittelwerte darstellen, nicht alle Abteilungsmitarbeiter auch für das Bewerbermanagement zuständig sind und bei (neuen) Stellenausschreibungen deutliche Spitzen auftreten, während z.B. bei Initiativbewerbungen im Gegensatz in aller Regel nur die einzelne Bewerbung geprüft werden muss.

Im Allgemeinen ist daher eine Bewerbervorauswahl als erforderliche Maßnahme für den Abschluss eines Arbeitsvertrags vom Verbot der automatisierten Entscheidung nach Art. 22 Abs. 2 lit. a DSGVO ausgenommen. Dies gilt nach den bisherigen Ausführungen allerdings nur soweit als die Datenauswertung und -entscheidung im Einzelfall durch einen menschlichen Entscheider für den Arbeitgeber unzumutbar ist. Ist nur eine Stelle ausgeschrieben und bewerben sich hierfür zwischen 10 und 15 Bewerber bei einem Personalverantwortlichen in einem kleineren Unternehmen, so steht die Bearbeitung dieser Bewerbungen kurzfristig im Vordergrund – eine automatisierte Vorauswahl ist nicht erforderlich. Letztendlich hängt es vom Einzelfall ab, ob computergestützte Vorauswahlen geboten sind oder nicht.

Um den Anforderungen des Verhältnismäßigkeitsgrundsatzes nachzukommen, muss die Anwendung des Systems gestuft erfolgen, d.h. datenschutzrechtlich weniger einschneidende Maßnahmen müssen vorrangig angewandt werden, während eine Entscheidung mittels Profiling als eine ins Persönlichkeitsrecht intensiver eingreifende Maßnahme erst in einem zweiten Schritt erfolgen darf.

Zunächst muss daher bei einer angenommenen Bewerberflut eine automatische Vorselektion anhand rein formaler Kriterien erfolgen. Erst wenn hiernach weiterhin eine derart große Anzahl an Stellenbewerbern übrigbleibt, dass auch diese nicht durch menschliche Entscheider bewältigbar ist, kommt eine weitere Selektion mittels Profiling- oder Scoring-Maßnahmen in Betracht.

Der Arbeitgeber muss im Rahmen dessen die betroffenen Bewerber genau über das Vorliegen und die Reichweite einer automatisierte Entscheidungsfindung sowie über die involvierte Logik und angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person, informie-

ren (Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g DSGVO). Ein Auskunftsrecht mit demselben Inhalt besteht aus Art. 15 Abs. 1 lit. h DSGVO.

Nach Art. 22 Abs. 3 DSGVO hat die betroffene Person zudem das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts sowie auf Anfechtung der Entscheidung.

Zwar schreibt Art. 35 DSGVO für den Fall der Aussortierung bei mangelnder formaler Qualifikation nicht explizit eine Datenschutzfolgenabschätzung vor, da hierfür ein Profiling erforderlich wäre (vgl. insofern auch Erwägungsgrund 91 S. 2: „*Eine Datenschutz-Folgenabschätzung sollte auch durchgeführt werden, wenn die personenbezogenen Daten für das Treffen von Entscheidungen auf bestimmte natürliche Personen im Anschluss an eine systematische und eingehende Bewertung persönlicher Aspekte natürlicher Personen auf der Grundlage eines Profilings dieser Daten oder im Anschluss an die Verarbeitung besonderer Kategorien von personenbezogenen Daten […] [erfolgt].*“).

Dennoch ist davon auszugehen – auch wenn nicht vom Regelbeispiel des Art. 35 Abs. 3 lit. a DSGVO erfasst[1261] –, dass Art. 35 Abs. 1 DSGVO einschlägig ist. Hiernach ist eine Datenschutz-Folgenabschätzung erforderlich, wenn diese Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat:

Bei der Bewerbung für ein Arbeitsverhältnis steht in aller Regel die Haupteinnahmequelle des Bewerbers im Vordergrund (Umstände sowie hohes Risiko) und bei solchen Systemen handelt es sich um neuartige Technologien im Personalbereich, die erst durch die zunehmende Verarbeitungsgeschwindigkeit ermöglicht wurden (Verwendung neuer Technologien). Fehler, die zu einer Nicht-Berücksichtigung führen, können gravierende Folgen für den einzelnen Betroffenen haben, wodurch ein hohes Risiko besteht. Es ist daher geboten, die möglichen Folgen und Risiken des Einsatzes eines solchen Systems exakt zu eruieren und insbesondere die Fehleranfälligkeit (z.B. beim Parsen von CVs oder sonstigen Unterlagen) zu bewerten, bevor dieses zum Einsatz kommt.

1261 Siehe bereits **D. § 1 V. 4.**

b) Betriebsverfassungsrechtlicher Kontext

Aus betriebsverfassungsrechtlicher Hinsicht stellt sich die Frage der Umsetzbarkeit aufgrund der Mitbestimmungsrechte bei personellen Maßnahmen aus § 99 BetrVG. Gem. § 99 Abs. 1 BetrVG hat in Unternehmen mit mehr als 20 wahlberechtigten Arbeitnehmern der Arbeitgeber den Betriebsrat *vor jeder Einstellung […] zu unterrichten, ihm die erforderlichen Bewerbungsunterlagen vorzulegen und Auskunft über die Person der Beteiligten zu geben*. Im Anschluss muss er die Zustimmung des Betriebsrats zu der geplanten Maßnahme einholen.

Der Arbeitgeber hat die Bewerbungsunterlagen *aller*[1262] Bewerber an den Betriebsrat zu übergeben, wozu das Bewerbungsschreiben mit allen Anlagen und die vom Arbeitgeber zum Einstellungsverfahren angefertigten eigenen Dokumente gehören.[1263]

Die Unterrichtung muss vor der jeweiligen Maßnahme stattfinden, wobei das Gesetz keinen konkreten Zeitpunkt angibt. Zweckmäßig ist es, den Betriebsrat so früh wie möglich zu informieren. Spätestens (wie sich aus § 99 Abs. 3 BetrVG ergibt) muss die Unterrichtung jedoch eine Woche vor der geplanten Einstellung stattfinden.[1264] Die Informationspflicht wird allerdings erst dann ausgelöst, wenn der Arbeitgeber sich darüber schlüssig geworden ist, welchen der Stellenbewerber er einstellen möchte.[1265]

Sinn und Zweck der Vorschrift ist nicht der Schutz des betroffenen Bewerbers, sondern der der übrigen Arbeitnehmer im Betrieb, andernfalls würde ein Zustimmungserfordernis zu einer Einstellung kaum Sinn ergeben.[1266]

Die Auskunftspflicht des Arbeitgebers gegenüber dem Betriebsrat erstreckt sich auf jene Bewerber, die er nicht berücksichtigen will.[1267] Argument ist, dass das Einstellungsverfahren mit der Auswahl durch den

1262 BT-Drs. IV/1786, S. 51.

1263 BAG, Beschl. v. 03.122.1985 – 1 ABR 72/83, AP BetrVG 1972 § 99 Nr. 29 unter II. 2. der Gründe; Beschl. v. 28.06.2005 – 1 ABR 26/04, NZA 2006, 111 (113) Rn. 23 m.w.N.

1264 ErfK/*Kania*, § 99 BetrVG Rn. 22.

1265 BAG, Beschl. v. 18.07.1978 – 1 ABR 8/75, AP BetrVG 1972 § 99 Nr. 7 unter II. 1. a) der Gründe.

1266 Vgl. Richardi/*Thüsing*, § 99 BetrVG Rn. 29.

1267 So bereits BAG, Beschl. v. 19.05.1981 – 1 ABR 109/78, AP BetrVG 1972 § 118 Nr. 18; Beschl. v. 03.122.1985 – 1 ABR 72/83, AP BetrVG 1972 § 99 Nr. 29; Beschl. v. 28.06.2005 – 1 ABR 26/04, NZA 2006, 111 (114) Rn. 25; ferner BeckOK ArbR/*Mauer*, § 99 BetrVG Rn. 13 m.w.N.

Arbeitgeber noch nicht erledigt ist und der Betriebsrat – im Falle der Verweigerung der Zustimmung – auch die Möglichkeit im Rahmen von § 99 BetrVG hat, *„Anregungen zu geben und Gesichtspunkte vorzubringen, die aus seiner Sicht für die Berücksichtigung eines anderen als des vom Arbeitgeber ausgewählten Stellenbewerbers sprechen.“*[1268] Diese weite Auffassung des BAG wird in der Literatur insbesondere hinsichtlich der offensichtlich ausscheidenden (z.B. wegen fehlenden Qualifikationsvoraussetzungen[1269]) Bewerber kritisiert.[1270] So wird überwiegend vertreten, dass diese Personen bereits nicht zum Kreis der Beteiligten gehören.[1271]

Die „Maßnahme“ stellt die Einstellung des schlussendlich durch den Arbeitgeber ausgewählten Arbeitnehmers selbst dar. Fraglich ist, inwiefern ein Arbeitgeber einem offensichtlich ungeeigneten oder chancenlosen Stellenbewerber bereits vor der Information und Zustimmung des Betriebsrats zum letztendlich gewählten Bewerber eine Absage erteilen darf. Im oben zitierten Urteil aus dem Jahre 1978[1272] stellte das Bundesarbeitsgericht klar, dass die Auswahl unter den Stellenbewerbern Sache des Arbeitgebers ist und erst wenn der Arbeitgeber sich für einen oder mehrere entschieden hat, er beim Betriebsrat um dessen Zustimmung zu der vorgesehenen Einstellung nachsuchen und ihm die dazu erforderlichen Auskünfte geben kann.

Obgleich der Betriebsrat über offensichtlich nicht in Betracht kommende Bewerber informiert werden muss, hat dieser lediglich ein Vetorecht betreffend die Einstellung des vom Arbeitgeber gewählten Kandidaten, da er nach § 99 Abs. 1 BetrVG nur die Zustimmung zur personellen Einzelmaßnahme verweigern kann. Er kann hingegen nicht die Einstellung eines bestimmten Bewerbers verlangen.[1273] Aus diesem Grund kann es dem Arbeitgeber auch nicht verwehrt sein, entsprechenden Stellenbewerbern eine Absage zu erteilen, wenn der Arbeitgeber diese ohnehin nicht berücksichtigen würde. Hieran ändern auch die o.g. Ausführungen zur Möglichkeit des Betriebsrats nichts, Anregungen zur Einstellung eines anderen Bewerbers zu äußern, der nach Auffassung des Betriebsrats besser geeignet

1268 BAG, Beschl. v. 19.05.1981 – 1 ABR 109/78, AP BetrVG 1972 § 118 Nr. 18 unter I. der Gründe.
1269 BAG, Beschl. v. 21.10.2014 – 1 ABR 10/13, NZA 2015, 311 (313) Rn. 29.
1270 *Gragert*, ArbRAktuell 2015, 135.
1271 So bspw. Richardi/*Thüsing*, § 99 BetrVG Rn. 156 m.w.N.; ähnlich MHdB-ArbR/*Lunk*, § 340 Die Mitbestimmung bei der Einstellung, Rn. 50.
1272 BAG, Beschl. v. 18.07.1978 – 1 ABR 8/75, AP BetrVG 1972 § 99 Nr. 7.
1273 Richardi/*Thüsing*, § 99 BetrVG Rn. 204 m.N.; MHdB-ArbR/*Lunk*, § 340 Die Mitbestimmung bei der Einstellung, Rn. 60.

ist. Zwar wird hierdurch die Effektivität der „Anregung" geschmälert, dennoch betrifft das Zustimmungsverfahren nach § 99 BetrVG nur die konkret ausgewählte Person durch den Arbeitgeber.

Betriebsverfassungsrechtlich wird daher eine automatisierte Vorauswahl bzw. ein automatisiertes Vorausscheiden von offensichtlich ungeeigneten Bewerbern nicht durch die Mitspracherechte aus § 99 Abs. 1 BetrVG verhindert. In jedem Falle ist der Betriebsrat aber über diese Teilnehmer des Bewerbungsverfahrens sowie die Gründe für die Aussortierung nach aktueller Rechtsprechung des BAG zu informieren, damit dieser seine Entscheidung über die Zustimmung oder Ablehnung mit einer breiteren Informationsbasis treffen kann sowie dem Arbeitgeber Gegenvorschläge unterbreiten kann.

Da der Betriebsrat aber ebenso wie eine Personalabteilung bei einer Bewerberflut (und nur in diesem Fall kommt diese Problematik überhaupt in Betracht) mit der Sichtung aller Bewerbungsunterlagen maßlos überfordert sein wird, werden in der Praxis häufig andere Absprachen betriebsintern getroffen.[1274]

Aus praktischen Gründen empfiehlt es sich, eine Absprache über die (beim Einsatz von Scoring) im zweiten Schritt anwendbaren Auswahlrichtlinien gem. § 95 BetrVG (dazu nachfolgend **2. b**) in diesem Abschnitt) zu treffen. Diese sollte bereits bei Verfassung der Betriebsvereinbarung, spätestens aber vor Einführung eines solchen Systems vorliegen. Durch eine solche können eventuelle Streitigkeiten im Rahmen des Zustimmungsverfahrens nach § 99 BetrVG, die dadurch entstehen könnten, dass sich der Betriebsrat durch die automatische Vorselektion übergangen fühlt, vermieden werden.

Zu beachten ist, dass der Betriebsrat zudem bereits in der Planungs- und Umsetzungsphase ein Mitbestimmungsrecht nach § 94 Abs. 1 BetrVG hat, wenn im Rahmen einer Bewerbungsplattform o.ä. standardisierte Fragebögen (auch in digitaler Form) zum Einsatz kommen.[1275]

c) Ergebnis

Sowohl aus datenschutzrechtlicher als auch betriebsverfassungsrechtlicher Sicht ist eine computergestützte Selektion der geeigneten Bewerber grund-

1274 Vgl. MHdB-ArbR/*Lunk*, § 340 Die Mitbestimmung bei der Einstellung, Rn. 50.
1275 Zur Reichweite des Mitbestimmungsrechts aus § 94 Abs. 1 BetrVG, **D. § 2 II. 2. a**).

sätzlich möglich. Voraussetzung ist, dass (a) die automatische Entscheidungsfindung gem. Art. 22 Abs. 2 lit. a DSGVO erforderlich ist und (b) der Betriebsrat auch über die aussortierten Bewerber umfassend informiert wird. Erforderlich ist eine Vorselektion dann, wenn das Unternehmen eine derart hohe Anzahl an Bewerbungen bekommt, dass es diesem nicht mehr zumutbar ist, alle Bewerbungen manuell zu prüfen und daher – um eine Berücksichtigung aller Bewerber zu ermöglichen – eine computergestützte Auswahl stattfindet.

Die Information des Betriebsrats kann praktischerweise über einen entsprechenden Zugriff auf das Auswahlsystem ermöglicht werden, wobei berücksichtigt werden muss, dass ein Bewerber der Weiterleitung seiner Bewerbungsunterlagen an den Betriebsrat widersprechen kann[1276] und im System für diesen Fall ein Sperrvermerk eingetragen werden müsste, dass der Betriebsrat auf diese Daten keinen Zugriff erhält. Durch einen solchen elektronischen Zugriff umginge man auch den in der rechtswissenschaftlichen Literatur bestehenden Streit hinsichtlich der Reichweite des Informationsrechts des Betriebsrats. Ohnehin besteht für die Mitglieder des Betriebsrats nach § 99 Abs. 1 S. 3 BetrVG eine Schweigepflicht betreffend die hierdurch erlangten Kenntnisse über die Bewerber.

Empfehlenswert, aber nicht zwingend erforderlich, ist eine betriebsinterne Absprache über das Vorgehen bei offensichtlich ungeeigneten Bewerbern; in diesem Rahmen hat der Betriebsrat zwar kein Mitspracherecht bzgl. der Absage, sodass solche auch schon vor Abschluss des Verfahrens automatisch versandt werden dürfen. Dennoch entwertet dies die Möglichkeiten des Betriebsrats, einen anderen, nach seiner Sicht geeigneteren Bewerber vorzuschlagen. Das könnte im Rahmen der Zustimmung zu Personalmaßnahmen nach § 99 Abs. 1 BetrVG zu unnötigen Verzögerungen und Ungereimtheiten führen, wenn beispielsweise der Betriebsrat seine Zustimmung zu einem gut geeigneten Bewerber nur deshalb verneint, weil er sich übergangen fühlt und zunächst ein Zustimmungsersetzungsverfahren nach § 99 Abs. 4 BetrVG geführt werden muss, auch wenn Maßnahme ggf. vorläufig nach § 100 BetrVG dennoch unmittelbar durchführbar ist.

1276 Richardi/*Thüsing*, § 99 BetrVG Rn. 171 m.w.N.

2. Ranking und automatische Bestenvorauswahl

Bleiben nach einem ersten (formalen) Selektionsvorgang so viele Bewerber übrig, dass eine Bearbeitung aller Bewerber durch HR-Verantwortliche immer noch unzumutbar ist und daher ausscheidet, können in einem weiteren Schritt weitere Maßnahmen erforderlich sein, die Bewerbermenge auf ein human bearbeitbares Maß zu senken. Hierfür kann ein Scoring und Ranking, verbunden mit einer Bestenvorauswahl dienen.

Alle nach Phase 1 übriggebliebenen Bewerber werden danach in einem weiteren computerbasierten Verfahren auf ihre Passgenauigkeit für die vorhergesehene Stelle bewertet und benotet. Auf Basis dieses Scores wird dann eine Bestenauswahl vorgenommen, dergestalt, dass die Bewerberanzahl so weit reduziert wird, dass eine manuelle Bearbeitung der übriggebliebenen Stellenbewerber möglich ist.

a) Datenschutzrechtlicher Rahmen

Aus datenschutzrechtlicher Hinsicht besteht nun ein beachtlicher Unterscheid zur formalen Vorselektion. Nun findet ein Profiling / Scoring im Sinne des Art. 4 Nr. 4 DSGVO statt, welches bedeutend stärker in die Persönlichkeitsrechte der betroffenen Bewerber eingreift als die reine Selektion nach formalen Kriterien. Nun werden die perspektivische Arbeitsleistung und das Verhalten durch einen Algorithmus bewertet und daraus eine Vorhersage in Form eines Wahrscheinlichkeitswerts (*Scores*) gebildet, anhand dessen dem HR-Verantwortlichen eine vorsortierte Liste angezeigt wird. Bewerber, die bei dieser Vorsortierung einen unteren Rang erreichen, könnten automatisch aussortiert oder – was einer automatischen Aussortierung gleichkommt[1277] – vom Personalverantwortlichen aufgrund des schlechten Scores nicht mehr beachtet werden.

aa) Anforderungen an das Bewerberscoring

Wie bereits auf den Seiten 321 ff. ausführlich dargestellt, ist ein Bewerberscoring grundsätzlich zulässig, sofern es auf Daten basiert, die zulässigerweise erhoben wurden. Es ist zu beachten, dass die Anzahl der „weichen"

1277 Anm.: Mangels inhaltlicher Entscheidung eines Menschen, hierzu **D. § 1 V. 3. c) aa)**.

Fakten, also Daten zur Persönlichkeit des Bewerbers, stark von der zu besetzenden Stelle abhängig ist. Während in unteren Hierarchieebenen (z.B. beim Arbeitnehmer in der Logistik oder Fertigung am Förderband) es zunächst kaum auf Führungskompetenzen ankommen dürfte, sieht dies beim Gruppen- oder Abteilungsleiter, der eine Personalverantwortung hat, bereits anders aus. Deutlich weitgehender dürfte das Fragerecht des Arbeitgebers bei Managern sein, die auch als leitende Angestellte im Sinne des § 5 Abs. 3 BetrVG zu qualifizieren sind.

Keinesfalls darf ein Totalabbild der Persönlichkeit als Grundlage für die automatisierte Entscheidung herangezogen werden. Bei allem, was kein solches Totalabbild darstellt, ist eine Einzelfallabwägung, basierend auf den Anforderungen der konkret zu besetzenden Stelle erforderlich.

Im Rahmen des Scorings muss darauf geachtet werden, dass in den Algorithmus nur solche Daten einfließen, die tatsächlich für die Generierung des Scores notwendig sind. Zudem muss der Score grundsätzlich zu korrekten Ergebnissen führen, wobei ausreichend ist, dass eine gewisse „Basisrationalität" besteht.[1278] Über die grundlegende Funktion des Scoring-Verfahrens hat der Arbeitgeber die Bewerber auch gem. Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g DSGVO aufzuklären, wobei er jedoch nicht die konkrete Scoring-Formel herausgeben muss (siehe zum Ganzen bereits S. 306 ff.).

bb) Anforderungen an die automatische Auswahlentscheidung

Im Anschluss an das Scoring und Ranking der Bewerber erfolgt eine automatische Bestenvorauswahl. Diese findet nicht nur dann statt, wenn der Computer nur bspw. die 10, 50 oder 100 besten Kandidaten anzeigt, sondern auch dann, wenn die Liste alle Bewerber enthält, die Personalverantwortlichen jedoch nur noch einen Bruchteil aller Bewerber aus den Top-Rängen selbst sichten. Auch in letzterem Fall entscheidet nämlich faktisch der vom Computer generierte Score über die Berücksichtigung im Bewerbungsverfahren und die Entscheidung bezüglich der anderen Bewerber wird nicht mehr menschlich verantwortet.[1279]

Es macht also aus datenschutzrechtlicher Hinsicht keinen Unterschied, ob direkt die Absagen an die nicht-berücksichtigten Stelleninteressenten versandt werden oder ein Mensch zum Ende des Bewerbungsprozesses

1278 *Gerberding/Wagner*, ZRP 2019, 116 (119).
1279 Hierzu bereits **D. § 1 V. 3. c) aa)**.

noch den entsprechenden Button klickt und den Vorschlag des Computers ohne weitere Prüfung übernimmt.

Daher muss für ein solches Verfahren der in Art. 22 Abs. 2 lit. a DSGVO statuierte Erforderlichkeitsgrundsatz gewahrt bleiben (siehe insofern bereits die Ausführungen unter **1. a**) dieses Abschnitts). Auf dieser Grundlage dürfen das Scoring und Ranking als eine Entscheidung vorbereitende Maßnahme auf alle Bewerber angewandt werden (hierzu bereits S. 321 ff.). Soweit es den Personalverantwortlichen aber zumutbar und möglich ist, die Bewerbungen nochmals zu sichten und auf Basis der Datengrundlage und nicht ausschließlich des Scores und Rankings zu entscheiden, muss dies auch vorgenommen werden, da dann eine vollautomatisierte Einzelfallentscheidung nicht erforderlich ist.

Pauschale Grenzen können jedoch nicht genannt werden. Letztendlich hängt es vom Einzelfall (insbesondere Größe der Personalabteilung sowie sonstige Arbeitsbelastung der Personalverantwortlichen) ab, welche Untergrenzen an Bewerbungen für die Automatisierung gelten.

b) Betriebsverfassungsrechtlicher Kontext

Zu den in Ziff. 1 dieses Abschnitts genannten Rechte des Betriebsrats kommen beim Einsatz von Scoringverfahren noch Mitbestimmungsrechte bei der Festlegung allgemeiner Beurteilungsgrundsätze und Auswahlrichtlinien nach den §§ 94 und 95 BetrVG hinzu. Diese Mitbestimmungsrechte entstehen nicht erst im konkreten Bewerbungsverfahren, sondern bereits in der Planungsphase vor Einführung eines solchen Systems. Für das Scoring müssen vorab bestimmte Grundsätze und Kriterien festgelegt werden, nach denen die Bewerber bewertet werden sollen. Diese stellen allgemeine Beurteilungsgrundsätze nach § 94 Abs. 2 sowie, falls auf dieser Basis dann auch eine Auswahl stattfindet, Auswahlrichtlinien nach § 95 BetrVG dar.[1280]

Zu beachten ist, dass der Arbeitgeber dem Betriebsrat nicht nur die Bewerbungsunterlagen aller Bewerber mitteilen muss, sondern auch den vom System generierten Score und Rang in der Liste.[1281] Nur so kann

---

1280 Zum Ganzen siehe **D. § 2 II. 2. b**) und **D. § 2 II. 3**.

1281 Der Arbeitgeber ist verpflichtet, alle Unterlagen anlässlich der Bewerbung, also auch solche Unterlagen, die der Arbeitgeber anlässlich der Bewerbung über die Person erstellt hat, dem Betriebsrat zu übermitteln, vgl. Richardi/*Thüsing*, § 99 BetrVG Rn. 166 m.w.N. aus der Rechtsprechung.

der Betriebsrat nachvollziehen, weshalb ein Arbeitgeber nur bestimmte Stelleninteressenten berücksichtigt und andere außer Betracht bleiben. Ebenfalls sollten bereits im Vorfeld entsprechende Absprachen mit dem Betriebsrat getroffen werden.

c) Ergebnis

Ein Ranking mit automatischer Bestenvorauswahl ist aus datenschutzrechtlicher Hinsicht grundsätzlich zulässig, sofern die Anzahl der eingehenden Bewerbungen ein solches Vorgehen erforderlich macht. Dies ist insbesondere dann der Fall, wenn nach einer ersten Selektion anhand formaler Kriterien (wie z.B. Nichterfüllung von Qualifikationsvoraussetzungen) als milderes Mittel weiterhin so viele Bewerbungen im Pool bleiben, dass es den menschlichen Entscheidern unzumutbar ist, die übrigen Bewerbungen in angemessener Zeit zu sichten und eine ordnungsgemäße Auswahl zu treffen.

In diesem Fall müssen dem Betriebsrat alle Unterlagen, somit auch der konkrete Score und Rang für die jeweiligen Bewerber, übermittelt werden, wobei dies bei rein digitalen Bewerbungen auch durch einen (eingeschränkten[1282]) Zugriff auf das Bewerbermanagementsystem erfolgen kann.[1283]

3. Vollständig automatisiertes Einstellungsmanagement

Wie sich aus den bisherigen Ausführungen unter Ziff. 1 und 2 ergibt, ist sowohl aus datenschutz- als auch betriebsverfassungsrechtlicher Hinsicht (Zustimmungserfordernis gem. § 99 BetrVG) ein vollständig automatisiertes Einstellungsmanagement unzulässig. In keinem Falle kann es erforderlich im Sinne von Art. 22 Abs. 2 lit. a DSGVO sein, dass eine Einstellung vollautomatisch abläuft, ohne dass ein menschlicher Entscheider eine zu-

---

1282 Der Bewerber hat die Möglichkeit, einer Weiterleitung seiner Unterlagen an den Betriebsrat zu widersprechen, vgl. Richardi/*Thüsing*, § 99 BetrVG Rn. 171 m.w.N.

1283 Grundsätzlich muss ein Arbeitgeber dem Betriebsrat die Unterlagen vorlegen, also physikalisch zur Verfügung stellen. Solange die Unterlagen aber ausschließlich digital vorlegen, muss der Arbeitgeber diese nicht extra zur Vorlage anfertigen (ErfK/*Kania*, § 99 BetrVG Rn. 21). Die Ermöglichung des Zugriffs erfüllt daher die Anforderungen des § 99 BetrVG.

mutbare Anzahl Bewerbungen noch selbst prüft. Während die Einstellung des konkret ausgewählten Bewerbers aufgrund der ausschließlich positiven Wirkung nicht vom Verbot des Art. 22 Abs. 1 DSGVO erfasst ist[1284], muss den anderen Bewerbern aber auch eine Absage erteilt werden. Zumindest hierfür muss ein menschlicher Entscheider eingeschaltet werden, der ein Minimum an Bewerbern noch manuell prüft.

Zulässig ist es im Rahmen des Entscheidungsprozesses jedoch, die in Frage kommenden Bewerber vollautomatisch zu einem Bewerbungsgespräch einzuladen und entsprechende Termine automatisch durch das System mit den Entscheidungsträgern abstimmen zu lassen, sofern die Vorauswahl bereits getroffen wurde und dadurch gegenüber den restlichen Bewerbern keine Entscheidung im Sinne des Art. 22 Abs. 1 DSGVO getroffen wird, die rechtliche Wirkung oder ähnliche Wirkungen entfalten würde. Die Einladung selbst stellt keine Entscheidung mit rechtlicher Wirkung oder ähnlicher Beeinträchtigung dar, sodass dieser Automatismus nicht vom Verbot der automatisierten Einzelfallentscheidung erfasst ist.

II. Laufendes Beschäftigungsverhältnis

Automatisierte Einzelfallentscheidungen sind nicht nur im Rahmen des Bewerbungsprozesses denkbar, sondern auch im laufenden Beschäftigungsverhältnis. So könnten auf Basis generierter Scores oder Leistungsbewertungen am Ende des Jahres automatisch Gehaltserhöhungen an High-Performer ausbezahlt oder bestimmte Arbeitnehmer für Weiterbildungen automatisch angemeldet werden. Aus praktischer Hinsicht könnte das so weit führen, dass Versetzungen oder Kündigungen durch das System bei längerfristigen Minderleistungen „ausgesprochen" werden. All diese Maßnahmen müssen aus datenschutzrechtlicher Hinsicht am Maßstab des Art. 22 DSGVO gemessen werden. Im Folgenden sollen diese Anwendungsszenarien aus datenschutzrechtlicher sowie betriebsverfassungsrechtlicher Sicht auf ihre Zulässigkeit untersucht werden.

a) Gehaltsveränderungen / Festlegung variabler Lohnbestandteile

Wie bereits kurz dargestellt, könnten automatisierte Prozesse dazu genutzt werden, den variablen Lohn von Arbeitnehmern aufgrund digitalisierter

1284 Siehe hierzu **D. § 1 V. 3. c) bb)**.

Zielvereinbarungen, Scores oder Umsatzzahlen zum jeweiligen Stichtag automatisiert festzulegen oder eventuelle Gehaltsveränderungen (z.B. eine automatische Erhöhung bei High-Performern) am Jahresende vollständig automatisch festgesetzt werden.

aa) Datenschutzrechtlicher Rahmen

Aus datenschutzrechtlicher Sicht muss zwischen dem Prozess der Erhebung und Verarbeitung der notwendigen Daten für die Entscheidung (§ 26 Abs. 1 S. 1 BDSG) sowie der Automation des Entscheidungsprozesses selbst (Art. 22 DSGVO) unterschieden werden.

(1) Festlegung und Auszahlung variabler Vergütungen

Sollen variable Gehaltsbestandteile aufgrund von Umsatzzahlen ausbezahlt werden, so handelt es sich noch nicht um ein Profiling im Sinne des Art. 4 Nr. 4 DSGVO, da keine persönlichen Aspekte, die sich auf eine natürliche Person beziehen, bewertet werden. Die Verwendung dieser Zahlen ist aus datenschutzrechtlicher Hinsicht völlig unproblematisch, da es sich nicht um personenbezogene Daten handelt. Erst durch die Verknüpfung mit dem jeweiligen Datensatz des zu bezahlenden Arbeitnehmers erhalten diese Daten eine datenschutzrechtliche Relevanz, da sie dann personenbezogen werden, insbesondere, wenn sie als Grundlage zur Bestimmung des variablen Vergütungsanteils einer natürlichen Person dienen.

Dennoch unterliegt diese Maßnahme nicht dem Verbot des Art. 22 Abs. 1 DSGVO, da bereits keine *Entscheidung* mit rechtlicher Wirkung oder ähnlicher Beeinträchtigung vorliegt: In diesem Fall wird lediglich ausgeführt, was zuvor vertraglich vereinbart wurde.[1285] Der Betroffene benötigt für diesen Prozess auch nicht den Schutz des Art. 22 Abs. 3 DSGVO, da er bei einer Falschberechnung durch den Computer (wenn z.B. falsche Umsatzzahlen als Grundlage herangezogen werden), bereits aus dem Arbeitsvertrag ein Recht auf Auszahlung des korrekten variablen Vergütungsbestandteils hat.

Etwas anderes kann gelten, wenn auf Basis von Zielvereinbarungen und Scores die Festlegung des variablen Bestandteils erfolgt. In aller Regel

1285 *Klar*, BB 2019, 2243 (2249); *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 19.

besteht zwar auch hier eine Abmachung, wie hoch der zu zahlende Anteil bei einer gewissen Bewertung ist, die Bewertung selbst, die Basis der Entscheidung ist, obliegt aber dem Arbeitgeber bzw. beim Scoring dem Computeralgorithmus. Maßgeblich ist, dass der Score vollautomatisch erstellt wird und die Entscheidung über die Auszahlung beinhaltet. Bei letzterem handelt es sich daher um eine von Art. 22 Abs. 1 DSGVO erfasste Entscheidung, da ohne Dazwischenschalten eines Menschen automatisch die variable Vergütung ausbezahlt wird. In solchen Fällen muss ein Recht auf Darlegung des eigenen Standpunkts und Anfechtung der Entscheidung nach Art. 22 Abs. 3 DSGVO gewährt werden.

Dies gilt nicht nur für eine vollautomatische Entscheidung, sondern auch für eine menschliche Entscheidung, die allein darauf fußt, dass der Score als Grundlage für die Auszahlung des variablen Vergütungsbestandsteils verwendet wird, denn dann wird der menschliche Entscheider nur noch formal eingeschaltet und prüft nicht mehr das Ergebnis der Entscheidung auf Basis der Datengrundlage.[1286] Der betroffene Arbeitnehmer stünde schutzlos dar, wenn er den Score, der als Grundlage der Entscheidung diente, nicht anfechten könnte und kein Recht auf Darlegung des eigenen Standpunkts bekäme.

Da die Nicht-Ausbezahlung der vollen variablen Vergütung in aller Regel eine erhebliche Beeinträchtigung darstellt (Art. 22 Abs. 1 DSGVO), unterliegt diese Maßnahme dem grundsätzlichen Verbot der automatisierten Einzelfallentscheidung. Fraglich ist, ob die Ausnahme der Erforderlichkeit nach Art. 22 Abs. 2 lit. a DSGVO einschlägig ist. Hierfür wäre es erforderlich, dass ein derart großer Datensatz als Grundlage dient, dass es für einen menschlichen Entscheider unzumutbar ist, diesen manuell abzuarbeiten. Dies wird in der Regel nicht der Fall sein.

Selbst dann dürfte aber eine vollautomatisierte Entscheidung, dergestalt, dass kein Mensch zumindest den Computervorschlag noch genehmigt, unzulässig sein. Jedenfalls den fachverantwortlichen Bereichs-/Gruppen-/Abteilungsleitern ist es zumutbar, die computergenerierten Scores zumindest noch auf ihre Plausibilität zu überprüfen. Zu weitgehend wäre es aber, diesen abzuverlangen, dass bei sehr komplexen Beurteilungsalgorithmen (falls solche notwendig sind, um eine faire Beurteilung zu gewährleisten), der Entscheider die gesamte Datengrundlage nochmals überprüfen muss; insofern ist eine automatisierte Entscheidung notwendig und unter der Ausnahme des Art. 22 Abs. 2 lit. a unter den in **D. § 1 V. 3. d) aa)** entwickelten Maßstäben zu rechtfertigen.

1286 Siehe hierzu **D. § 1 V. 3. c) aa)**.

(2) Berechnung und Auszahlungen von Gehaltserhöhungen

Etwas anderes gilt, wenn am Jahresende Gehaltserhöhungen automatisch festgelegt und ausbezahlt werden sollen. Eine Gehaltserhöhung stellt ein (ggf. konkludentes) Angebot des Arbeitgebers an den Arbeitnehmer dar, das durch vorbehaltslose Weiterarbeit und Entgegennahme des erhöhten Entgelts durch den Arbeitnehmer konkludent gem. § 151 BGB angenommen wird.[1287] Um von Art. 22 DSGVO erfasst zu sein, müsste eine (nachteilige) rechtliche Wirkung vorliegen. Eine rechtliche Wirkung liegt dann vor, wenn sich der rechtliche Status der betroffenen Person in irgendeiner Weise (nachteilig) verändert.[1288] Zwar ist zweifelhaft, ob durch die Abgabe eines konkludenten Angebots durch den Arbeitgeber sich der rechtliche Status des Arbeitnehmers verändert[1289], jedenfalls handelt es sich hierbei nicht um eine nachteilige rechtliche Wirkung, sodass die Maßnahme „automatisierte Gehaltserhöhung" in aller Regel nicht vom Verbot des Art. 22 Abs. 1 DSGVO erfasst ist. Eine Ausnahme bilden diejenigen Fälle, in denen der Algorithmus (in unzulässiger Weise) diskriminiert oder willkürlich entscheidet, sodass gegen den arbeitsrechtlichen Gleichbehandlungsgrundsatz[1290] oder Diskriminierungsverbote[1291] verstoßen wird.

Für die letztere Maßnahme benötigt es daher keiner besonderen datenschutzrechtlichen Rechtfertigung nach Art. 22 Abs. 2 DSGVO.

1287 Vgl. LAG München, Urt. v. 19.01.2017 – 3 Sa 668/16, BeckRS 2017, 152341 Rn. 45.

1288 *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 22 DSGVO Rn. 32, wobei hier keine nachteilige rechtliche Wirkung gefordert wird.

1289 Dies ist wohl anzunehmen, da aufgrund der Bindung des Antragenden an das Angebot (§ 145 BGB) der Antragsempfänger eine Rechtsposition dergestalt bekommt, dass er das Angebot innerhalb der Annahmefrist zu den angebotenen Konditionen annehmen kann und der Antragende dies nicht mehr einseitig zurückziehen kann. Unklar in diesem Zusammenhang: *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 22 DSGVO Rn. 34, der das Beispiel des Angebots zwar nennt, aber nicht auf die Person des Abgebenden eingeht; wohl dafür *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 22: Grundsätzlich ist jede Rechtsfolge erfasst, die eine Rechsposition begründet. *Schulz* schränkt das Recht aber auch auf nachteilige Rechtsfolgen ein, sodass die Begründung einer Rechtsposition des Betroffenen auch nach seiner Auffassung nicht darunterfallen dürfte.

1290 Zur Einordnung des arbereitsrechtlichen Gleichbehandlungsgrundsatzes unter die Kriterien des Art. 22 DSGVO, vgl. bereits oben **D. § 1 V. 3. c) bb)**.

1291 Ehmann/Selmayr/*Hladjk*, Art. 22 DSGVO Rn. 9.

bb) Betriebsverfassungsrechtlicher Kontext

Im betriebsverfassungsrechtlichen Kontext sind vor allem im Vorfeld solcher Maßnahmen weitgehende Mitbestimmungsrechte des Betriebsrats gegeben. Hierzu zählen insbesondere § 87 Abs. 1 Nr. 10 und 11 BetrVG.[1292] Während Nr. 10 die Lohngerechtigkeit dadurch sicherstellen soll, dass der Betriebsrat bei der betrieblichen Lohngestaltung, insbesondere bei der Aufstellung von Entlohnungsgrundsätzen und Einführung und Anwendung von neuen Entlohnungsmethoden ein Mitspracherecht hat, dient Nr. 11 demselben Zweck, allerdings spezifisch bei leistungsbezogenen Entgelten. § 87 Abs. 1 Nr. 11 BetrVG ist weiter als Nr. 10, da ersterer auch ein Mitbestimmungsrecht hinsichtlich der Lohnhöhe statuiert. Dies folgt daraus, dass die Festlegung der Geldfaktoren immer unter Anwendung eines Beurteilungsspielraums erfolgen müssen und enormen Druck auf die Arbeitnehmer erzeugen können.

Ein weiteres, in diesem Zusammenhang zu beachtendes Mitbestimmungsrecht statuiert § 94 Abs. 2 BetrVG: Die Mitbestimmung hinsichtlich der Aufstellung allgemeiner Beurteilungsgrundsätze.[1293] Diese Beurteilungsgrundsätze benötigt es, um eine Grundlage für Scoring und Profiling zu schaffen und einen „Leistungsbezugsrahmen" festzulegen. Auch diese müssen in Zusammenarbeit mit dem Betriebsrat vorab festgelegt werden. Das Mitbestimmungsrecht erstreckt sich ferner auf die Frage, ob die Bewertung vollautomatisch erfolgt oder eine Person dazwischengeschaltet wird.[1294]

Sollen technische Einrichtungen zur Überwachung der Leistung eingesetzt werden und diese Daten zur Festlegung der variablen Vergütung genutzt werden, so muss bereits vor der Einführung der technischen Einrichtungen der Betriebsrat nach § 87 Abs. 1 Nr. 6 BetrVG beteiligt werden.[1295]

cc) Ergebnis

Es kann festgehalten werden, dass nicht jegliche Entscheidungen im Personalbereich von Art. 22 Abs. 1 DSGVO erfasst sind; insbesondere Gehaltser-

1292 Siehe die Grundlagen unter **D. § 2 II. 1. c**).
1293 Vgl. **D. § 2 II. 2. b**).
1294 Richardi/*Thüsing*, § 94 BetrVG Rn. 62.
1295 Zum Mitbestimmungsrecht bei technischen (Überwachungs-)Einrichtungen, siehe bereits ausführlich **D. § 2 II. 1. b**).

höhungen sind – die Diskriminierungs- und Willkürfreiheit vorausgesetzt – nicht vom Verbot erfasst. Umsatzabhängige variable Vergütungen, die automatisiert ausbezahlt werden, unterliegen mangels einer automatisierten Einzelfallentscheidung ebenfalls nicht dem Verbot. Erfasst sind hingegen Leistungsbeurteilungen durch den Computer, sofern diese zu einer erheblichen Beeinträchtigung in Form einer (verminderten) variablen Vergütung führen können, wenn ein Algorithmus die Entscheidung über die Auszahlung entweder vollautomatisch durchführt oder ein menschlicher Entscheider den computergenerierten Score schlicht übernimmt.

Während die vollautomatische Durchführung nicht unter dem Aspekt der Erforderlichkeit gerechtfertigt werden kann, ist die Lage bei der Übernahme durch einen Menschen, verbunden mit einer Plausibilitätsprüfung, anders zu bewerten. In letzterem Fall kann es (dies ist im Einzelfall zu prüfen) durchaus aufgrund einer komplexen Datenausgangslage erforderlich sein, dass der gebildete Score weitgehend übernommen wird. Der betroffene Arbeitnehmer hat zu seinem Schutz ein Recht auf Anfechtung der Entscheidung und Darlegung des eigenen Standpunkts im Einzelfall nach Art. 22 Abs. 3 DSGVO.

b) Anmeldung für Weiterbildungen (Personalförderung)

Advanced People Analytics können auch dazu genutzt werden, um ein (Weiterbildungs-)Profil zu generieren, das die fachlichen/persönlichen Stärken und Schwächen des Arbeitnehmers aufzeigt (zu den Voraussetzungen einer solchen Profilbildung **E. § 1 II** sowie **E. § 1 III. 2. c**)).

Auf Basis dieses Profils könnten Arbeitnehmer dann automatisch im Rahmen der Personalförderung durch das HR-Management-System zu Fortbildungen angemeldet werden. In einer sehr fortschrittlichen Variante könnte ein solches System den digitalen Kalender des jeweiligen Arbeitnehmers analysieren und Fortbildungen so terminieren, dass keine wichtigen Termine verpasst werden. Dies könnte so weit führen, dass das System den Termin der Fortbildung automatisch in den Kalender einträgt und den Arbeitnehmer per E-Mail informiert.

Im Kern der Betrachtung stehen hier berufliche Fortbildungen im Sinne des § 1 Abs. 1 und 4 BBiG.[1296] Diese kann der Arbeitgeber einseitig per Direktionsrecht anordnen und den Arbeitnehmer zur Teilnahme verpflich-

1296 Einen Überblick gibt *Poeche*, Stichwort "Fortbildung", in: Küttner, Personalbuch 2020, Rn. 2 ff.

ten.[1297] Voraussetzung ist, dass „diese Schulungen bzw. Fortbildungsmaßnahmen der Ausübung der vertraglich geschuldeten Tätigkeit förderlich sind, d.h. so weit die im Rahmen der Schulung vermittelten Kenntnisse typischerweise im vereinbarten Tätigkeitsbereich einzusetzen sind."[1298]

Denkbar ist auch, dass für Fortbildungsmaßnahmen Verträge abgeschlossen werden, insbesondere wenn es sich um kostspielige Fortbildungen (z.B. Vorbereitungskurs zum Steuerberaterexamen oder eine Pilotenausbildung) handelt und eine Bindung des Arbeitnehmers an den Arbeitgeber gewollt ist.[1299] Da aber bereits aus praktischer Hinsicht eine automatisierte Einzelfallentscheidung aufgrund der besonderen Auswirkungen auf das Arbeitsverhältnis und der Notwendigkeit weiterer Verhandlungen ausscheidet, wird diese Möglichkeit in dieser Arbeit nicht weiter untersucht.

aa) Datenschutzrechtlicher Rahmen

Bei den Schulungsmaßnahmen, die durch Direktionsrecht angeordnet werden, besteht eine Verpflichtung des Arbeitnehmers an diesen teilzunehmen. Diese Entscheidung entfaltet also eine rechtliche Wirkung[1300], die nicht lediglich vorteilhaft für den Arbeitnehmer ist (Nicht-Folgeleistung ist eine Pflichtverletzung), sodass grundsätzlich das Verbot des Art. 22 Abs. 1 DSGVO eingreift, mit der Folge, dass der Ausnahmetatbestand der Erforderlichkeit nach Abs. 2 lit. a vorliegen müsste.

Eine Erforderlichkeit erscheint nach den unter **D. § 1 V. 3. d) aa)** herausgearbeiteten Grundsätzen höchst zweifelhaft: Auch in solchen Konstellationen ist zwischen dem Profiling des Arbeitnehmers als ersten Schritt der Fortbildungsplanung, der im Anschluss folgenden automatischen Anmeldung als zweiten Schritt und der Eintragung im Kalender und Mitteilung an den Arbeitnehmer als dritten Schritt zu unterscheiden. Erstere Maßnahme stellt noch keine automatisierte Einzelfallentscheidung dar, sondern ist als Advanced People Analytics-Maßnahme und somit einfachen Verarbeitungsvorgang (siehe oben **E. § 1 III. 2**) einzuordnen. Dasselbe gilt für

1297 *Klinkhammer/Peters*, ArbRAktuell 2015, 369 (370); *Poeche*, Stichwort "Fortbildung", in: Küttner, Personalbuch 2020, Rn. 16.

1298 LAG Rheinland-Pfalz, Urt. v. 23.11.2016 – 2 Ca 1147/16, BeckRS 2017, 123929 Rn. 36 m.w.N.

1299 Vgl. auch die Empfehlung von *Klinkhammer/Peters*, ArbRAktuell 2015, 369 (370).

1300 Zum Merkmal der „rechtlichen Wirkung" siehe **D. § 1 V. 3. c) bb) (1)**.

letzteres: Die Eintragung im Kalender; diese ist mangels Entscheidung mit rechtlicher Wirkung oder ähnlicher Beeinträchtigung ebenfalls nicht von Art. 22 Abs. 1 DSGVO erfasst.

Im Kern der Betrachtung steht daher die Erforderlichkeit einer automatischen Datierung für und Anmeldung von Fortbildungsmaßnahmen für Arbeitnehmer. Dies dürfte in aller Regel zu verneinen sein, da die Situation im Vergleich zu den bisher untersuchten (z.B. die Bewerberflut in **E. § 2 I**) eine völlig unterschiedliche ist.[1301] In diesem Fall müssen nicht wenige HR-Verantwortliche eine (vergleichsweise) extrem hohe Anzahl an Entscheidungen nahezu gleichzeitig treffen, sondern je nach Fortbildung sind immer nur wenige Arbeitnehmer betroffen und die inhaltliche Entscheidung über die Notwendigkeit und das Datum kann durchaus auch vom jeweiligen Gruppen- oder Abteilungsleiter getroffen werden. Eine gangbare Alternative ist es, dass das System Vorschläge generiert und die Ausgangslage des Vorschlags für den Entscheidungsträger transparent dargestellt wird, sodass dieser auf Basis der Datengrundlage dem Vorschlag folgen kann. So können in aller Regel auch persönliche Erfahrungen des Vorgesetzten mit dem jeweiligen Arbeitnehmer in die Entscheidung miteinfließen, sodass es sich bei der Übernahme des Vorschlags dennoch nicht um eine „blinde Übernahme" handelt und somit keine automatisierte Einzelfallentscheidung i.S.d. Art. 22 DSGVO vorliegt.

Alternativ können bei optionalen Schulungen, die nicht per Direktionsrecht angeordnet werden, den Arbeitnehmern Vorschläge unterbreitet werden (z.B. in einem persönlichen Dashboard oder per E-Mail), bei denen dieser dann entsprechend seinem persönlichen Zeitplan ein passendes Datum auswählen (sofern mehrere zur Verfügung stehen) und sich hierfür per Mausklick anmelden kann. Die Daten werden im Anschluss automatisch in das Fortbildungssystem übernommen und entsprechende Kurse gebucht. In diesem Fall handelt es sich nicht um eine automatisierte Einzelfallentscheidung, da der Computer letztlich (ähnlich wie bei einer Bestellung auf Amazon o.ä.) nur ausführt, was der Arbeitnehmer (und der Arbeitgeber, indem der dem Arbeitgeber die Möglichkeit zur „freien" Buchung eines Kurses überlässt) entschieden hat.

1301 So i.E. auch *Hinz*, 11. Arbeitsrecht, in: Kaulartz/Ammann/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, Rn. 25.

bb) Betriebsverfassungsrechtlicher Kontext

Sämtliche Maßnahmen der Berufsbildung i.S.d. § 1 Abs. 1 BBiG, wozu auch Fortbildungen, betriebliche Lehrgänge, Seminare etc. gehören, unterliegen den Beteiligungsrechten des Betriebsrats nach §§ 96 - 98 BetrVG.[1302] Das Beteiligungsrecht bezieht sich vor allem auf betriebliche Maßnahmen, d.h. solche, bei denen der Arbeitgeber Träger bzw. Veranstalter der Bildungsmaßnahme ist, unabhängig von der örtlichen Durchführung.[1303] Dies ist immer dann der Fall, wenn der Arbeitgeber – rechtlich gesehen – einen beherrschenden Einfluss auf Inhalt und Organisation hat.[1304] Handelt es sich um eine überbetriebliche Bildungsmaßnahme, z.B. auf Basis eines Kooperationsvertrags zwischen mehreren Arbeitgebern, so kann der Betriebsrat dort mitbestimmen, wo der Arbeitgeber noch eigene Festlegungen für die spätere Maßnahme treffen kann (z.B. wenn der Arbeitgeber den Inhalt bestimmen/beeinflussen kann oder den Zeitpunkt der Veranstaltung).[1305]

Bei vollständig außerbetrieblichen Maßnahmen scheitert ein Mitbestimmungsrecht des Betriebsrats an der mangelnden Gestaltungsmacht des Arbeitgebers.[1306] Hinsichtlich des Berufsbildungsbedarfs und der Fragen der Berufsbildung der Arbeitnehmer des Betriebs hat der Betriebsrat jedoch ein Beratungsrecht nach § 96 Abs. 1 S. 2 BetrVG – auch bei vollständig externen Maßnahmen.[1307]

All diese Beteiligungsrechte hindern den Arbeitgeber aber nicht daran, bestimmte Maßnahmen für bestimmte Arbeitnehmer automatisiert anzubieten.

Lediglich unter den Voraussetzungen des § 98 Abs. 3 BetrVG kann der Betriebsrat Vorschläge für die Teilnahme von Arbeitnehmern oder Gruppen von Arbeitnehmern an Berufsbildungsmaßnahmen machen. Dies ist der Fall, wenn der Arbeitgeber die Maßnahmen entweder selbst durchführt, Arbeitnehmer für außerbetriebliche Maßnahmen freistellt oder die Kosten ganz oder teilweise trägt. Dieses Vorschlagsrecht geht so weit, dass bei einer Uneinigkeit über die Vorschläge nach § 98 Abs. 4 BetrVG die

1302 BeckOK ArbR/*Mauer*, § 96 BetrVG Rn. 2 f.
1303 ErfK/*Kania*, § 96 BetrVG Rn. 8.
1304 BAG, Beschl. v. 04.12.1990 – 1 ABR 10/90, AP BetrVG 1972 § 97 Nr. 1.
1305 BAG, Beschl. v. 18.04.2000 – 1 ABR 28/99, AP BetrVG 1972 § 98 Nr. 9 unter B. I. 2. c) cc) der Gründe.
1306 BAG, Beschl. v. 18.04.2000 – 1 ABR 28/99, AP BetrVG 1972 § 98 Nr. 9 unter B. I. 2. a) bb) der Gründe m.w.N.
1307 ErfK/*Kania*, § 96 BetrVG Rn. 8 m.w.N.

Einigungsstelle angerufen werden kann. Das Recht ist also nicht nur ein Vorschlagsrecht, sondern ein Mitbestimmungsrecht in Form eines Initiativrechts.[1308] Die fachlichen Zulässigkeitsvoraussetzungen für die jeweilige Bildungsmaßnahme obliegen aber ausschließlich dem Arbeitgeber.[1309] Der Betriebsrat muss also eigene Vorschläge machen, um z.B. bei Kapazitätsengpässen über die Auswahl der Arbeitnehmer nach dem vom Arbeitgeber festgelegten Zulässigkeitskriterien mitbestimmen zu können.[1310]

In letzterem Fall entscheidet bei Streitigkeiten die Einigungsstelle nicht nur über die Vorschläge des Betriebsrats, sondern auch über jene, die vom Arbeitgeber ausgewählt wurden, gemeinsam und wählt die Arbeitnehmer anhand der festgelegten Kriterien aus, bis die Kapazitätsgrenze der Bildungsmaßnahme erreicht ist; ein generelles Mitbestimmungsrecht hinsichtlich der Auswahl des Arbeitgebers besteht daher nicht.[1311]

Aus betriebsverfassungsrechtlicher Sicht ist es aber daher notwendig, geplante Bildungsmaßnahmen zunächst mit dem Betriebsrat abzusprechen, bevor solche dem Arbeitnehmer verbindlich angeboten werden und dieser sich einen Platz über das Fortbildungssystem buchen kann. Empfehlenswert ist, die Vorschlagsliste des Arbeitgebers, die durch ein Scoring / Profiling der Arbeitnehmer produziert wurde, dem Betriebsrat zu übermitteln, sodass dieser überprüfen kann, ob jene Arbeitnehmer, die der Betriebsrat vorschlagen würde, bereits auf der Liste sind. Vor der Anmeldung für die Schulung ist sodann zu überprüfen, ob der Betriebsrat eigene Vorschläge macht und ob diese im Rahmen der Kapazitäten der Bildungsmaßnahme liegen und den fachlichen Zulässigkeitsvoraussetzungen des Arbeitgebers entsprechen. Hier kann ein Scoring der Vorschläge des Betriebsrats helfen, im Streitfall eine einvernehmliche Lösung zu finden, ohne dass es zu einer Anrufung der Einigungsstelle nach § 98 Abs. 4 BetrVG kommen muss.

cc) Ergebnis

Ein vollständig automatisiertes Bildungsmanagement durch ein intelligentes Personalmanagementsystem scheidet sowohl aus datenschutzrecht-

1308 Richardi/*Thüsing*, § 98 BetrVG Rn. 60.
1309 BAG, Beschl. v. 08.12.1987 – 1 ABR 32/86, AP BetrVG 1972 § 98 Nr. 4; ferner Richardi/*Thüsing*, § 98 BetrVG Rn. 61 m.w.N.
1310 Vgl. BAG, Beschl. v. 20.04.2010 – 1 ABR 78/08, NZA 2010, 902 (903 f.) Rn. 16.
1311 BAG, Beschl. v. 08.12.1987 – 1 ABR 32/86, NZA 1988, 401 f.

lichen als auch betriebsverfassungsrechtlichen Gründen aus. Für einen Teil der Bildungsmaßnahmen ist dies bereits aus praktischer Hinsicht undenkbar, da weitere Vereinbarungen zwischen Arbeitgeber und Arbeitnehmer, z.B. im Hinblick auf die Kostentragung oder eventuelle Bindungen des Arbeitnehmers (insbesondere bei höherpreisigen und längerfristigen Bildungsmaßnahmen[1312]) getroffen werden müssen. Der Großteil der Bildungsmaßnahmen wird in der Praxis (wohl) per Direktionsrecht angeordnet oder dem Arbeitnehmer die Teilnahme freigestellt. Lediglich bei ersteren läge eine automatisierte Einzelfallentscheidung vor, deren Zulässigkeit aber an der Erforderlichkeit der Maßnahme gem. Art. 22 Abs. 1 lit. a DSGVO scheitert. Zudem hat der Betriebsrat bei Bildungsmaßnahmen ein Vorschlagsrecht nach § 98 Abs. 3 BetrVG. Dies gilt auch bei externen Schulungsmaßnahmen, sofern Arbeitnehmer dafür freigestellt werden oder er die Kosten ganz oder teilweise trägt. Dies dürfte die überwiegende Anzahl der Fortbildungen im Rahmen des Arbeitsverhältnisses betreffen. Da in aller Regel die Maßnahmen nur eine bedingte Kapazität haben, ist damit zu rechnen, dass es zu Engpässen kommen kann und daher die Betriebsparteien sich über die Teilnahme aller, also nicht nur der Vorschläge des Betriebsrats, sondern auch der vom Arbeitgeber vorgesehenen Fortbildungsteilnehmer, einigen müssen.

Eine automatisierte Einzelfallentscheidung (bspw. in Form einer Anmeldung für die Schulung) führt daher auch aus betriebsverfassungsrechtlichen Gründen zu Problemen.

Möglich bleibt es aber dennoch, die Arbeitnehmer in diesem Rahmen zu scoren bzw. profilen[1313] und eine Vorschlagsliste generieren zu lassen. Ebenso unproblematisch, da keine Entscheidung mit rechtlicher Wirkung oder ähnlicher Beeinträchtigung vorliegt, ist nach erfolgter Anmeldung eine automatische Eintragung in den Kalender des jeweiligen Arbeitnehmers und eine Information per E-Mail oder das automatisierte Versenden einer Termineinladung zur Schulung per E-Mail, die der Arbeitnehmer dann bestätigen kann.

1312 *Poeche*, Stichwort "Rückzahlungsklausel", in: Küttner, Personalbuch 2020, Rn. 1 ff.

1313 Hierbei handelt es sich um eine Advanced People Analytics-Maßnahme, die den unter **E. § 1 III. 2** beschriebenen Voraussetzungen unterliegt.

c) Versetzungen und Kündigungen

Ein weiteres mögliches Einsatzszenario für automatisierte Einzelfallentscheidungen stellen Versetzungen und Kündigungen dar. Dies kommt etwa in Betracht, wenn Kapazitätsengpässe in einer anderen Niederlassung bestehen oder über ein Scoring der Arbeitsleistung über einen größeren Zeitraum festgestellt wird, dass ein Arbeitnehmer ein sog. Low-Performer ist und deshalb gekündigt werden soll. Insbesondere bei Kündigungen sind nicht nur datenschutzrechtliche und betriebsverfassungsrechtliche, sondern auch kündigungsschutzrechtliche Fragen zu klären, weshalb diese Maßnahmen im Folgenden gesondert geprüft werden.

aa) Versetzungen

Unter einer Versetzung versteht man (im betriebsverfassungsrechtlichen Sinne, vgl. § 95 Abs. 3 BetrVG) die Zuweisung eines anderen Arbeitsbereichs, die voraussichtlich die Dauer von einem Monat überschreitet oder die mit einer erheblichen Änderung der Umstände verbunden ist, unter denen die Arbeit zu leisten ist.[1314] Lediglich wenn die Arbeitnehmer nach der Eigenart des Arbeitsverhältnisses nicht ständig an einem bestimmten Arbeitsplatz beschäftigt werden, handelt es sich nicht um eine Versetzung.

Ein anderer Arbeitsbereich dem Arbeitnehmer wird zugewiesen, wenn diesem ein neuer Tätigkeitsbereich übertragen wird, sodass der Gegenstand der geforderten Arbeitsleistung nun ein anderer wird und sich das Gesamtbild der Tätigkeit verändert. Von einer Veränderung ist auch auszugehen, wenn sich die Umstände, unter denen die Arbeit zu erbringen ist, wesentlich verändern. Nicht ausreichend hierfür ist, wenn sich lediglich die Arbeitszeit ändert.[1315]

Es muss nicht zwingend ein Wechsel des Arbeitsplatzes stattfinden. So kann es bereits als Versetzung gewertet werden, wenn z.B. im Rahmen

---

1314 *Nota bene:* Individualarbeitsrechtlich gibt es keine einheitliche Definition für eine Versetzung; insbesondere gibt es dort keine starren zeitlichen Fristen, vgl. *Poeche*, Stichwort "Versetzung", in: Küttner, Personalbuch 2020, Rn. 2 ff. In aller Regel kommt es jedoch zu einem Gleichlauf mit dem betriebsverfassungsrechtlichen Begriff.

1315 Zum Begriff des Arbeitsbereichs bereits BAG, Beschl. v. 23.11.1993 – 1 ABR 38/93, AP BetrVG 1972 § 95 Nr. 33 unter B. I. 1. der Gründe; Beschl. v. 19.02.1991 – 1 ABR 21/90, AP BetrVG 1972 § 95 Nr. 25 unter B. II. der Gründe.

einer Matrixorganisation neue Vorgesetzte hinzukommen, die eigene disziplinarische Befugnisse haben.[1316]

In aller Regel liegt eine Versetzung vor, wenn ein Arbeitsplatz an einem anderen Ort zugewiesen wird, auch wenn die zu erbringende Arbeitsleistung inhaltlich unverändert bleibt. Dasselbe gilt, wenn der Arbeitnehmer in eine andere organisatorische Einheit eingegliedert wird.[1317]

Ebenso um eine Versetzung handelt es sich, wenn dem Arbeitnehmer eine Tätigkeit im Home-Office zugewiesen wird. Fehlt es an einer Zuweisung und wird ihm lediglich die Option eröffnet, während sein bisheriger Arbeitsplatz bestehen bleibt, liegt keine Versetzung vor.[1318]

(1) Datenschutzrechtlicher Rahmen

Individualarbeitsrechtlich handelt es sich bei der Versetzung um eine einseitige Änderung des Arbeitsortes per Direktionsrecht gem. § 106 GewO[1319], wobei dieses arbeitsvertraglich durch Versetzungsklauseln eingeschränkt oder erweitert werden kann.[1320] Wird eine solche Versetzung mittels Direktionsrecht per automatisierter Einzelfallentscheidung vorgenommen, unterliegt diese grundsätzlich dem Verbot aus Art. 22 Abs. 1 DSGVO und muss daher erforderlich im Sinne des Buchst. a des Absatzes 2 sein, da keine anderen Ausnahmetatbestände einschlägig sind.[1321]

Nach den bisher entwickelten Maßstäben müsste hierfür eine derart große Menge an Daten auszuwerten sein, dass ein bzw. mehrere Entscheider damit „überfordert" sind, m.a.W. es nicht mehr zumutbar ist, die Entscheidung selbst zu treffen.

Da Versetzungen nur vereinzelt und nicht als „Massenphänomen" stattfinden, ist eine automatisierte Einzelfallentscheidung nicht erforderlich und somit unzulässig.

1316 ErfK/*Kania*, § 99 BetrVG Rn. 14 m.w.N.

1317 Vgl. BAG, Beschl. v. 18.02.1986 – 1 ABR 27/84, AP BetrVG 1972 § 99 Nr. 33; Beschl. v. 18.10.1988 – 1 ABR 26/87, AP BetrVG 1972 § 99 Nr. 56.

1318 ErfK/*Kania*, § 99 BetrVG Rn. 15.

1319 Versetzungen, die nicht vom Direktionsrecht erfasst sind, bedürfen einer Änderungskündigung und werden somit von den Ausführungen unter bb) erfasst.

1320 Im Überblick *Poeche*, Stichwort "Versetzung", in: Küttner, Personalbuch 2020, Rn. 2 ff. m.w.N.

1321 Zur Erforderlichkeit im Sinne von Art. 22 Abs. 2 lit. a DSGVO siehe bereits ausführlich **D. § 1 V. 3. d**) **aa**).

Hingegen ist es aber zulässig, dass Versetzungsempfehlungen durch Personalsoftware vorbereitet werden und auf Grundlage eines Scorings erfolgen. Mangels rechtlicher Wirkung oder ähnlicher erheblicher Beeinträchtigung für den Betroffenen kann auch automatisiert eine Unterrichtung des Betriebsrats über den bzw. die zu versetzenden Mitarbeiter erfolgen. Dennoch bleibt es den Verantwortlichen – anders als beispielsweise im Fall des Bewerbungsverfahrens – zumutbar, die Datengrundlage zu sichten und diese zu überprüfen und auf dieser Basis die Letztentscheidung (nach positiver Rückmeldung durch den Betriebsrat) zu treffen.

(2) Betriebsverfassungsrechtlicher Kontext

Das Betriebsverfassungsrecht regelt mit § 99 Abs. 1 BetrVG die Mitbestimmungsrechte des Betriebsrats bei Versetzungen. Der Betriebsrat muss hierüber informiert werden und der geplanten Maßnahme zustimmen. Die Gründe für eine Zustimmungsverweigerung sind in § 99 Abs. 2 BetrVG abschließend aufgezählt,[1322] können jedoch durch freiwillige Betriebsvereinbarungen erweitert werden.[1323] Hierfür hat der Betriebsrat nach § 99 Abs. 3 BetrVG eine Woche Zeit. Verweigert er die Zustimmung, so muss der Arbeitgeber beim Arbeitsgericht beantragen, die Zustimmung zu ersetzen (§ 99 Abs. 4 BetrVG), in dringenden Fällen kann er die Maßnahme nach § 100 BetrVG vorläufig durchführen.

Aus betriebsverfassungsrechtlicher Sicht wäre es daher grundsätzlich möglich, dass arbeitgeberseitig die Entscheidung automatisiert gefällt und der Betriebsrat im Anschluss hiervon unterrichtet wird, bevor die Maßnahme vollzogen wird.

(3) Ergebnis

Vollständig automatisiert lassen sich Versetzungen in der Praxis mangels Erforderlichkeit nicht umsetzen. Möglich ist es aber, den Entscheidungsvorgang so weit zu automatisieren, dass auch der Betriebsrat über die geplante Maßnahme automatisch unterrichtet wird und diesem die Ergebnisse des Scoring-Verfahrens (sowie die Datengrundlage) mitgeteilt werden,

1322 Richardi/*Thüsing*, § 99 BetrVG Rn. 208.
1323 BAG, Beschl. v. 23.08.2016 – 1 ABR 22/14, NZA 2017, 194 (198 f.) Rn. 39 ff.

sodass dieser nach § 99 Abs. 1 BetrVG die Zustimmung erteilen kann.[1324] Für die endgültige Entscheidung muss aber ein menschlicher Entscheider nochmals die Datengrundlage überprüfen und auf dieser Basis den Vorschlag des Algorithmus bestätigen.

bb) Kündigungen

Dieselben Überlegungen bei der Versetzung gelten auch für die Kündigung, wobei zusätzlich die Vorgaben des Kündigungsschutzgesetzes einzuhalten sind. Zudem erfolgt die Beteiligung des Betriebsrats nach § 102 BetrVG. Eine ohne Anhörung des Betriebsrats ausgesprochene Kündigung ist unwirksam (§ 102 Abs. 1 S. 2 BetrVG).

Lediglich im Falle einer Massenentlassung könnte es zu ähnlichen Fällen wie im Bewerbungsverfahren kommen, also dass über so viele Personen auf einer breiten Basis entschieden werden muss, dass es den Verantwortlichen nicht mehr zumutbar ist, die gesamte Datenbasis noch manuell zu überblicken. Maßgeblich ist wiederum die jeweilige Betriebsgröße[1325] und die Anzahl der Entlassungen. Kündigungsschutzrechtlich handelt es sich nach § 17 Abs. 1 KSchG um eine meldepflichtige Massenentlassung, wenn in Betrieben mit 21 - 59 Arbeitnehmern innerhalb von 30 Kalendertagen mehr als 5 Arbeitnehmer entlassen werden. In diesem Fall wird man noch nicht von einer Erforderlichkeit nach Art. 22 Abs. 2 lit. a DSGVO ausgehen dürfen. Kritisch sieht dies auch in den Fällen von § 17 Abs. 1 Nr. 2 und 3, die eine Anzeigepflicht ab 6 bzw. 25 und 30 Arbeitnehmern innerhalb von 30 Tagen vorsehen.

Es sind aber Fälle denkbar, in denen eine derart große Anzahl an Arbeitnehmern entlassen werden muss, dass es in einem zumutbaren Zeitraum nicht möglich ist, die angesetzten Kriterien für die Entlassung im Detail zu überprüfen, sondern lediglich eine Plausibilitätsprüfung des Ergebnisses in Betracht kommt. In solchen (Ausnahme-)Fällen wäre eine automatisierte Einzelfallentscheidung nach Art. 22 Abs. 2 lit. a DSGVO zulässig, wobei unter Wahrung des Verhältnismäßigkeitsgrundsatzes weiterhin erforder-

---

1324 Die Zustimmung gilt nach § 99 Abs. 3 a.E. auch als erteilt, wenn der Betriebsrat sich nicht binnen einer Woche nach Unterrichtung äußert.

1325 Es gilt der Betriebsbegriff des BetrVG (§§ 1 und 4 BetrVG), vgl. APS/*Moll*, § 17 KSchG Rn. 3 Beim Vorhandensein mehrerer Betriebe ist zudem der europäische Betriebsbegriff der Massenentlassungsrichtlinie (kurz: MERL) heranzuziehen, vgl. hierzu *Kreitner/Seidel/Voelzke*, Stichwort "Massenentlassung", in: Küttner, Personalbuch 2020, Rn. 4 ff.

lich bleibt, dass so viele Daten wie möglich, zumindest aber die Plausibilität durch einen menschlichen Entscheider geprüft wird.

Bei jeder Massenentlassung müssen der Agentur für Arbeit nach § 17 Abs. 2 und 3 die Gründe für die geplanten Entlassungen, die Zahl und die Berufsgruppen der zu entlassenden Arbeitnehmer, die Zahl und die Berufsgruppen der in der Regel beschäftigten Arbeitnehmer, den Zeitraum, in dem die Entlassungen vorgenommen werden sollen sowie die vorgesehenen Kriterien für die Auswahl der zu entlassenen Arbeitnehmer mitgeteilt werden. Dem Betriebsrat müssen zusätzlich noch die für die Berechnung etwaiger Abfindungen vorgesehenen Kriterien mitgeteilt werden.

(1) Betriebsverfassungsrechtlicher Rahmen bei der Massenentlassung

Nach § 111 Nr. 1 BetrVG liegt eine Betriebsänderung vor, wenn ein Betrieb oder wesentliche Betriebsteile eingeschränkt oder stillgelegt werden.[1326] Anders als die Meldepflicht in § 17 Abs. 1 KSchG gilt § 111 BetrVG bei einer Unternehmensgröße (nicht: Betriebsgröße) von mehr als 20 wahlberechtigen Arbeitnehmer.[1327] Die ständige Rechtsprechung des Bundesarbeitsgerichts greift für die Feststellung einer Betriebsänderung nach § 111 S. 3 Nr. 1 BetrVG grundsätzlich auf die Grenzen des § 17 Abs. 1 KSchG zurück.[1328] Besondere Regelungen sind in § 112a BetrVG enthalten, wenn die geplante Betriebsänderung allein in der Entlassung von Arbeitnehmern besteht. Hiernach wird die *Erzwingbarkeit* von Sozialplänen eingeschränkt, wenn es sich um Maßnahmen des Personalabbaus handelt.[1329] Der Arbeitgeber muss jedoch weiterhin versuchen, einen Interessensausgleich herbeizuführen.[1330]

Gegenstand des Sozialplans ist der Ausgleich oder die Milderung der wirtschaftlichen Nachteile, die den Arbeitnehmern infolge der geplanten Betriebsänderung entstehen, wie sich aus der Legaldefinition in § 112

1326 Allgemein zur Betriebsänderung sowie spezifisch zu § 111 Nr. 4 und 5 bereits unter **D. § 2 II. 6.**

1327 *Fitting*, § 111 Rn. 18 f.

1328 Vgl. statt aller BAG, Urt. v. 09.11.2010 – 1 AZR 708/09, NZA 2011, 466 (467) Rn. 15 m.w.N.; Beschl. v. 28.03.2006 – 1 ABR 5/05, NZA 2006, 932 (933) Rn. 18 m.w.N.

1329 Richardi/*Annuß*, § 112a BetrVG Rn. 2.

1330 BeckOK ArbR/*Besgen*, § 112a BetrVG Rn. 2; Richardi/*Annuß*, § 112a BetrVG Rn. 2.

Abs. 1 S. 2 BetrVG ergibt. Dieser hat die Wirkung einer Betriebsvereinbarung und ist zwischen Arbeitgeber und Betriebsrat zu verhandeln.

Der Interessenausgleich regelt hingegen die organisatorische Umsetzung der Betriebsänderung und die damit verbundenen personellen Maßnahmen. Hierin sollen die Interessen des Arbeitgebers an einer wirtschaftlichen Führung des Betriebs mit denen der Arbeitnehmer am Erhalt ihrer Arbeitsplätze und -bedingungen ausgeglichen werden. Anders als der Sozialplan wirkt dieser nicht normativ.[1331]

Während der Interessensausgleich also um das Ob und Wie der Maßnahmen geht, regelt der Sozialplan nur noch den Ausgleich der sozialen Folgen. Bevor eine Selektion der zu entlassenden Mitarbeiter durch einen Algorithmus stattfinden kann, muss mit dem Betriebsrat im Rahmen eines Interessensausgleichs über Auswahlrichtlinien verhandelt werden, wobei die vier „Grunddaten" Betriebszugehörigkeit, Lebensalter, Unterhaltspflichten und Schwerbehinderung in einem erheblichen und ausgewogenen Maß berücksichtigt werden müssen. Hierzu kann ein Punktesystem dienen.[1332]

Hierfür könnten zusätzliche Daten aus dem Personalmanagementsystem, z.B. die mittels *Advanced People Analytics* gewonnen wurden, mit in die Auswahlrichtlinien einfließen. Diese könnten neben den zwingend zu berücksichtigenden Kriterien weitere Anhaltspunkte für eine sozial gerechte Auswahl liefern. Verarbeitungsgrundlage ist wiederum § 26 Abs. 1 S. 1 BDSG.

Im Anschluss an den Interessensausgleich können die dort vereinbarten Auswahlrichtlinien in das System eingearbeitet und eine Liste der zu entlassenden Mitarbeiter generiert werden, z.B. über ein Scoring-System, das alle Kriterien berücksichtigt und eine entsprechende Bewertung pro Mitarbeiter erstellt. Anstatt ausschließlich die vier „Grunddaten" zu berücksichtigen und eine entsprechende Punktezahl daraus zu berechnen, kann mittels eines Scoring-Systems eine deutlich differenziertere (und in der Regel gerechtere) Auswahl getroffen werden, die weitere Faktoren (z.B. Teamfähigkeit, wenn vorwiegend in Teams gearbeitet wird etc.) berücksichtigt. Je nach Anzahl der zu entlassenden Mitarbeiter kann es dem Arbeitgeber unzumutbar sein, alle Bewertungskriterien des Auswahlalgorithmus zu überprüfen, sondern lediglich noch eine Plausibilitätsprüfung

1331 *Schmidt*, Stichwort "Interessensausgleich", in: Küttner, Personalbuch 2020, Rn. 1 m.w.N.

1332 *Schmidt*, Stichwort "Interessensausgleich", in: Küttner, Personalbuch 2020, Rn. 5.

durchführbar sein. Bei letzterem handelte es sich dann um eine automatisierte Einzelfallentscheidung nach Art. 22 Abs. 1 DSGVO, die nach Abs. 2 lit. a DSGVO aufgrund von Erforderlichkeit gerechtfertigt sein kann. Dies ist im Einzelfall zu prüfen.

Die Ausbezahlung etwaiger im Sozialplan festgelegten Abfindungen kann hingegen ohne weiteres vollautomatisiert erfolgen, denn hier findet keine automatisierte Entscheidung mehr statt. Der Computer führt lediglich die zuvor mit dem Betriebsrat vereinbarten Regelungen aus und entscheidet nicht selbst.[1333] Beschäftigte sind bei Berechnungsfehlern dadurch geschützt, dass der Sozialplan eine normative Wirkung hat und sie somit einen unmittelbaren Rechtsanspruch aus dem Sozialplan herleiten können.

(2) Kündigungsschutzrechtliche Vorgaben

Neben den Beteiligungsvorschriften der §§ 17 ff. KSchG ist auch der individualrechtliche Kündigungsschutz der §§ 1 ff. KSchG anwendbar,[1334] sodass bei einer betriebsbedingten Kündigung – wie bei der Massenentlassung – auch eine Sozialauswahl nach § 1 Abs. 3 KSchG getroffen werden muss.[1335] Es gelten grundsätzlich dieselben vier Kernkriterien wie bei Auswahlrichtlinien im Interessensausgleich (siehe oben); anders als beim Interessensausgleich ist die Aufzählung der Kriterien jedoch abschließend, wobei dem Arbeitgeber ein Wertungsspielraum zusteht[1336]. Nach § 1 Abs. 3 S. 2 KSchG müssen jedoch solche Arbeitnehmer nicht in die Sozialauswahl miteinbezogen werden, deren Weiterbeschäftigung, insbesondere wegen ihrer Kenntnisse, Fähigkeiten und Leistungen oder zur Sicherung einer ausgewogenen Personalstruktur des Betriebs, im berechtigten betrieblichen Interesse liegt.

Die Kenntnisse beziehen sich auf das Wissen des Arbeitnehmers, die Fähigkeiten auf die sog. Soft-Skills, die nicht zwingend die Hauptleistung betreffen müssen und die Leistungen auf qualitative oder quantitative

1333 Zum Kriterium der „Entscheidung" siehe **D. § 1 V. 3. c**).

1334 BAG, Urt. v. 06.12.1973 – 2 AZR 10/73, NJW 1974, 1263; APS/*Moll*, Vor § 17 KSchG Rn. 17 m.w.N.; *Kreitner/Seidel/Voelzke*, Stichwort "Massenentlassung", in: Küttner, Personalbuch 2020, Rn. 11.

1335 *Kreitner/Seidel/Voelzke*, Stichwort "Massenentlassung", in: Küttner, Personalbuch 2020, Rn. 11.

1336 *Eisemann/Seidel/Voelzke*, Stichwort "Kündigung, betriebsbedingte", in: Küttner, Personalbuch 2020, Rn. 34 m.w.N.

Güte der geschuldeten Leistung im Vergleich zu anderen Arbeitnehmern, sofern sie sich objektivieren lassen.[1337]

Ebenfalls sind Arbeitnehmer mit einem Sonderkündigungsschutz wie beispielsweise Schwerbehinderte (§§ 85 ff. SGB IX), Schwangere und junge Mütter (§§ 99 MuSchG, 18 BEEG) sowie betriebsverfassungsrechtliche Funktionsträger[1338] von der Sozialauswahl ausgeschlossen.[1339]

Die Anwendung von *Advanced People Analytics* bzw. der Daten aus dem Personalmanagementsystem erlaubt es dem Arbeitgeber schnell und unkompliziert zu den Daten der Sozialauswahl zu kommen, wobei die Auswahl in zwei Schritten zu erfolgen hat:

In einem ersten Schritt werden all jene Arbeitnehmer ausgeschlossen, die nicht an der Sozialauswahl teilnehmen. Hierbei kann mittels APA ermittelt werden, wer die Top-Performer im jeweiligen Betrieb, somit unverzichtbar und von der Sozialauswahl ausgeschlossen sind. Die Daten aus den APA ermöglichen dem Arbeitgeber den Nachweis der betrieblichen Erforderlichkeit jener Arbeitnehmer.

Im zweiten Schritt werden die verbleibenden Arbeitnehmer anhand der in § 1 Abs. 3 S. 1 KSchG festgelegten Kriterien einer Sozialauswahl unterzogen, wobei auch das System dabei behilflich sein kann, die Wertung der einzelnen Kriterien zu bestimmen und eine sozial gerechte Liste der zu kündigenden Arbeitnehmer zu generieren. Die Ausarbeitung der Auswahlrichtlinie hat gem. § 112 Abs. 1 BetrVG ohnehin im Rahmen eines Interessensausgleichs zu erfolgen, sodass eine vollständige Automatisierung des Vorgangs ausscheidet.

(3) Ergebnis

Während automatisierte Einzelfallentscheidungen nach Art. 22 Abs. 1 DSGVO in aller Regel bei Kündigung ausgeschlossen sind, ist ein Anwendungsfall zumindest denkbar: Die Entlassung einer Vielzahl von Arbeitnehmern, insbesondere die Massenentlassung nach §§ 17 ff. KSchG. In diesem Fall kann – insbesondere bei sehr großen Betrieben – die Datengrundlage, als Basis für die Sozialauswahl und den Interessensausgleich genutzt werden soll, so groß sein, dass es den Verantwortlichen nicht zumutbar ist,

1337 APS/*Vossen*, § 1 KSchG Rn. 670 ff.
1338 Aufzählung aus *Eisemann/Seidel/Voelzke*, Stichwort "Kündigung, betriebsbedingte", in: Küttner, Personalbuch 2020, Rn. 26.
1339 BAG, Urt. v. 17.11.2005 – 6 AZR 118/05, NZA 2006, 370 (371) Rn. 17.

eine Entscheidung unter Nachprüfung der gesamten Datengrundlage zu treffen. Wird ein System eingesetzt, dass entsprechende Listen generiert, kann es bei hoher Komplexität der Auswahlkriterien und einer Vielzahl von Fällen dazu kommen, dass nur noch eine Plausibilitätsprüfung möglich ist. In einem solchen Fall liegt eine automatisierte Einzelfallentscheidung vor, die jedoch von der Ausnahme des Art. 22 Abs. 1 lit. a DSGVO erfasst und somit rechtmäßig ist.

Neben dem Sonderfall der Massenentlassung können Advanced People Analytics bei jeder betriebsbedingten Kündigung behilflich sein, entsprechende Kriterien für die Sozialauswahl festzulegen und Listen zu generieren, die dann aber noch von einem menschlichen Entscheider nachzuprüfen sind. Dennoch lässt sich durch die Feststellung z.B. der High-Performer im Unternehmen leichter die soziale Auswahl treffen und insbesondere im gerichtlichen Prozess ein Ausschluss dieser Arbeitnehmer von dieser auch nachweisen.

Keine Fall des Art. 22 Abs. 1 DSGVO stellt es mangels Entscheidung dar, wenn das System nur noch die bereits von den menschlichen Verantwortungsträgern getroffenen Entscheidungen ausführt. Klassischer Anwendungsfall hierfür wäre die Festlegung und Ausbezahlung der Abfindungshöhe nach dem Sozialplan für die einzelnen Arbeitnehmer.

III. Zusammenfassung

Im Bewerbermanagement können automatisierte Einzelfallentscheidungen im Sinne des Art. 22 Abs. 1 DSGVO bei hohen Bewerberzahlen zulässig sein. Grund hierfür ist, dass aufgrund mangelnder Kapazitäten in der HR-Abteilung bei Bewerberfluten es schlichtweg aus praktischen Gründen ausscheidet, alle Bewerbungen einzeln zu sichten. Im Sinne eines fairen Bewerbungsverfahrens, bei dem alle Bewerbungen berücksichtigt werden, kann es erforderlich sein, automatisierte Einzelfallentscheidungen einzusetzen. Ein solches Vorgehen wäre unter den o.g. Voraussetzungen auf die Ausnahme des Art. 22 Abs. 2 lit. a DSGVO zu stützen.

Etwas anderes gilt im laufenden Arbeitsverhältnis: Dort ist die Häufigkeit von für verschiedene Arbeitnehmer gleichzeitig zu treffenden Einzelfallentscheidungen deutlich geringer, sodass in aller Regel die Erforderlichkeit einer automatisierten Einzelfallentscheidung verneint werden muss. Möglich bleibt ein Automatismus, der beispielsweise automatische Vorschläge für Fortbildungsveranstaltungen an bestimmte Arbeitnehmer sendet. Mangels rechtlicher Wirkung ist dieses Szenario nicht vom Verbot

des Art. 22 Abs. 1 DSGVO erfasst und somit ohne weitere Rechtfertigung zulässig.

Allenfalls im Rahmen von Massenentlassungen könnten in laufenden Beschäftigungsverhältnissen bzw. zur Beendigung solcher automatisierte Entscheidungen zulässig sein und zwar dann, wenn die Anzahl der zu entlassenden Arbeitnehmer und zu berücksichtigenden Kriterien so hoch ist, dass eine durch den Algorithmus (bspw. auf Basis eines Scorings) generierte Vorschlagsliste nicht mehr in jedem Einzelfall durch einen menschlichen Entscheider überprüft werden kann. Dies dürfte aber einen eng begrenzten Ausnahmefall darstellen.

§ 3 Dashboards

Die Generierung von People Analytics-Daten erfolgt in vielfältiger Weise im Hintergrund, wobei hierfür verschiedene Log-Dateien von Systemen, unzählige Datenbanken (SQL, OLAP etc.) sowie ggf. verschiedene sonstige Softwaresysteme als Datengrundlage herangezogen werden. Die Ergebnisse der People Analytics werden wiederum in der integrierten Datenbank des People Analytics-Systems gespeichert oder – falls diese im Rahmen eines Personalmanagement-Systems erfolgen – im HRM-System selbst. Hierbei handelt es sich zumeist aber um Rohdaten, die in Form einer Datenbank gespeichert und zunächst „umgewandelt“[1340] werden müssen, um für den Menschen zugänglich zu sein.

Beispiel: Das IT-System speichert für die E-Mail-Auswertung das aktive Fenster des Computers und den Empfänger der E-Mail, die gerade getippt wird, alle 10 Sekunden, um eine Zeitauswertung des Arbeitstags zu ermöglichen. Im Protokoll speichert der Computer alle 10 Sekunden eine Zeile ab, beispielsweise in der Form „2020-03-26 08:03:10 E-Mail: true, Rcpt: max@mustercompany.de“.

Die Anzeige hunderter Datenbankzeilen oder Log-Dateien ist für den Mensch, der auf dieser Basis entscheiden will, kaum hilfreich. Hier benötigt es eine Abfrage (z.B. in der Abfragesprache SQL bei Datenbanken), die diese Daten aggregiert und selektiert, sodass diese in einer Form ange-

1340 Genauer: Mittels spezifischen Datenbank-Abfragen, wie SQL-Befehle, aggregiert und selektiert werden.

zeigt werden können, die auch hilfreich für den Menschen ist.[1341] Dies geschieht häufig in Form eines Dashboards.

Hiermit könnte dem Arbeitnehmer beispielsweise angezeigt werden, dass er am Tag 3 Stunden mit dem Schreiben von E-Mails verbracht hat und der E-Mail-Verkehr mit max@mustercompany.de insgesamt 45 Minuten in Anspruch genommen hat. Mit Hilfe eines Kuchendiagramms der täglichen Arbeitszeit ließe sich das beispielsweise gut darstellen.

Bei solchen Dashboards stellt sich jedoch insbesondere aus datenschutzrechtlicher Sicht die Frage, welche Kategorien von Daten an welche Empfänger (nur der Arbeitnehmer selbst [nachfolgend **I.**], die Abteilungs- oder Unternehmensleitung [**II.**]) übermittelt werden und inwiefern diese aggregiert, bzw. anonymisiert werden (müssen) (nachfolgend **III.**).

I. Persönliches Dashboard für den Arbeitnehmer

Die datenschutzrechtlich am wenigsten einschneidende Maßnahme ist jene, bei der ausschließlich der Arbeitnehmer Zugriff auf seine über die IT-Systeme gesammelten Daten bekommt und Dritte (also z.B. des Team-, Abteilungs- oder Unternehmensleiters) keine Einsicht erhalten können. Derjenige, über den die Daten gesammelt werden, behält grundsätzlich die Datenmacht, auch wenn der Arbeitgeber der Verarbeiter ist. Sichergestellt werden kann dies beispielsweise durch eine Verschlüsselung, bei welcher nur der Arbeitnehmer das Entschlüsselungskennwort hat.[1342] Dennoch handelt es sich bei diesen Daten – auch aus Sicht des Arbeitgebers als Verarbeiter – um personenbezogene Daten, auch wenn er keine Möglichkeit zum direkten Zugriff hat.[1343] Dies ergibt sich bereits aus Erwägungsgrund 26 der DSGVO.[1344]

1341 Von der Wichtigkeit einer entsprechenden Aufbereitung spricht *Jentzsch*, HR Performance 2013, 60 (61).

1342 Vgl. hierzu auch zum sog. Hashing von Daten *Voitel*, DuD 2017, 686; zu den verschiedensten Formen der Verschlüsselung kompakt im Überblick Paal/Pauly/*Martini*, Art. 32 DSGVO Rn. 34a.

1343 Siehe bereits **D. § 1 I. 4. c).**

1344 Vgl. HdbIT-DSR/*Conrad et al.*, § 22 Cloud Computing, Rn. 262 f.

1. Datenschutzrechtliche Verarbeitungsgrundlage

a) Einwilligung

Für ein Dashboard, auf welches nur der Arbeitnehmer Zugriff hat, kommt zuvorderst die Einwilligung nach Art. 6 Abs. 1 lit. a, 7 DSGVO i.V.m. § 26 Abs. 2 BDSG in Betracht. Voraussetzung ist, dass diese eindeutig, freiwillig, in informierter Weise für einen oder mehrere bestimmte Zwecke abgegeben wurde.[1345] Diese kann im Beschäftigungsverhältnis auch regelmäßig in elektronischer Form erteilt werden, wie § 26 Abs. 2 S. 3 BDSG klarstellt.

Umgesetzt werden kann dies in der Praxis in formeller Hinsicht dadurch, dass der Arbeitnehmer beim ersten Start des Dashboards und somit vor der damit verbundenen Sammlung und Verknüpfung diverser IT-Systemdaten mit seinem Benutzerprofil, in einem Anmelde- oder Registrierungsbildschirm seine Einwilligung per Mausklick abgibt. Dies ist bei elektronischen Diensten absoluter Praxisstandard, der auch im Rahmen des Arbeitsverhältnisses angewandt werden kann.

Die Besonderheit ist, dass die ansonsten im Arbeitsverhältnis eher zweifelhafte Freiwilligkeit in dieser Situation unproblematisch ist, da der Arbeitgeber auf die verschlüsselten Daten, die im Rahmen des Dashboards für den Arbeitnehmer gesammelt werden, keinen inhaltlichen Zugriff erhält, sofern eine ausreichend sichere Verschlüsselungsmethode nach dem Stand der Technik (vgl. Art. 32 Abs. 1 lit. a DSGVO) eingesetzt wird.[1346]

Für symmetrische Verschlüsselungsverfahren wird derzeit AES-128/192/256 empfohlen, wobei die Kennziffer die Bit-Länge angibt. Je höher die Bit-Länge, desto sicherer ist die Verschlüsselung. Bei asymmetrischen Versschlüsselungsverfahren wird mindestens ECIES-250, DLIES-2000, RSA 2000, curve25519, curve448 oder ECC-Brainpool empfohlen, wobei bei ECIES eine Mindestbitlänge von 384 Bit vorliegen sollte und bei RSA/DLIES 3072 Bit.

1345 Zu den materiellen Voraussetzungen der Einwilligung, siehe **D. § 1 III. 2. a) bb)**.

1346 Von den Branchenverbänden werden immer wieder aktualisierte Handreichungen zum „Stand der Technik“ herausgegeben, so z.B. aktuell *TeleTrusT - Bundesverband IT-Sicherheit e.V.*, IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum "Stand der Technik" technischer und organisatorischer Maßnahmen, <www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/2020-01_TeleTrusT_Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DEU.pdf>.

Wird mit Hashing-Verfahren gearbeitet, so sollte SHA-256/384/512 bzw. SHA3-256/384/512 verwendet werden; SHA1 und MD5 entsprechen hingegen nicht mehr dem Stand der Technik.[1347]

Selbstverständlich bedarf es bei den Verschlüsselungstechniken immer wieder Aktualisierungen, insbesondere wenn die Rechenkapazität steigt und die Algorithmen somit schneller geknackt werden können oder sich ein Algorithmus im Nachhinein als unsicher darstellt, weil eine Schwachstelle gefunden wird. Arbeitgeber müssen daher als Verantwortliche im Sinne der DSGVO den technischen Fortschritt immer beobachten und ggf. unverzüglich handeln.

Voraussetzung ist, dass ausschließlich der Arbeitnehmer das erforderliche Kennwort zur Entschlüsselung hat. Andernfalls ist die Freiwilligkeit zweifelhaft, da ein etwaiger Druck seitens des Arbeitgebers bestehen könnte, die Einwilligung zur Datenverarbeitung abzugeben, wenn dieser hierdurch ebenfalls Zugriff auf die Arbeitnehmerdaten bekommen könnte.

b) Erforderlichkeit gem. § 26 Abs. 1 S. 1 BDSG / Berechtigtes Interesse gem. Art. 6 Abs. 1 lit. f DSGVO

Im Einzelfall kann sich darüber hinaus die Frage stellen, ob eine Datenverarbeitung für das persönliche Dashboard erforderlich im Sinne von § 26 Abs. 1 S. 1 BDSG sein kann, m.a.W. dem Arbeitnehmer die Nutzung des Dashboards „aufgezwungen" werden kann. Dies kann beispielsweise dadurch geschehen, dass das Dashboard automatisch als Startseite des Browsers aufgerufen wird oder dem Arbeitnehmer täglich eine E-Mail mit einer zusammenfassenden Darstellung durch das System zugesandt wird.

Wenn der Arbeitgeber unabhängig vom Einverständnis des Arbeitnehmers möchte, dass dies in Form einer täglichen Zusammenfassung dem jeweiligen Arbeitnehmer angezeigt wird, würde die Einwilligung als Legitimationsgrundlage kein taugliches Mittel darstellen, da diese jederzeit widerrufbar ist. Der Arbeitgeber kann zwar nicht sicherstellen, dass seine Beschäftigten die Daten wirklich zur Selbstoptimierung[1348] nutzen, dennoch

---

1347 *TeleTrusT - Bundesverband IT-Sicherheit e.V.*, IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum "Stand der Technik" technischer und organisatorischer Maßnahmen, <www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/2020-01_TeleTrusT_Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DEU.pdf>, S. 25.

1348 Vgl. **C. § 4 V.**

ist die Wahrscheinlichkeit einer Kenntnisnahme und Auseinandersetzung mit den Daten wahrscheinlicher.

Da bereits die Geeignetheit unerwünschten Scorings zur Erreichung des angestrebten Ziels für zweifelhaft ist,[1349] muss dies erst recht für die Nutzung der durch das Scoring gewonnen Daten für den Arbeitnehmer gelten. Auch hier besteht die Problematik, dass die Anzeige der Daten in aller Regel nicht zur gewünschten Selbstoptimierung führt, wenn ein Arbeitnehmer solche Auswertungen – aus welchem Grund auch immer – ablehnt. Jedenfalls besteht jedoch auch hier ein milderes Mittel: Die Einholung einer Einwilligung beim Arbeitnehmer.

c) Betriebsvereinbarung

Unter den bereits getroffenen Erwägungen stellt sich die Frage, ob eine Verarbeitung auf Basis einer Betriebsvereinbarung legitimiert werden könnte oder ob der Umstand, dass die Einwilligung schnell und per Mausklick abgegeben werden kann, der Möglichkeit der Verarbeitung auf Grundlage einer Betriebsvereinbarung entgegensteht.

Auch in einer Betriebsvereinbarung müssen sich die Betriebspartner an die Datenschutzgrundsätze und somit insbesondere an die Datenminimierung bzw. Erforderlichkeit der Datenverarbeitung halten. Sie haben jedoch das Recht, per Betriebsvereinbarung eigene Legitimationstatbestände zu schaffen, die sich am Grundsatz der Erforderlichkeit orientieren bzw. die Rahmenbedingungen der Einwilligung spezifizieren.[1350]

Aufgrund der mangelnden Geeignetheit und objektiven Erforderlichkeit der Datenverarbeitung bei einem Dashboard, bei welchem ausschließlich der Beschäftigte darauf Zugriff hat, kann diese auch durch eine Betriebsvereinbarung nicht legitimiert werden. Die zweifelhafte Eignung der Datenverarbeitung zur Erreichung des erstrebten Zwecks kann hierdurch ebenfalls nicht verbessert werden; auch hier steht die Einwilligung als milderes Mittel, das das Selbstbestimmungsrecht des Betroffenen besser wahrt und gleich effektiv ist, einer Erforderlichkeit entgegen.

Möglich bleibt es aber, die Bedingungen für die Einwilligung zu konkretisieren, wobei die Grundsätze aus Art. 7 DSGVO gewahrt bleiben müssen. Es wäre also nicht möglich, die Einwilligung oder die Widerruf-

1349 Vgl. die Ausführungen unter **E. § 1 III. 2. c) dd) (2) (c)**.
1350 Hierzu siehe bereits **D. § 1 V. 2**.

lichkeit dieser (Art. 7 Abs. 3 S. 1 DSGVO) per Betriebsvereinbarung vollständig auszuschließen.[1351]

Aufgrund mangelnder Rechenkapazitäten bei einem Tochterunternehmen eines Konzerns könnte eine (Konzern-)Betriebsvereinbarung jedoch die Datenübermittlung an eine Konzernzentrale legitimieren, insbesondere, wenn es sich (wie häufig) um zentralisierte IT-Strukturen handelt. Die DSGVO kennt selbst kein ausdrückliches Konzernprivileg. Lediglich in Erwägungsgrund 48 ist festgeschrieben, dass für die Übermittlung innerhalb der Unternehmensgruppe für interne Verwaltungszwecke ein berechtigtes Interesse bestehen kann. Art. 88 Abs. 2 DSGVO fordert bei einer Konzernübermittlung entsprechende Konkretisierungen in einer Betriebsvereinbarung.[1352] Diesbezüglich können in einer Konzernbetriebsvereinbarung spezifischere Vorschriften geschaffen werden.[1353]

2. Betriebsverfassungsrechtlicher Kontext

Bei der Einführung von Dashboards hat der Betriebsrat ein Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG, da es sich um eine technische Einrichtung handelt, die geeignet ist, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.[1354] Nach § 75 Abs. 2 BetrVG hat der Betriebsrat sicherzustellen, dass der Arbeitgeber die Persönlichkeitsrechte der betroffenen Arbeitnehmer wahrt. Hierzu gehört auch sicherzustellen, dass der Arbeitgeber keinen heimlichen Zugriff auf das System erhält. Dem Betriebsrat daher auch ein Schutzauftrag hinsichtlich der Integrität und Sicherheit eines solchen Datenverarbeitungssystems.

Zur frühzeitigen und effektiven Ausübung seiner Rechte stehen dem Betriebsrat bereits in der Planungsphase nach § 90 Abs. 1 Nr. 2 BetrVG umfassende Unterrichtungs- und Beratungsrechte zu. Es müssen ihm auch die erforderlichen Unterlagen zur Beurteilung vorgelegt werden.

1351 Vgl. EuArbRK/*Franzen*, Art. 88 DSGVO Rn. 11; EuArbRK/*Franzen*, Art. 7 DSGVO Rn. 6; ferner *Körner*, NZA 2019, 1389 (1392).

1352 Dazu unten im Überblick **F. § 2 III**.

1353 Die Diskussion über die Reichweite solcher Vereinbarungen befindet sich jedoch noch in Kinderschuhen, vgl. *Körner*, NZA 2019, 1389 (1395); *Wurzberger*, ZD 2017, 258 (259 f.).

1354 Trotz des Wortlauts „bestimmt" (vgl. § 87 Abs. 1 Nr. 6 BetrVG) reicht die Geeignetheit zur Überwachung nach st. Rspr. des BAG, vgl. hierzu bereits **D. § 2 II. 1. b**).

Durch Dashboards könnte der Arbeitgeber auch den Zweck verfolgen, dass das betriebliche Ordnungsverhalten beeinflusst wird.[1355] Es ist nicht erforderlich, dass der Arbeitgeber verbindliche Verhaltensrichtlinien aufstellt, um das Mitbestimmungsrecht aus § 87 Abs. 1 S. 1 BetrVG auszulösen; ausreichend ist bereits eine Beeinflussung durch arbeitgeberseitige Maßnahmen wie beispielsweise die Zurverfügungstellung eines Dashboards.

3. Anwendungsbeispiel: Office 365 & Microsoft Delve MyAnalytics

Um die abstrakten Ausführungen etwas zu veranschaulichen, wird im Folgenden kurz das Beispiel des Dashboards von Microsoft Office 365 bzw. Delve MyAnalytics beschrieben. Hierbei handelt es sich um ein Werkzeug, das mit der Anwendungssoftware „Office 365", die wohl in den meisten Unternehmen verwendet werden dürfte, mitgeliefert wird. Über die Nutzung von vernetzten Cloud- und Online-Diensten wird es dem sog. Office Graph, einem selbstlernenden Algorithmus aus dem KI-Bereich, ermöglicht, die Arbeit von Personen, ihren Beziehungen und Interkationen untereinander zu analysieren. Durch diese Analysen können nicht nur die Beziehungen und Interaktionen der Nutzer untereinander (siehe hierzu nachfolgend § **4**), sondern auch das Nutzungsverhalten von Programmen und Dokumenten aufgezeigt werden sowie Prognosen darüber getroffen werden, wer besonders „produktiv" ist und in welchen Bereichen verbessert werden kann oder welche Dokumente für welche Arbeitnehmer von Interesse sein könnten. MyAnalytics stellt dem Arbeitnehmer dar, wie und wofür die Arbeitszeit genutzt wurde, also wie viel Zeit in Meetings und dem Verfassen von E-Mails verbracht werden, wieviel Zeit des Tages wirkliche „Focustime" ist und wieviel ein Arbeitnehmer nach Feierabend arbeitet. Ebenfalls gibt MyAnalytics Vorschläge, wenn ineffiziente Meetings besucht werden (z.B. solche die viele Teilnehmer haben, länger als 60 Minuten dauern und in regelmäßigen Abständen wiederkehren)[1356] und gibt

1355 Siehe hierzu **D. § 2 II. 1. a**).

1356 Vgl. *Knapp*, Delve Analytics - Ich weiß wer du bist, weißt du's?, 12.11.2015, abrufbar unter: https://www.brandmysharepoint.de/delve-analytics-ich-weiss-wer-du-bist-weisst-dus/ (letzter Abruf am: 31.03.2020).

Rückmeldungen, welche Mails relevant sind und mit wem häufig und intensiv zusammengearbeitet wird.[1357]

Microsoft verfolgt zwar nicht standardmäßig den hier für notwendig erachteten Ansatz der Einwilligung bei Self-Analytics,[1358] lässt sich jedoch so durch den Administrator konfigurieren, dass sich Benutzer selbst aktiv dafür anmelden müssen. Ebenfalls wird auf der Datenschutz-Informationswebsite von Microsoft klargestellt, dass MyAnalytics nicht für die Bewertung, Überwachung, automatische Entscheidungsfindung, Profilerstellung oder Überwachung von Mitarbeitern vorgesehen ist, sondern lediglich einzelnen Personen der Einblick in ihre eigenen Statistiken gewährt wird. Auch ein Zugriff auf Informationen von anderen Kollegen wird unterbunden. Die Daten werden dazu im Exchange-Online-Postfach[1359] des jeweiligen Mitarbeiters gespeichert, sodass diese vor Zugriffen von Dritten geschützt sind.

Den Arbeitnehmern steht zudem frei, welche Daten sie in die Analytics miteinbeziehen wollen, also ob lediglich Postfachdaten (E-Mail, Kalender, Chat- oder Anrufaktivitäten) oder auch Windows 10-Aktivitätsveraufsdaten (welche Anwendungen und Apps werden auf welchen Geräten verwendet) oder inkrementelle Daten (z.B. grober Anteil gelesener E-Mails[1360]) verwendet werden sollen.[1361]

Ohne nun die technischen Details dieser Softwarelösung zu analysieren, darf grundsätzlich davon ausgegangen werden, dass unter den bisher genannten Gesichtspunkten diese Form der Analytics eine grundsätzlich datenschutzkonforme Umsetzung darstellen. Voraussetzung ist selbstver-

---

1357 Eine kurze Analyse der Analyticsmöglichkeiten von Office 365 gibt *Hanke*, Datenschutzprobleme und Gestaltungsmöglichkeiten in der Praxis, 2018, abrufbar unter: https://www.arbeitnehmerkammer.de/fileadmin/user_upload/Veranstaltungen/Veranstaltungsdokumentation/Downloads/Datenschutzrecht_20180221_Hanke.pdf (letzter Abruf am: 31.03.2020).

1358 Dies widerspricht zwar dem Grundsatz „Privacy by Default" (Art. 25 DSGVO), dieser Grundsatz trifft jedoch grundsätzlich den Verantwortlichen, der das Produkt einsetzen möchte, also vornehmlich den Arbeitgeber.

1359 Das ist der E-Mail-Server von Microsoft; die Daten unterliegen hier einem besonderen Schutz vor Zugriffen Dritter.

1360 Es werden keine Leseraten für E-Mails, die an weniger als 5 Empfänger versandt wurden, angezeigt. Ebenso kein prozentualer Anteil, sondern lediglich, ob die Leserate über oder unter einem bestimmten Schwellenwert liegt, der von der Anzahl der E-Mail-Empfänger abhängt.

1361 Siehe das Datenschutzhandbuch für myAnalytics-Administratoren (Stand: 14.03.2020), https://docs.microsoft.com/de-de/workplace-analytics/myanalytics/overview/privacy-guide (letzter Abruf am: 31.03.2020).

ständlich, dass der Arbeitgeber das Modell der Einwilligung wählt und kein persönlicher Druck aufgebaut wird, sich für myAnalytics anzumelden, da es ansonsten an der Freiwilligkeit mangeln würde und eine Einwilligung daher unwirksam wäre.

II. Dashboard mit Zugriff auf Informationen der einzelnen Arbeitnehmer

Anders als das individuelle Dashboard für den Arbeitnehmer, das durch eine Einwilligung problemlos legitimiert werden kann, birgt ein Dashboard für Vorgesetzte oder Teams mit Zugriff auf Informationen der einzelnen Arbeitnehmer aus datenschutzrechtlicher Perspektive ein größeres Risikopotential. Insbesondere besteht eine große Gefahr der Überwachung, wenn Verhaltens- und Leistungsdaten minutengenau und mit maximaler Detailtiefe durch Vorgesetzte überwacht werden können.

Vielerorts werden bereits (insbesondere im HR-Bereich) Dashboards eingesetzt, um einen Überblick über die Arbeitnehmer zu erhalten. Solange es sich bei den angezeigten und analysierten Daten um Stammdaten handelt und keine Überwachung ausgelöst wird, ist dies datenschutzrechtlich mit Bezug auf *People Analytics* unproblematisch.[1362] De facto ist es dieselbe Situation, wie wenn der Personalverantwortliche in die Akte blicken würde – in diesem Fall lediglich in digitaler Form.

Moderne Lösungen gehen jedoch weiter und ermöglichen auch eine Verhaltens- und Leistungsüberwachung auf Team-/Abteilungs- oder Unternehmensebene in diversen Abstufungen.

Es muss daher grundsätzlich zwischen zwei verschiedenen Dashboard-Typen unterschieden werden. Einerseits (nachfolgend **1.**) solche Dashboards, die nur die digitale Personalakte darstellen sowie andererseits „Überwachungsdashboards" mit unterschiedlicher Detailtiefe (nachfolgend **2.**). Während erstere keine Neuigkeit darstellen, sondern im Rahmen von Personalmanagementsystemen bereits seit Jahrzenten angewandt werden, gewinnen zweitere hauptsächlich mit dem Aufkommen von *Advanced People Analytics* an Popularität. Diese ermöglichen eine Leistungs- und Verhaltenserfassung und -bewertung in Echtzeit und eröffnen Verantwortungsträgern die Option, auf dynamische Veränderungen im Unternehmen flexibel und schnell zu reagieren.

1362 Siehe die diesbezüglichen Ausführungen zu Simple People Analytics, **E. § 1 III. 1.**

In beiden Varianten scheidet in aller Regel die Einwilligung mangels Freiwilligkeit aus, da nicht ausschließlich gleichgelagerte Interessen verfolgt werden bzw. kein Vorteil für den Arbeitnehmer entsteht, sondern er vielmehr negative Folgen daraus zu befürchten hat.[1363]

1. Dashboard für den HR-Bereich ohne kontinuierliche Erfassung von Leistungsdaten (vor allem Stammdaten)

Wie bereits angedeutet, handelt es sich beim Dashboard ohne Leistungsdatenerfassung um eine datenschutzrechtlich weitgehend unproblematische Digitalisierung der Personalakte, die kein People Analytics-spezifisches Problem ist. Es wird daher im Folgenden nur kurz am Rande auf etwaige Problembereiche bei der Digitalisierung hingewiesen. Zwar werden bereits in klassischen Personalmanagement-Systemen im Rahmen der Personalakte vielfach Simple People Analytics (siehe bereits **E. § 1 III. 1.**) angewandt; hierbei handelt es sich lediglich um die Fortschreibung von Trends. Zumeist werden die Stammdaten des Mitarbeiters, sein Kenntnis- und Wissenstand, Fortbildungen, etwaige Abmahnungen, Gehaltstabellen usw. angezeigt.

Sofern konzernweit ein HR-IT-System wie beispielsweise SAP SuccessFactors oder Workday eingesetzt wird, muss ein Erlaubnistatbestand zur Übermittlung von Daten an die Konzernzentrale oder andere Konzernunternehmen vorliegen. Nach Art. 88 Abs. 2 DSGVO lassen sich solche Übermittlungen in einer Konzernbetriebsvereinbarung regeln.[1364] Auf diese Problematik wird jedoch nicht näher eingegangen, da diese kein spezifisches Problem der Zulässigkeit von People Analytics-Systemen und -Verfahren ist.

Jedenfalls muss aber – unabhängig von etwaigen Übermittlungen – ein schlüssiges Berechtigungskonzept vorliegen, welches sicherstellt, dass nur diejenigen Arbeitnehmer Zugriff auf die Daten haben, für die ein solcher auch zur Erfüllung ihrer Aufgaben erforderlich ist. Hierüber hat der Betriebsrat, der ohnehin Mitbestimmungsrechte nach § 87 Abs. 1 Nr. 6 sowie umfassende Beratungsrechte nach § 90 Abs. 1 Nr. 2 BetrVG hat[1365], nach § 75 Abs. 2 BetrVG zu wachen.

1363 Vgl. hierzu auch **D. § 1 III. 2. a) bb) (2)**.
1364 *Lücke*, NZA 2019, 658 (666).
1365 Siehe bereits **E. § 1 IV. 1**.

2. Dashboard mit Leistungserfassung für Team- und Abteilungsleiter

Eine erweiterte Möglichkeit des Dashboards stellt Daten von Advanced People Analytics nicht nur für den konkreten Arbeitnehmer, sondern auch für die jeweils Personal- und Fachverantwortlichen dar. Dies bietet die Möglichkeit, jederzeit die Performance der eigenen Team- oder Abteilungsmitglieder einzusehen und rasch bei Fehlentwicklungen gegensteuern zu können bzw. „Top-Performer" gezielt weiter zu fördern oder Boni o.ä. zu gewähren.

Relevant ist, dass die Arbeitnehmer nicht einem dauerhaften Überwachungsdruck durch Analytics-Maßnahmen und ein damit verbundenes Monitoring ausgesetzt werden.[1366] Die Zulässigkeit solcher Maßnahmen hängt jedoch vom Einzelfall ab. So können – wie bereits unter **E. § 1 III. 2. a) cc) (4)** dargestellt – in Call-Centern sog. *Bedienerplatzreports*[1367] zulässig sein, wenn dies für eine effektive Steuerung der Arbeitsplätze notwendig ist, andererseits aber Belastungsstatistiken in der Versicherungsbranche unzulässig sein, wenn hierdurch das gesamte Arbeitsspektrum auf elektronischem Wege anhand quantitativer Kriterien durchgehend analysiert wird.[1368]

Letztlich hängt der zulässige Umfang der Datenverarbeitung insbesondere vom konkreten Zweck und der Absicherung für eine zweckfremde Verarbeitung ab. Dieser Maßstab gilt insbesondere auch für die Darstellung in Dashboards. Der jeweilige innerbetriebliche Empfänger der Daten spielt daher eine entscheidende Rolle.

Beispiel: Bei der Analyse der täglichen Bildschirmarbeitszeit durch einen (unabhängigen) Arbeitsmediziner ist die Gefahr eines individuellen Überwachungsdrucks überschaubar, wenn die Daten ausschließlich durch diesen im Rahmen von gesundheitspräventiven Maßnahmen evaluiert werden (z.B. wie viele Stunden sitzt ein konkreter Beschäftigter täglich vor dem Bildschirm). Hingegen könnte dieselbe Auswertung bei einer Anzeige für den Vorgesetzten zu einem unzulässigen Überwachungsdruck führen. Letzterer könnte aus der Zeitangabe schlussfolgern, dass bestimmte Arbeitnehmer zu wenig arbeiten und daraus personelle Maßnahmen herleiten.

Ebenso kann die Darstellung von Team-Leistungsdaten für den Teamleiter zur Koordinierung des Teams erforderlich sein, nicht hingegen auf

1366 Diesbezüglich gelten dieselben Voraussetzungen wie unter **E. § 1 III. 2. a) cc) (4)** dargestellt.
1367 BAG, Beschl. v. 30.08.1995 – 1 ABR 4/95, NZA 1996, 218.
1368 BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205.

dieser detaillierten Basis für den Abteilungsleiter; für letzteren reichen i.d.R. aggregierte Daten auf Team-Ebene aus, um wiederum die Teams zu koordinieren.

Es ist zu beachten, dass der Arbeitnehmer in bestimmte Datenverarbeitungen (z.B. im Beispiel in die Auswertung durch den Arbeitsmediziner) einwilligen kann, da in Situationen, in denen dem Arbeitnehmer lediglich Vorteile aus der Einwilligung erwachsen oder gleichgelagerte Interessen verfolgt werden, eine Freiwilligkeit nach § 26 Abs. 2 S. 2 Alt. 2 BDSG vermutet wird.[1369] Dieselbe Darstellung könnte bei einem anderen Empfänger (selbst wenn sie demselben Zweck diente) jedoch zu hohen Zweifeln an der Freiwilligkeit führen (z.B., wenn die Einwilligung zur Darstellung beim Vorgesetzten erfolgt). Bei letzterem könnte sich der Arbeitnehmer genötigt fühlen, die Einwilligung abzugeben, um keine Repressalien befürchten zu müssen.

Die Leistungsüberwachung mittels Dashboards ist nicht ausgeschlossen, wenn hierdurch kein Überwachungs- und Anpassungsdruck erzeugt wird. Dies wäre beispielsweise der Fall, wenn monatliche Leistungsbeurteilungen durch den Vorgesetzten erfolgen oder bestimmte Ziele zu Monatsbeginn vereinbart werden und am Ende des Monats überprüft wird, inwiefern diese Ziele durch die jeweiligen Arbeitnehmer eingehalten wurden. Letzteres könnte in elektronischem Wege erfolgen, wenn zu Monatsbeginn bestimmte Aufgaben verteilt werden und der laufende Fortschritt betreffend diese vereinbarten Ziele hierbei verfolgt wird (z.B. im Rahmen von Projekten). Zum Monatsende könnte eine Auswertung erfolgen, welche der vereinbarten Ziele inwieweit erreicht wurden. Anders als im unter Ziff. **E. § 1 III. 2. a) cc) (4)** dargestellten Beispiel werden durch diese (Projekt-)Fortschrittsüberwachung nicht alle wesentlichen Aspekte in quantitativer und qualitativer Hinsicht überwacht, sondern es erfolgt lediglich eine deutlich weniger detaillierte Überwachung der einzelnen Arbeitsabschnitte. Insbesondere bei zeitkritischen Projekten ist dies ohnehin notwendig, um bei eventuellen Problemen oder prognostizierten Engpässen schnell und flexibel reagieren zu können, z.B. indem ein weiterer Arbeitnehmer ins Team genommen wird. Eine solche Datenverarbeitung wäre erforderlich und verhältnismäßig für die Durchführung des Beschäftigungsverhältnisses nach § 26 Abs. 1 S. 1 BDSG.

Klar ist auch, dass dieses Beispiel nicht auf jeden Arbeitsplatz und Arbeitnehmer übertragbar ist, sondern nur dort, wo die Arbeit mit vorgege-

1369 Zum Kriterium der Freiwilligkeit der Einwilligung, siehe auch **D. § 1 III. 2. a) bb) (2)**.

benen Arbeitszielen möglich ist. Dies ist jeweils im Einzelfall zu beurteilen. Insbesondere dort, wo projektbezogen mit klaren Zeitvorgaben (z.B. bei SCRUM-Projekten[1370]) gearbeitet wird oder ohnehin eine dauernde Erfassung von Arbeitsvorgängen erforderlich ist (z.B. in der Logistik) und Arbeitnehmer mit einer Überwachung der Kennzahlen rechnen müssen, erzeugen solche Maßnahmen keinen unzulässigen Überwachungsdruck und sind daher als zulässig zu erachten, soweit für die Leistungsbeurteilung keine weiteren Daten hiermit verknüpft werden, um ein detaillierteres Abbild des Beschäftigten zu bekommen.

Bei den innerbetrieblichen Empfängern muss darauf geachtet werden, dass ein Zugriff auf diese Daten ebenso nur im Rahmen der Erforderlichkeit möglich ist.

Aus betriebsverfassungsrechtlicher Hinsicht gelten dieselben Maßstäbe wie bei Advanced People Analytics, d.h. der Betriebsrat hat zwingende Mitbestimmungsrechte aus § 87 Abs. 1 Nr. 6 BetrVG hinsichtlich der zugrundeliegenden Datenerfassung; ggf. auch aus § 87 Abs. 1 Nr. 1 BetrVG, wenn nicht nur das Leistungsverhalten untersucht wird. Wird die Gestaltung der Lohnstruktur daran angeknüpft, so können auch Mitbestimmungsrechte aus § 87 Abs. 1 Nr. 10 und 11 BetrVG entstehen.[1371] Darüber hinaus besteht eine Unterrichtungs- und Beratungspflicht nach § 92 Abs. 1 BetrVG, da es sich insofern auch um Personalplanungsmaßnahmen i.w.S. handelt.[1372]

Aufgrund diverser Mitbestimmungsrechte und der Pflicht, mit dem Betriebsrat zu verhandeln, empfiehlt es sich dringend, konkretisierende („*spezifischere*“) Regelungen zu Dashboards in Betriebsvereinbarungen zu treffen. Hierdurch können die Unsicherheiten, die bei einer Anwendung von § 26 Abs. 1 S. 1 BDSG bestehen (Inwiefern sind die Daten erforderlich? Welche Empfänger benötigen die Daten? Ab welcher Ebene muss aggregiert werden? Ab welcher Aggregationsebene kann von einer Anonymität im Unternehmen ausgegangen werden?), vermieden werden. All diese Fragen lassen sich in einer Betriebsvereinbarung, die legitimierend für die Datenverarbeitung ist, regeln.

1370 Hier erfolgen einzelne „Sprints“ mit täglichen Besprechungen der Mitglieder. In jedem „Sprint“ werden Ziele festgelegt, die bis zu einem bestimmten Termin erledigt sein müssen, vgl. zur dieser Methode der Projektarbeit HdbIT-DSR/*Sarre*, § 1 Erstellung und Pflege von Software, Rn. 60.

1371 Hierzu siehe bereits oben **D. § 2 II. 1. c**).

1372 Siehe **D. § 2 II. 4**.

III. Dashboard mit Zugriff auf aggregierte Daten (Team-, Abteilungsebene)

Die dritte und datenschutzrechtlich weniger bedenkliche Maßnahme ist die Anzeige von aggregierten Daten z.B. auf Team- oder Abteilungsebene. Für diese Daten ist nach dem legitimationsbedürftigen Anonymisierungsvorgang[1373] und dem ggf. vorzunehmenden Kompatibilitätstest kein Datenschutzrecht mehr anwendbar, sodass der Verarbeiter die Daten nach freiem Belieben verarbeiten darf.

1. Notwendigkeit einer wirksamen Anonymisierung und k-Anonymität

Das Kernproblem, das sich hier stellt, ist allerdings die wirksame *Anonymisierung* der Daten.[1374] Die für solche Dashboards vorgenommene Anonymisierungstechnik ist die Aggregation von Daten. Eine solche liegt vor, wenn aus bestimmten Einzeldaten Durchschnittswerte gebildet oder diese durch allgemein gehaltene Aussagen (Merkmalsaggregation) ersetzt werden.[1375]

Beispiel: Wenn auf der Dashboard-Ebene die (expliziten) Identifizierungsmerkmale nicht angezeigt werden, hingegen aber die dafür beispielsweise Arbeitszeit des letzten Arbeitstages, wäre es für einen Teamleiter recht einfach festzustellen, von welchem Teammitglied diese Daten sind. In diesem Fall lägen weiterhin personenbezogene Daten vor. Etwas anderes gälte dann, wenn lediglich die durchschnittliche Arbeitszeit des Teams angezeigt wird. Selbst Ausreißer in den Daten wären in der Folge nicht mehr einer Person zuordenbar.

Als möglichen Anwendungsfall für die Merkmalsaggregation kann ein interdisziplinäres Team angeführt werden, in welchem zwei Programmierer, drei im IT-Endlevel-Support, eine Person im Marketing, eine weitere im Bereich Buchhaltung sowie ein Manager als Teamleiter arbeitet. Unterteilt man diese Personen in „IT-Personen" und „Nicht-IT-Personen", so sind die Merkmale derart aggregiert, dass eine Zuordnung zu Einzelpersonen nicht mehr möglich ist. Wird hingegen eine detaillierte Aggregation vorgenommen, z.B. nach Unternehmensbereichen, wären der Marketer, der Buchhalter und der Manager identifizierbar.

1373 Hierzu bereits **E. § 1 III. 1. b) aa)**.
1374 Grundlegend **D. § 1 I. 4. b)**.
1375 Vgl. *Dammann*, in: Simitis, Bundesdatenschutzgesetz, § 3 BDSG Rn. 207.

Diskutiert wird dies unter dem Stichwort der *k-Anonymität*.[1376] Dieser Faktor beschreibt die Anzahl der Personen, die dasselbe Merkmal haben müssen, sodass diese nicht als „Ausreißer" in den Daten identifiziert werden können. Eine höhere k-Anonymität kann beispielsweise durch die Vergrößerung bestimmter Intervalle erzielt werden.

Beispiel: Im Unternehmen soll eine Klassifizierung nach Gehaltsebenen erfolgen. Werden die Intervalle zu klein gehalten (30.000 – 30.500 Euro Jahresgehalt statt 30.000 – 35.000 Euro), könnte dies dazu führen, dass Beschäftigte hierdurch identifiziert werden, obwohl es zunächst den Anschein macht, dass anonyme Daten vorliegen. Eine Anonymisierung ließe sich durch Erhöhung des Intervalls herbeiführen.

Gefahrpotential entsteht insbesondere durch den Einsatz von Big Data, wenn beispielsweise eine Verlinkung mehrerer Datensätze erfolgt. Obwohl bestimmte Merkmale auf aggregierter Basis (mit dort ausreichendem k-Faktor) vorliegen, könnte eine Identifizierung einzelner Beschäftigter stattfinden.

Beispiel: Ein Arbeitgeber versucht Anonymität herzustellen, indem er die Datensätze aggregiert speichert und keine personenbezogenen Daten in der Datenbank ablegt. Es werden folgende Datensätze gespeichert:

Hausmeister in der Gehaltsspanne 30.000 – 40.000 Euro:	mittlere Leistung
Hausmeister in der Gehaltsspanne 50.000 – 60.000 Euro:	hohe Leistung
Außenbereichspflege in der Gehaltspanne 30.000 – 40.000 Euro:	mittlere Leistung
Außenbereichspflege in der Gehaltsspanne 50.000 – 60.000 Euro:	hohe Leistung

Auf den ersten Blick wirken diese Daten anonym und können beispielsweise die Erkenntnis bringen, dass ein höheres Gehalt zu einer höheren Leistung führt. Angenommen, es befindet sich nur ein Hausmeister „XY" in der Gehaltsspanne 50.000 – 60.000 Euro, so wäre die Angabe „hohe Leistung" ein zwar pseudonymisiertes, aber personenbezogenes Datum über XY. Wären die Tätigkeitsbereiche nicht mit der Gehaltsspanne verknüpft gespeichert worden, so läge eine höhere k-Anonymität vor, da die Personen der Außenbereichspflege ebenfalls miteinbezogen worden wären:

Leistung in der Gehaltsspanne 30.000 – 40.000 Euro:	mittel
Leistung in der Gehaltsspanne 50.000 – 60.000 Euro:	hoch

1376 *Article 29 Data Protection Working Party*, Opinion 05/2014 on Anonymization Techniques (WP 216), S. 16.

Eine direkte Zuordnung hätte daher nicht mehr erfolgen können, insbesondere wenn die Angabe der Leistung lediglich einen Durchschnittswert vieler Arbeitnehmer darstellt. Es hätte dann nicht mehr eruiert werden können, ob nun der einzelne Hausmeister in dieser Gehaltsspanne eine hohe oder niedrige Leistung erbringt.

Es zeigt sich an diesem Beispiel: Je mehr Merkmale in den Datensätzen vorhanden sind, die eine Zuordnung erlauben, desto höher ist eine Wahrscheinlichkeit der Identifizierung einer einzelnen Person.

Bei der Speicherung von solchen Daten muss also darauf geachtet werden, dass die jeweiligen k-Faktoren so hoch sind, dass durch eine Verknüpfung der Merkmale keine Identifizierbarkeit hergestellt werden kann. Eine Lösung könnte sein, die jeweiligen Faktoren individuell abzuspeichern und nicht zu verknüpfen. Im obigen Beispiel wäre es für die Berechnung der Durchschnittsleistung in einer gewissen Gehaltsspanne nicht erforderlich, dass die Daten mit dem Tätigkeitsbereich verbunden gespeichert werden.

Im dem weiter oben Beispiel von Microsoft MyAnalytics werden z.B. die Leseraten von E-Mails in zweifacher Hinsicht anonymisiert: Einerseits erfolgt ein Rendering der Leserate in die Kategorien „hoch" und „niedrig" statt der Angabe von Prozentzahlen, andererseits wird eine solche nicht angezeigt, wenn nicht mindestens fünf Empfänger die Nachricht erhalten haben (dies ist wieder ein Anhaltspunkt zur sog. k-Anonymität).[1377]

Die k-Anonymität ist nur ein mögliches Modell, die Bestimmbarkeit und somit die Anwendung des Datenschutzrechts auszuschließen.[1378] Für die Anwendbarkeit der DSGVO kommt es aber nicht darauf an, dass ein bestimmter k-Faktor vorliegt, sondern dass unter „vernünftigerweise" angewandten Mitteln zur Identifizierung eine Bestimmbarkeit ausgeschlossen ist (Erwägungsgrund 26).[1379] Für die Bewertung ist maßgeblich, wie hoch die Wahrscheinlichkeit einer erfolgreichen Re-Identifizierung einer Person ist. Ist dieses vernachlässigbar, weil es so gering ist, dann sind die Daten nicht personenbezogen und die DSGVO findet keine Anwendung.[1380]

1377 Vgl. https://docs.microsoft.com/de-de/workplace-analytics/myanalytics/overview/privacy-guide (letzter Abruf am: 16.04.2020) unter der Überschrift „Leseraten von E-Mails".

1378 Weitere Modelle zeigt *Götz*, Big Data im Personalmanagement, S. 75 auf.

1379 Zur Auslegung des Begriffs „vernünftigerweise" siehe bereits **D. § 1 I. 4. c) bb) (1)** unter dem Aspekt der Pseudonymisierung.

1380 Vgl. hierzu noch unter altem Datenschutzrecht *Brisch/Pieper*, CR 2015, 724 (727).

2. Risikobasierter Ansatz der DSGVO: Re-Identifizierungsrisiko

Ein weiterer Faktor ist das Geheimhaltungsinteresse der betroffenen Personen bzw. das Interesse Dritter an der Kenntnis bestimmter Informationen sowie Zugriffsmöglichkeiten, die das Re-Identifikationsrisiko bestimmen. Je unwichtiger die Daten und je kleiner der Zugriffskreis, desto eher sind Informationen anonym.

Beispiel: Während wohl wenig Aufwand betrieben wird, einzelne Personen herauszufiltern, wenn Gehaltsspannen in einem Unternehmen für Personengruppen veröffentlicht werden, wären die Geschäftskontakte hochrangiger Manager sicherlich höher gefährdet. Noch extremer ist es, wenn (abseits der People Analytics) beispielsweise Geheimdienstinformationen im Internet veröffentlicht werden.

Es zeigt sich bei diesen Beispielen deutlich der risikobasierte Ansatz der DSGVO.[1381] Dieser schlägt sich auch beim Risiko der Re-Identifizierung beim Einsatz von Big Data-Technologien nieder; wenn kein hohes Interesse an der Identifikation von Arbeitnehmern besteht, muss der Arbeitgeber auch nicht gezielt Schutzmaßnahmen vor solchen Technologien implementieren.

3. Betriebsverfassungsrechtlicher Kontext

Obwohl anonyme Daten vorliegen, dürfen betriebsverfassungsrechtliche Mitbestimmungsrechte nicht außer Betracht bleiben: Der Betriebsrat hat ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG, auch wenn nur anonyme Daten erfasst werden, denn das Mitbestimmungsrecht soll gerade auch den Datenschutz und die Persönlichkeitsrechte der Arbeitnehmer schützen und darauf hinwirken, dass Arbeitgeber wirksame Anonymisierungstechniken einsetzen.[1382] Sollen die genannten Daten genutzt werden, um das Verhalten von Arbeitnehmern im Betrieb zu beeinflussen, so hat der Betriebsrat auch nach § 87 Abs. 1 Nr. 1 BetrVG mitbestimmen.

Informations- und Beratungspflichten aus § 92 BetrVG verpflichten den Arbeitgeber den Betriebsrat bereits bei der Planung miteinzubeziehen, auch wenn nicht mit personenbezogenen Daten gearbeitet wird. Letztlich

---

1381 Hierzu bereits **E. § 1 I. 2. d) ee)** sowie **E. § 1 III. 2. b) (2)**; ferner *Veil*, ZD 2015, 347.

1382 Zum Schutzzweck von § 87 Abs. 1 Nr. 6 BetrVG, siehe **D. § 2 II. 1. b)**.

sollen die Statistiken dem Arbeitgeber dazu dienen, seine Personalmaßnahmen zu optimieren.

Unabhängig hiervon hat der Betriebsrat auch ein Mitbestimmungsrecht aus § 90 Abs. 1 Nr. 2 BetrVG, da solche Dashboards auch eine technische Anlage darstellen. Ob daneben auch eine Betriebsänderung nach § 111 S. 3 Nr. 5 BetrVG vorliegt, hängt von der Auswirkung der erweiterten anonymen Analysen auf die Arbeitsplätze und den Arbeitsablauf ab.[1383]

IV. Zusammenfassung

Dashboards stellen ein wichtiges Mittel zur Visualisierung der Ergebnisse aus den People Analytics dar. Da die (weiter oben dargestellten) Analysen lediglich Rohergebnisse liefern, die erst noch ein einem weiteren Verarbeitungsvorgang für die jeweiligen Endanwender aufgearbeitet und dargestellt werden müssen, sind diese in der datenschutz- und betriebsverfassungsrechtlichen Prüfung gesondert zu betrachten. Insgesamt gibt es drei Ebenen, die jeweils gesonderte Verarbeitungsvorgänge darstellen und einzeln bewertet werden müssen: (1) Die Erhebung der Daten durch IT-Systeme oder manuelle Eingaben von Daten durch Beschäftigte. (2) Die Analysen durch People Analytics-Systeme/-Maßnahmen, die die Rohdaten auswerten und hieraus weitere Erkenntnisse für das Management erzielen; sowie (3), die Umwandlung der Ergebnisse der Analysen in ein benutzerfreundliches Format – meist anhand von Dashboards über Web- oder Mobile-Applications, mit der Möglichkeit der Zusammenfassung und Aggregation von Daten, genauso wie – vereinzelt – der detailgenauen Betrachtung von Einzelergebnissen aus den Auswertungen, z.B. wenn der Teamleiter auf dem Übersichtsdashboard feststellt, dass die Teamleistung in dieser Woche gesunken ist und der Veränderung auf den Grund gehen möchte.

Dashboards sind eng verknüpft mit den zugrundeliegenden People Analytics-Auswertungen. Möglich ist es aber in diesem Zusammenhang, dass die Analysesoftware von einem Hersteller stammt, der mittels einer API[1384]

1383 Vgl. zu den Mitbestimmungsrechten (bei Advanced People Analytics) bereits **E. § 1 IV. 2.**

1384 „Application Programming Interface“, eine Anwendungs-Programmierschnittstelle, die einen standardisierten und veröffentlichten Zugriff auf das System ermöglicht, um weitere Anwendungen auf Basis des technischen Systems zu erstellen, vgl. auch *Fischer/Hofer*, Lexikon der Informatik, S. 45 Stichwort "API"; siehe aus der juristischen Literatur auch *Janik*, in: Geppert/Schütz,

die Auswertung durch andere Softwares ermöglicht. So könnte sich ein Unternehmen dafür entscheiden, ein anderes Dashboard einzusetzen als jenes, das vom Hersteller der PA-Software zur Verfügung gestellt wird (beispielsweise, weil es einfacher zu bedienen oder übersichtlicher ist). In solchen Fällen muss der Verwender der Software dann auch darauf achten, dass die Dashboard-Software den Datenschutzbestimmungen entspricht (insbesondere betreffend die Datensicherheit).

§ 4 Netzwerk-Graphen / Netzwerkanalysen

Eine besondere Art der Darstellung von Daten aus People Analytics stellen sog. Netzwerk-Graphen und Netzwerkanalysen dar. Auch solche werden grundsätzlich in Dashboards dargestellt, erfüllen aber einen anderen Zweck und geben deutlich vertieftere Blicke in die Arbeitnehmerstruktur, weshalb diesen in dieser Arbeit ein eigener Abschnitt gewidmet werden soll.

Durch die Digitalisierung der Arbeit und die konstante Erfassung von Systemdaten durch die eingesetzten Systeme (automatische Speicherungen z.B. durch Textverarbeitungssoftware in der Cloud, Auswertungen von Kollaborationslösungen wie Microsoft Teams oder Slack, Verbindungsdaten von Telefonanlagen, innerbetriebliche soziale Netzwerke wie Facebook Business oder Yammer) ist die „Vermessung der Belegschaft“[1385] möglich geworden.

People Analytics sind ein Teil dieser Vermessungsmöglichkeiten und werden immer breitflächiger eingesetzt. Der *Enterprise Social Graph* ist eine andere Form der Auswertung, die sich auf die innerbetrieblichen Kommunikationswege fokussiert und die Verbindungen zwischen einzelnen Aktoren im Netzwerk „Unternehmen“ analysiert. Hierdurch können Personen in Schlüsselpositionen sowie wichtige Kommunikationswege und -probleme identifiziert werden.[1386] Die organisatorische Netzwerkanalyse gehört ebenfalls zum breiten Themenfeld der People Analytics.

Mithilfe solcher Auswertungen lässt sich insbesondere feststellen, wo Vertrauen in Organisationen besteht und wer die Träger der Unterneh-

---

Beck'scher TKG-Kommentar, § 48 TKG Rn. 17 (allerdings spezifisch zu APIs bei Fernsehgeräten).

1385 So auch der Titel der Ausarbeitung zu diesem Thema von *Höller/Wedde*, Die Vermessung der Belegschaft.

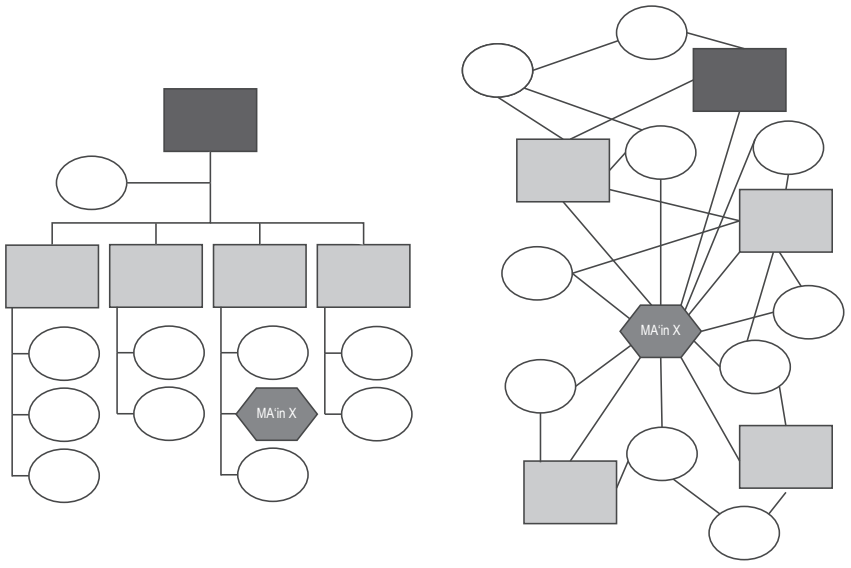
1386 Vgl. *Höller/Wedde*, Die Vermessung der Belegschaft, S. 10 ff.

menskultur sind. Dies hilft Unternehmen festzustellen, an welcher Stelle Innovation, Kreativität und Prozesse unterstützt oder behindert werden.[1387] Deutlich sichtbar wird in solchen Analysen, dass es neben der formellen Organisation (Hierarchie) auch noch eine informelle gibt und die Kommunikation nicht streng entlang von Hierarchielinien verläuft, sondern auch oftmals direkt zwischen den Wissensträgern (umso mehr, je schlechter eine Hierarchiestruktur funktioniert).

Beispiel: Eine Mitarbeiterin (X) befindet sich in der Hierarchiestruktur am unteren Ende und hat daher niemanden unter sich. Nach der formellen Organisation würde sie sich somit am Ende der Kommunikationskette befinden; Kommunikationswege nach formeller Struktur würden daher über den Vorgesetzten nach oben verlaufen und über andere Vorgesetzte wieder nach unten zu anderen Arbeitnehmern. Nach einer Analyse des unternehmensinternen Kommunikationsnetzes ergibt sich allerdings, dass X sich im Mittelpunkt jeglicher Kommunikationswege befindet, die Kommunikation also nicht über die formelle Struktur erfolgt, sondern sich die Arbeitnehmer anderer Hierarchiebäume direkt an sie wenden.

1387 *Thiel*, Organisationsentwicklung 2010, 78 (79).

Abbildung 2: Formelle vs. informelle Organisation (angelehnt an Thiel 2010, S. 80 Abbildung 2)



Dieses Beispiel zeigt, dass die Mitarbeiterin X wohl hohe Kompetenz und/oder Vertrauen bei anderen Arbeitnehmern besitzt, obwohl aus der formalen Hierarchiestruktur zwar auf den ersten Blick der (Fehl-)Schluss gezogen werden könnte, dass sie am unteren Ende der Kette entbehrlich ist. Aus der informellen Struktur ergibt sich aber, dass sie trotz ihrer niedrigen Hierarchieposition das wichtigste Kettenglied der Kommunikationswege zwischen verschiedenen Abteilungen ist. Es wäre daher ein fataler Fehler des Arbeitgebers, diese Arbeitnehmerin zu verlieren.

Würde beispielsweise die Frage gestellt werden: „Vom wem holen Sie Rat für wichtige technische Fragestellungen?“, dann zeigt das obere Diagramm, dass sowohl Linienmanager als auch Fachkräfte in erster Linie sie fragen, sie mithin eine hohe technische Kompetenz hat.[1388] Für den Arbeitgeber lohnt es also X mit einer Gehaltserhöhung, Beförderung oder sonstigen Incentives im Unternehmen zu halten, wenn sie über einen

1388 *Thiel*, Organisationsentwicklung 2010, 78 (80).

Arbeitgeberwechsel nachdenkt. Würde das Diagramm auch den Arbeitnehmern zur Verfügung gestellt, so könnte X über ihre herausragende Stellung in der Struktur Kenntnis erlangen (sofern es ihr noch nicht bewusst ist) und möglicherweise Forderungen stellen.

Solche Netzwerkgraphen können auf verschiedene Wege erzeugt werden: Einerseits ist die Erstellung eines solchen Mithilfe von (standardisierten) Fragebögen möglich (nachfolgend **I.**), andererseits können – wie im Beispiel des Office Graph – die IT-Daten ausgewertet werden, um Kommunikationswege und Kollaborationen aufzuzeigen (nachfolgend **II.**).

I. Netzwerk-Analyse anhand von (standardisierten) Fragebögen

Im „klassischen" Sinne ist eine Netzwerk-Analyse dergestalt möglich, dass den Arbeitnehmern Fragebögen ausgehändigt (oder über E-Mail oder das Intranet) zur Verfügung gestellt werden. In diesen Fragebögen werden – je nach Art der Analyse – verschiedene Fragen gestellt, um mehr über das organisationsinterne Netzwerk zu erfahren. *Thiel* listet in seiner Ausarbeitung zur sozialen Netzwerkanalyse verschiedene Netzwerktypen auf, die analysiert werden können:[1389]

Das Arbeitsnetzwerk, welches Verbindungen im Rahmen des Tagesgeschäfts abbildet („*Mit wem tauschen Sie Informationen, Dokumente oder Ressourcen im Alltagsgeschäft aus?*"), das Strategienetzwerk, das Richtungsentscheidungen aufzeigen soll („*Mit wem sprechen Sie über Zukunft und Vision der Organisation?*), das soziale Unterstützungsnetzwerk („*Mit wem sprechen Sie über Themen, die Sie sozial und beruflich in der Organisation beschäftigten?*"), das Innovationsnetzwerk („*Mit wem kommen Sie zu Diskussionen und Treffen zusammen, um neue Ideen zu entwickeln?*") sowie das Expertennetzwerk („*Von wem holen Sie sich Rat und Wissen für Ihre Arbeit?*").

1. Datenschutzrechtliche Analyse

Die Netzwerkanalyse kann nicht anhand von anonymisierten Daten stattfinden, da ansonsten die Beziehungen der einzelnen Netzwerkakteure nicht dargestellt werden können. Mithin müssen die Analysen mit personenbezogenen Daten erfolgen und unterliegen daher dem Datenschutz-

1389 *Thiel*, Organisationsentwicklung 2010, 78 (84).

recht. Es stellt sich die Frage, ob die Daten zur Durchführung des Beschäftigungsverhältnisses erforderlich sind i.S.v. § 26 Abs. 1 S. 1 BDSG.[1390]

Eine Erforderlichkeit liegt jedenfalls vor, wenn der Arbeitgeber die Daten zur Erfüllung seiner vertraglichen oder gesetzlichen Pflichten oder Wahrnehmung seiner Rechte benötigt.[1391] Diese Zweckbestimmung der „Durchführung des Arbeitsverhältnisses" ist allerdings weit zu verstehen, sodass grundsätzlich alle mit dem Arbeitsverhältnis in Zusammenhang stehenden Maßnahmen darunter zu fassen sind.[1392] Mithin auch die Netzwerkanalyse, wenn sie dem Zweck dient, die Arbeitsorganisation und somit die Durchführung des konkreten Arbeitsverhältnisses zu optimieren.

Letztlich erfolgt eine Verhältnismäßigkeitsprüfung, bei der die Interessen des Arbeitgebers an der Datenverarbeitung (hier: Kenntnis der Netzwerkstruktur(en) im Unternehmen) mit dem Geheimhaltungsinteresse bzw. Persönlichkeitsrecht der Arbeitnehmer abgewogen und in angemessenen Ausgleich gebracht werden müssen.[1393]

Bei der Analyse der Netzwerkstruktur mit Fragebögen muss darauf geachtet werden, dass das Ergebnis betriebliche Daten sind und nicht etwa private Kommunikationswege abgefragt werden („*Mit wem gehen Sie gerne in die Mittagspause? Mit wem tauschen Sie sich über private Angelegenheiten aus?*"). Bei solchen Maßnahmen überwiegt jedenfalls das Persönlichkeitsinteresse des Arbeitnehmers, da diese Daten allenfalls am Rande für das Arbeitsverhältnis von Interesse sein könnten. Hier lassen sich Parallelen unzulässigen Fragen des Arbeitgebers bei der Einstellung und zur Auswertung von privaten E-Mails herleiten, die ebenfalls aufgrund des Geheimhaltungsinteresses des Arbeitnehmers und mangelnden Bezug zum Arbeitsverhältnis unzulässig sind.

Die oben aufgezeigten Analysen stellen jedoch den betrieblichen Kontext in den Mittelpunkt, sodass das Recht auf Privatheit (bzw. Persönlichkeitsrecht) des Arbeitnehmers grundsätzlich in den Hintergrund rückt. Es stellt sich vor allem die Frage, ob diese Analysen „erforderlich" sind, es also kein milderes, gleich effektives Mittel zur Erreichung des angestrebten Ziels gibt. Die Vorteile und Ziele der Netzwerkanalyse stehen dabei im Fokus: Es soll aufgezeigt werden, welche Arbeitnehmer in Schlüsselposi-

---

1390 Zur weiten Zweckbestimmung des Zwecks „Durchführung des Beschäftigungsverhältnisses" siehe bereits **E. § 1 I. 1. b) bb)**.

1391 BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 114.

1392 *Zöll*, in: Taeger/Gabel, DSGVO - BDSG, § 26 BDSG Rn. 38.

1393 *Maschmann*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, § 26 BDSG Rn. 18 f.

tionen im Unternehmen arbeiten bzw. wo wichtige Kommunikationswege verlaufen, um beispielsweise Probleme bei der formalen Hierarchie aufzudecken und die hierfür (eigentlich) vorgesehenen Kanäle verbessern zu können. Andernfalls könnten mitunter Arbeitnehmer übermäßig belastet werden, da für diese eine andere Aufgabe zugewiesen ist, sie aber immer nach Rat gefragt werden und hierdurch zusätzlicher Arbeitsaufwand in Form von Beantwortung von Fachfragen generiert wird.

Dafür ist das effektivste Mittel die Netzwerkanalyse, die gerade den Zweck hat, die informelle Organisationsstruktur zu beleuchten und in den Vordergrund zu bringen; mildere, gleich effektive Mittel sind nicht ersichtlich. Selbstverständlich muss dabei die Frage aufgeworfen werden, welche Erkenntnisse erzielt werden sollen. Soll lediglich das Expertennetzwerk im Unternehmen aufgezeigt werden, so wäre es nicht erforderlich, auch Fragen zum Strategie- oder Arbeitsnetzwerk zu stellen. Das gewählte Mittel muss mit dem angestrebten Ziel abgestimmt sein.

Im dargestellten Rahmen bestehen aus datenschutzrechtlicher Hinsicht daher keine Bedenken, wenn mittels der (manuellen) Netzwerkanalyse betriebliche Fragestellungen untersucht werden.

2. Betriebsverfassungsrechtlicher Kontext

Aus betriebsverfassungsrechtlichem Kontext kommt in erster Linie das Mitbestimmungsrecht aus § 94 Abs. 1 BetrVG in Betracht. Hiernach bedürfen Personalfragebögen der Zustimmung des Betriebsrats, wobei als Personalfragebogen eine formularmäßige Zusammenfassung von Fragen verstanden wird, die dem Arbeitgeber ein Bild von der Person und der Qualifikation verschaffen sollen.[1394]

Fragebögen im Rahmen von Netzwerkanalysen dienen jedoch nicht primär dazu, dem Arbeitgeber ein Bild von der Person und Qualifikation zu vermitteln, sondern das innerbetriebliche Netzwerk näher aufzudecken, weshalb weiter zu prüfen ist, ob § 94 Abs. 1 BetrVG tatsächlich für solche Fragebögen anwendbar ist. Die Norm dient dazu, sicherzustellen, dass der Arbeitgeber den Arbeitnehmern nur solche Fragen stellen kann, für die ein berechtigtes Auskunftsbedürfnis besteht.[1395]

1394 Hierzu siehe bereits **D. § 2 II. 2. a)**.

1395 BAG, Beschl. v. 21.09.1993 – 1 ABR 28/93, AP BetrVG 1972 § 94 Nr. 4 unter B. II. 1. a) der Gründe; siehe auch die Regierungsbegründung zu § 94 BetrVG, BT-Drs. IV/1786, S. 50.

Das Schutzbedürfnis im Hinblick auf die Ausforschungsgefahr besteht jedoch auch bei diesen Fragestellungen wie obiges Beispiel zu unzulässigen Fragen bei der Netzwerkanalyse zeigt. Aus der Systematik mit Abs. 2 S. 1ergibt sich, dass sich die Fragebögen auf persönliche Angaben beziehen müssen.[1396] Es handelt sich um einen zustimmungsbedürftigen Fragebogen, wenn beispielsweise Fragen für Stellenbeschreibungen und Anforderungsprofile gestellt werden, die hieraus gewonnen Daten aber auch Rückschlüsse auf Leistung oder Eignung der Befragten zulassen.[1397] Aus dem Schutzzweck der Norm lässt sich daher herleiten, dass alle formalisierten und standardisierten Erhebungen durch den Arbeitgeber (so bspw. auch Mitarbeiterbefragungen) vom Zustimmungserfordernis des § 94 Abs. 1 BetrVG erfasst sind.[1398] Zwar werden solche im laufenden Beschäftigungsverhältnis in der Regel eingesetzt, wenn dem Arbeitnehmer andere Aufgaben übertragen werden sollen,[1399] das Telos gebietet jedoch keine Beschränkung auf diesen Anwendungsbereich.[1400] Zu beachten ist, dass es aufgrund von § 5 Abs. 3 BetrVG keiner Zustimmung bedarf, wenn eine Netzwerkanalyse mit Hilfe von Fragebögen lediglich auf der Ebene der leitenden Angestellten durchgeführt wird.[1401]

Neben § 94 Abs. 1 BetrVG kommt als weiterer Mitbestimmungstatbestand, insbesondere wenn die Fragebögen am Computer ausgefüllt werden sollen, immer § 87 Abs. 1 Nr. 6 BetrVG in Betracht, wenn verhaltens- und leistungsbezogene Daten erhoben werden.[1402] Allerdings erfordert letztere Norm, dass Leistung und Verhalten mithilfe einer technischen Einrichtung überwacht werden, wobei die Überwachungseignung ausreichend ist.[1403] Während das Intranet (in welchem z.B. die Fragebögen hochgeladen werden) jedenfalls ein mitbestimmungspflichtiger Tatbestand ist,[1404] weil sich aufgrund der Log-Dateien der Webserver eine Überwachung

1396 Richardi/*Thüsing*, § 94 BetrVG Rn. 10.
1397 Richardi/*Thüsing*, § 94 BetrVG Rn. 11, jedoch etwas im Widerspruch mit den unter Rn. 10 aufgeführten Angaben, dass Fragebögen zur Leistung und zum Verhalten des Arbeitnehmers nicht erfasst sein würden.
1398 ErfK/*Kania*, § 94 BetrVG Rn. 2; siehe auch BAG, Beschl. v. 21.09.1993 – 1 ABR 28/93, AP BetrVG 1972 § 94 Nr. 4
1399 GK-BetrVG/*Raab*, § 94 BetrVG Rn. 2.
1400 So wohl – jedenfalls bei nicht-anonymen Befragungen – auch *Moll/Roebers*, DB 2011, 1862 (1864).
1401 Vgl. GK-BetrVG/*Raab*, § 94 BetrVG Rn. 8.
1402 Richardi/*Thüsing*, § 94 BetrVG Rn. 10.
1403 Zum Tatbestand von § 87 Abs. 1 Nr. 6 BetrVG siehe bereits **D. § 2 II. 1. b**).
1404 Richardi/*Richardi/Maschmann*, § 87 BetrVG Rn. 499; ebenso beim Betrieb einer Facebook-Seite *Fitting*, § 87 Nr. 6 223a.

einfach realisieren lässt, ist dies mit spezifischem Blick auf die eingestellten Fragebögen zu hinterfragen. Für letztere ist bereits zweifelhaft, ob die Fragebögen selbst eine technische Einrichtung darstellen, da diese lediglich mit Hilfe anderer technischen Einrichtungen realisiert werden. Allerdings sind an die Voraussetzungen des § 87 Abs. 1 Nr. 6 BetrVG keine allzu hohen Anforderungen zu stellen.[1405] So ist es ausreichend, wenn hierzu im Intranet bspw. ein neues Software-Modul eingesetzt wird, das diese Befragungen ermöglicht.

Im Kern steht die Frage der Überwachungseignung: Bei digitalen Fragenbögen ist diese grundsätzlich vorhanden, da die Zugriffszeiten und -daten der einzelnen Arbeitnehmer ohne hohen Aufwand erfasst werden können und damit einhergehend eine Verhaltens- und Leistungsüberwachung möglich wird. Das gleiche gilt bei elektronischen Auswertungen von manuell erfassten Fragebögen, allerdings nur für jene Arbeitnehmer, die die Auswertung durchführen.

Zu beachten ist, dass sich das Mitbestimmungsrecht nicht auf den Inhalt der Fragebögen bezieht, sondern nur auf die Form.[1406] Lediglich, wenn die Befragung ausschließlich manuell durchgeführt wird (oder eine Auswertung extern erfolgt), entfällt die Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG.

Sofern die Arbeitnehmer zur Teilnahme an der Netzwerkanalyse verpflichtet werden oder ein ähnlicher Teilnahmedruck aufgebaut wird, betrifft dies das Ordnungsverhalten im Betrieb, sodass der Betriebsrat – ebenfalls nicht zum Inhalt, aber zur Teilnahmepflicht – ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG hat.[1407]

Soweit es sich bei der Netzwerkanalyse um eine Maßnahme der Personalplanung (dies der Regelfall sein) handelt, ist nach § 92 Abs. 1 BetrVG der Betriebsrat hierüber zu unterrichten und mit ihm zu beraten.[1408] Die Unterrichtungspflicht resultiert auch aus der Ermöglichung der allgemeinen Aufgabenerfüllung des Betriebsrats nach § 80 Abs. 2 BetrVG.[1409]

1405 *Fitting*, § 87 Nr. 6 Rn. 224 f.
1406 *Fitting*, § 87 Nr. 6 Rn. 226; *Moll/Roebers*, DB 2011, 1862 (1863).
1407 Ausreichend ist bereits, wenn die Arbeitnehmer in die Richtung gelenkt werden, *Moll/Roebers*, DB 2011, 1862 (1863); allgemein zu § 87 Abs. 1 Nr. 1 BetrVG siehe bereits **D. § 2 II. 1. a**).
1408 Vgl. **D. § 2 II. 4**.
1409 *Moll/Roebers*, DB 2011, 1862.

II. Automatisierte Erstellung eines „Enterprise Social Graph"

Eine moderne Form der Netzwerkanalyse, wenn auch hiermit etwas andere Fragestellungen erarbeitet werden, stellt der *Enterprise Social Graph* dar, der durch die Auswertung der innerbetrieblichen Kollaboration (meist durch die hierbei eingesetzten Softwarelösungen selbst) erstellt wird. Anders als bei der Netzwerkanalyse anhand von Fragebögen werden den Arbeitnehmern keine spezifischen Fragen gestellt, die diese beantworten sollen, sondern die Kommunikationswege und -häufigkeiten sowie Antwortzeiten und -anzahl, angesetzte Meetings (inkl. Teilnehmer), geteilte Dokumente usw. automatisiert ausgewertet und somit ein Netzwerk der digitalen Kollaboration aufgezeichnet. Ermöglicht wird diese Form der Auswertung durch die zunehmende Digitalisierung und immer leistungsfähigere Kollaborationslösungen, welche die gesamte innerbetriebliche Zusammenarbeit abbilden.

Als wohl populärstes Beispiel kann hier *Microsoft Office 365* genannt werden. In der Office-Suite lässt sich in vielen Unternehmen die komplette Zusammenarbeit abbilden. Gearbeitet wird in Microsoft Word, Excel, PowerPoint oder Outlook. Die Daten werden auf dem eigenen OneDrive-Speicher für individuelle Dokumente oder auf dem SharePoint-Server für im Unternehmen geteilte Dokumente, also in der (Azure) Cloud von Microsoft, gespeichert. Die Kommunikation erfolgt über Outlook und entweder einen On-Premise-Exchange-Server oder einen Exchange-Server in der Microsoft Cloud, ebenso wie die Telefonie. Nahtlos in das System fügt sich seit jüngerer Zeit Microsoft Teams ein, das kurze Chats und innerbetriebliche Telefonate und Videokonferenzen zwischen Arbeitnehmern (aber auch mit Externen) ermöglicht.

Durch das digitale Abbild des gesamten digitalen betrieblichen Lebens in einer Software-Suite lassen sich einfach sehr aufschlussreiche Auswertungen erstellen, ohne zunächst verschiedenartige Systeme verknüpfen und die Daten aufeinander anpassen zu müssen. Teilweise geschieht dies durch einen selbstlernenden Algorithmus, der die verschiedenen Quellen automatisch vernetzt und für den Benutzer veranschaulicht.[1410] Dies bedeutet aber keineswegs, dass die Systeme in sich geschlossen sind. Vielfach bieten die Software-Anbieter APIs[1411] an, um es Drittanbietern zu ermögli-

1410 *Ruchhöft*, CuA 2017, 8 (9).
1411 Siehe bereits Fn. 1384; ferner *Ruchhöft*, CuA 2017, 8 (10).

chen, diese Daten einfach auszulesen und so erweiterte Nutzungsmöglichkeiten zu generieren.[1412]

Leider ist auch dieses Thema bislang nur stiefmütterlich in der rechtswissenschaftlichen Literatur behandelt worden. In der Kommentierung von *Gola* zu § 26 BDSG ist lediglich der Hinweis vorhanden, dass solche Auswertungen allein im Rahmen von § 26 Abs. 1 S. 2 BDSG, also bei repressiven Maßnahmen, gerechtfertigt sein können.[1413] Andererseits weist insbesondere in die Praxis-Literatur darauf hin, dass aufgrund feingliedriger Einstellungen solche Anwendungen wie beispielsweise der Microsoft Graph durchaus datenschutzkonform gestaltet werden können.[1414]

Letztlich verbieten sich auch zu diesem Themenkomplex pauschalisierte Aussagen, sondern es muss im Einzelfall untersucht werden, inwiefern Netzwerkanalysen in Form eines Enterprise Social Graph durch Softwarelösungen angefertigt werden dürfen.

1. Datenschutzrechtliche Analyse

Im Vordergrund der Zulässigkeitsprüfung steht selbstverständlich (wiederum) das Datenschutzrecht, genauer § 26 Abs. 1 S. 1 BDSG. Es ist die Frage aufzuwerfen, ob und inwiefern automatisierte Analysen des Kommunikations- und Arbeitsalltags als erforderlich für die Durchführung des Arbeitsverhältnisses anzusehen sind. Im Kern handelt es sich bei dieser Abwägung, wie bereits mehrfach aufgezeigt, nicht um eine Erforderlichkeit im Sinne einer objektiven Notwendigkeit, sondern um eine Verhältnismäßigkeitsprüfung, verbunden mit einer Abwägung der Arbeitgeberinteressen mit denen der Arbeitnehmer.[1415]

1412 Bei Office 365 ist dies beispielsweise die Microsoft Graph-API, siehe https://developer.microsoft.com/de-de/graph (letzter Abruf am: 05.05.2020).

1413 *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 81.

1414 *Ruchhöft*, CuA 2017, 8 (11).

1415 Hierzu bereits ausführlich **D. § 1 IV. 2. b**), **E. § 1 I. 1. b**) **bb**), **E. § 1 III. 2. a**) **cc**) (**4**) sowie **E. § 3 I. 1. b**).

a) Legitimes Ziel

Zunächst muss es sich um ein legitimes Ziel handeln, das der Arbeitgeber mit der Einführung und Nutzung des Enterprise Social Graph verfolgt. Er benötigt also ein berechtigtes Interesse an den Daten.

Anders als bei Fragebögen, die spezifische Fragestellungen erfassen, werden beim Enterprise Social Graph alle elektronischen Logdaten mithilfe von künstlicher Intelligenz ausgewertet, um so bislang unentdeckte Zusammenhänge aufdecken zu können. Jegliche (soziale) Interaktionen wie Liken, Bloggen, Kommentieren, das Öffnen von Dokumenten (auch unbearbeitet), der Empfang, aber auch der Zeitraum zwischen Empfang und Lesen der E-Mail sowie zwischen Lesen und Versenden einer Antwort können bis ins kleinste Detail (bei Zeiträumen auf Millisekunden genau) erfasst und ausgewertet werden. Jede Interaktion stellt eine eigene Beziehung dar, die irgendwie durch einen Algorithmus bewertet werden muss.[1416] Im Unterschied zu spezifischen Fragestellungen, wo nur jene Beziehungen aufgezeigt werden, die konkret erarbeitet werden möchten, erfasst der Enterprise Social Graph auch Beziehungen, die für konkrete Fragestellungen völlig irrelevant sind. Zur Bewältigung dieser Datenflut kommen selbstlernende Algorithmen und künstliche Intelligenz[1417] zum Einsatz, die durch eine kontinuierliche Anpassung der Auswertung die relevanten Datensätze herausfiltern und für diese die spezifische Fragestellung bestmöglich gewichten und bewerten. Die Berechnungen sind hochkomplex und wären ohne leistungsfähige IT-Systeme von Menschenhand nicht zu bewerkstelligen (klassische *Big Data*-Anwendung[1418]).

Der Vorteil eines Enterprise Social Graph gegenüber der „klassischen" Netzwerkanalyse ist, dass eine Echtzeitauswertung stattfinden kann, während bei ersterer nur der Ist-Zustand zu einem bestimmten Zeitpunkt abgefragt werden kann. Ein innerbetriebliches Netzwerk ist hochdynamisch und verändert sich ständig. Durch eine Aufzeichnung über einen bestimmten Zeitraum lassen sich nicht nur tagesaktuelle Auswertungen erstellen, sondern auch die Veränderung im zeitlichen Verlauf darstellen, ohne hierfür regelmäßige Befragungen durchführen zu müssen.[1419] Diese Daten können gewinnbringend in die unternehmensinterne Organisati-

1416 Vgl. *Höller/Wedde*, Die Vermessung der Belegschaft, S. 25.
1417 Zur Funktionsweise von künstlicher Intelligenz und selbstlernenden Algorithmen siehe bereits grundlegend **C. § 2 II. 2**.
1418 Vgl. **C. § 2 II. 1**.
1419 *Höller/Wedde*, Die Vermessung der Belegschaft, S. 25.

ons- und Personalentwicklung einfließen, indem beispielsweise Missstände aufgedeckt und wichtige Akteure (sog. *Broker*) zwischen zwei in sich geschlossenen kleineren sozialen Netzwerken (sog. *Cliquen*) oder sogar zentrale Akteure, die eine Vielzahl von Cliquen vernetzen (sog. *Hidden Champions*) gefunden werden können.[1420]

Allerdings ist zu beachten, dass insbesondere bei erlaubter Privatnutzung der betrieblichen Infrastruktur auch nicht-betriebsbezogene Daten aufgezeichnet und analysiert werden, die der Privatsphäre der Nutzer zugeschrieben werden (z.B. Chats zwischen zwei befreundeten Arbeitnehmern). Auch diese würden dann eine Netzwerkstruktur darstellen. Durchaus möglich könnte es sein, dass der Arbeitgeber ebenfalls ein Interesse an diesen Daten hat. Ein solches wäre aber nicht mehr als legitim zu bezeichnen, da er für eine solche Auswertung, die rein dem Privatleben der Arbeitnehmer zuzuschreiben ist, keine Berechtigung hat; in diesem Bereich überwiegen die Grundrechte des Arbeitnehmers. Es kann eine Parallele zur Diskussion um das Einsichtsrecht des Arbeitgebers bei der erlaubten Privatnutzung des E-Mail-Accounts gezogen werden.[1421] Grundsätzlich ist nach h.M. ein Zugriff auf das E-Mail-Postfach möglich, jedoch nicht auf den Inhalt privater E-Mails.[1422]

Bei der Netzwerkanalyse ist die Auswertung von Chat-Beziehungen allerdings ein Problem: Die Software unterscheidet nicht zwischen privaten und dienstlichen Chats, sondern wertet nur die Verbindungsdaten aus, sodass private Chats zwingend miterfasst werden.

Sofern solche jedoch lediglich am Rande miterfasst werden und nicht gezielt untersucht werden (dies dürfte technisch derzeit auch noch nicht möglich sein), ist dies jedoch eine Frage der Angemessenheit der Maßnahme und nicht des Ziels. Ist das Ziel, einen Überblick über das betriebliche soziale Netzwerk und die Arbeitsbeziehungen zu erhalten, so hat der Arbeitgeber ein berechtigtes Interesse daran und es ist legitim.

1420 *Thiel*, Organisationsentwicklung 2010, 78 (81, 83 f.).

1421 Vgl. *Traut*, § 7. Überwachung der Nutzung von Internet und Social Media - Datenschutzrechtliche Grenzen, in: Thüsing/Wurth, Social Media im Betrieb, Rn. 35 f., wobei hier Chats aufgrund der Echtzeitkommunikation eher mit der Telefon- als mit der E-Mail-Nutzung verglichen werden; siehe aber Rn. 38 a.E. wonach dauerhaft fixierte Kommunikation in Form von Social Media ähnlich wie E-Mails zu beurteilen sein dürften; ferner bereits oben **D. § 3 I. 2. b**) **aa**).

1422 Statt aller LAG Berlin-Brandenburg, Urt. v. 16.02.2011 – 4 Sa 2132/10, ZD 2011, 43; *Traut*, § 7. Überwachung der Nutzung von Internet und Social Media - Datenschutzrechtliche Grenzen, in: Thüsing/Wurth, Social Media im Betrieb, Rn. 38.

b) Geeignetes Mittel

Fraglich ist aber, ob die soziale Netzwerkanalyse durch Algorithmen, also durch einen Enterprise Social Graph überhaupt ein geeignetes Mittel darstellt, die vorhandenen Arbeitsbeziehungen korrekt abzubilden und ein korrektes Bild über das Unternehmen zu verschaffen. Die Datenqualität ist für die Beurteilung von entscheidender Bedeutung; wird das Netzwerk völlig falsch dargestellt, so ist das Mittel nicht tauglich zur Erreichung des angestrebten Ziels und die Datenverarbeitung durch eine solche Software unzulässig.

Noch vor wenigen Jahren wäre die Überprüfung der Verhältnismäßigkeit klar zugunsten der Arbeitnehmer ausgefallen, da es technisch (noch) nicht möglich war, das Arbeitsleben korrekt darzustellen: Ein Großteil der Kommunikation fand früher nicht über digitale Wege statt, die hätten vermessen werden können. Durch die Digitalisierung der Arbeit ist allerdings ein Wandel eingetreten; die momentane Corona-Krise verhilft diesen Auswertungstechnologien zu einer enormen Genauigkeit, da derzeit nahezu der gesamte Alltag digital erfasst wird, wenn Arbeitnehmer im Home-Office beispielswiese über Office 365 arbeiten und ausschließlich über Microsoft Teams (als Teil der Office-Suite) kommunizieren. Aber auch abseits der Krise geht Microsoft daraus aus, dass bereits 20 Stunden der wöchentlichen Arbeitszeit durch die Auswertung von Kalender- und E-Mails erfasst und ausgewertet werden können und somit 50 % der Zeit eines Vollzeitbeschäftigten.[1423] Hierdurch besteht eine hohe Aussagekraft des digitalen Abbilds, sodass die Analyse solcher Daten durchaus geeignet ist, aussagekräftige Informationen zu erteilen. Nach der derzeitigen Krise dürfte der Digitalisierungsgrad und somit die auswertbaren Daten um ein Vielfaches höher sein, selbst wenn wieder weitgehend Normalität eintritt. Da davon auszugehen ist, dass diejenigen Beschäftigen, die digital viel zusammenarbeiten auch im analogen Bereich mehr Kontakt haben, ist der „digitale Fußabdruck" auch repräsentativ für die Netzwerkanalyse.

Aus diesem Grund wird von Experten von einer hohen Aussagekraft innerbetrieblicher sozialer Graphen ausgegangen.[1424] Der Enterprise Social

1423 *Hanke*, Datenschutzprobleme und Gestaltungsmöglichkeiten in der Praxis, 2018, abrufbar unter: https://www.arbeitnehmerkammer.de/fileadmin/user_upload/Veranstaltungen/Veranstaltungsdokumentation/Downloads/Datenschutzrecht_20180221_Hanke.pdf (letzter Abruf am: 31.03.2020).

1424 *Höller/Wedde*, Die Vermessung der Belegschaft, S. 24.

Graph stellt daher ein geeignetes Mittel zur Erreichung des angestrebten Ziels dar.

c) Erforderlichkeit

Die Erforderlichkeit einer Maßnahme ist gegeben, wenn kein milderes, gleich effektives Mittel zur Verfügung steht. Wie bereits erläutert, dient der Enterprise Social Graph, die komplexen und sich ständig verändernden Beziehungen innerhalb eines Unternehmens in Echtzeit und im Zeitverlauf darstellen zu können. Da jede Interaktion eine neue Beziehung darstellt, handelt es sich hier um hochkomplexe Netzwerke, die nur mit immenser Rechenkapazität ausgewertet und mit selbstlernenden Algorithmen (KI) gewinnbringend analysiert werden können. Menschliche Auswertungen scheiden hingegen aus.

Es sind daher keine Gründe ersichtlich, an der Erforderlichkeit des Mittels zur Erreichung des angestrebten Ziels zu zweifeln.

d) Angemessenheit

Genauer geprüft werden muss allerdings – wie bereits im Rahmen des Prüfungspunktes „legitimes Ziel" angesprochen – die Angemessenheit der Maßnahme, also die Verhältnismäßigkeit im engeren Sinne. Bei dieser Prüfung werden die jeweiligen (Grund-)Rechtspositionen der beteiligten Akteure, also der Arbeitnehmer und des Arbeitgebers miteinander abgewogen. Zu beachten ist, dass es keinen Vorrang bestimmter Rechte gibt, sondern letztlich ein Begründungsvorgang erforderlich ist, bei welchem erörtert werden muss, warum – im spezifischen Fall – das Arbeitgeberinteresse an der Kenntnis des sozialen Netzwerks höher als das Geheimhaltungsinteresse des Arbeitnehmers ist. Maßgeblich ist u.a. die Eingriffsintensität der zugelassenen bzw. verbotenen Maßnahmen in die jeweiligen Rechtspositionen, die sich gegenüberstehen.[1425]

1425 Vgl. hierzu *Traut*, § 7. Überwachung der Nutzung von Internet und Social Media - Datenschutzrechtliche Grenzen, in: Thüsing/Wurth, Social Media im Betrieb, Rn. 38 f.

aa) Unterscheidung zwischen privaten und betrieblichen Daten kaum möglich

Sofern eine Analyse rein betrieblicher Daten stattfindet, so ist eine Maßnahme mangels Eingriffs in eine geschützte Rechtsposition der Arbeitnehmer klar zulässig. Dies ist beispielsweise der Fall, wenn statt eines betrieblichen Netzwerks Umsatzkennzahlen einzelner Unternehmensbereiche, Abteilungen oder Teams einer Analyse unterzogen werden.

Beim sozialen Netzwerk des Betriebs ist dies allerdings nicht so einfach, da auch ein betriebliches Netzwerk aus Menschen besteht, die auch persönlich bzw. privat in einer Beziehung stehen. Der Mensch ist keine Maschine, die nur Arbeitsaufgaben streng nach einem vorgegebenen Arbeitsablauf abarbeitet und die vorprogrammierten und vorgesehenen Beziehungen unterhält. Vielmehr gehört zu einem guten (und vom Arbeitgeber erwünschten) Betriebsklima auch zu einem großen Teil die private Interaktion. Diese erfolgt nicht nur persönlich unter Zimmerkollegen, sondern zu einem erheblichen Ausmaß auch im Rahmen digitaler Kommunikation, bspw. durch kurze Chats, E-Mails ggf. auch terminierte Meetings, die im Kalender erfasst werden – aktuell aufgrund zahlreichen Home-Office-Konstellationen noch umso mehr.

Eine Auswertung, die sich rein auf die betriebsbezogene Kommunikation erstreckt, ist mit der derzeitigen Technik (noch) nicht möglich, da die Programme nicht den Inhalt der Kommunikation analysieren und private Beziehungen aus den Auswertungen ausschließen. Es werden als Nebenprodukt immer private Verknüpfungen im Enterprise Social Graph erfasst.

bb) Bewertung der Eingriffsintensität

Hier stellt sich die Frage, ob die Erfassung solcher Daten als „Nebenprodukt" die Erstellung eines Enterprise Social Graph im Ganzen unzulässig macht. Hier ist auf die o.g. Maßstäbe zurückzugreifen, sodass es maßgeblich auf die Eingriffsintensität ankommt.

(1) Keine heimliche Netzwerkanalyse möglich

Offensichtlich dürfte sein, dass eine Netzwerkanalyse nicht heimlich durchgeführt werden darf, da dies die Eingriffsintensität enorm steigert

und auch nicht geboten ist. Allenfalls im Bereich der repressiven Maßnahmen nach § 26 Abs. 1 S. 2 BDSG kann im Einzelfall für einzelne Personen eine solche angemessen sein,[1426] wenn beispielsweise innerbetriebliche Betrugsfälle aufgedeckt und mögliche Mittäter identifiziert werden sollen. In allen anderen Bereichen müssen die Mitarbeiter vor der Einführung eines Enterprise Social Graph über den Verarbeitungszweck, die verarbeiteten Daten sowie Folgen informiert werden (vgl. Art. 13 DSGVO). Nur dann können Arbeitnehmer, die sich u.a. auch über private Angelegenheiten über betriebliche Kommunikationskanäle (mitunter zulässigerweise) austauschen auf andere Kanäle ausweichen, wenn sie nicht wünschen, dass private Verbindungen nicht aufgedeckt werden.

(2) Inhalt/Persönlichkeitsrelevanz bzw. Kernbereichsbezug

Eine besonders schwere Beeinträchtigung liegt vor, wenn ein Grundrecht im Kernbereich betroffen ist,[1427] z.B. im Bereich des Persönlichkeitsrechts muss ein Bürger die Möglichkeit im Bereich der privaten Lebensgestaltung haben, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art ohne die Angst einer (staatlichen) Überwachung zum Ausdruck bringen zu können. So ist der Zugriff auf private Tagebücher oder Film- und Tondokumente grundsätzlich untersagt.[1428]

Zusammen mit dem Kernbereich und deshalb gemeinsam zu behandeln ist die Persönlichkeitsrelevanz bzw. der Inhalt der Kommunikation. Es ist die Frage aufzuwerfen, welche Umstände und Inhalte werden erfasst und wie persönlich sind diese? Wird auf den Inhalt der Kommunikation zugegriffen?[1429]

1426 *Gola* ist der Auffassung, dass eine Rechtfertigung allein im repressiven Bereich stattfinden kann, ohne aber im Einzelnen darauf einzugehen, vgl. *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 81.

1427 BVerfG, Urt. v. 27.02.2008 – 1 BvR 370, 595/07, BVerfGE 120, 274 (335 f.) – Online-Durchsuchungen; BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (1189) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54.

1428 BVerfG, Beschl. v. 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367 (373 f.) – Tagebuch; Urt. v. 27.02.2008 – 1 BvR 370, 595/07, BVerfGE 120, 274 (335 f.) – Online-Durchsuchungen.

1429 *Traut*, § 7. Überwachung der Nutzung von Internet und Social Media - Datenschutzrechtliche Grenzen, in: Thüsing/Wurth, Social Media im Betrieb, Rn. 33.

Derzeitige Softwarelösungen zum Enterprise Social Graph werten ausschließlich Verbindungsdaten der Kommunikation aus (Wer mit wem und wie häufig?) sowie kalendarische Einträge zu Meetings (hier aber ebenfalls nur Datum, Uhrzeit und Teilnehmer) im Falle des Office-Graphen.

In den Kernbereich von Grundrechten von Arbeitnehmern wird nicht eingegriffen; allenfalls kann das Persönlichkeitsrecht des Arbeitnehmers tangiert sein, wobei die Eingriffsintensität in das Persönlichkeitsrecht mangels Auswertung des Kommunikationsinhalts äußerst gering ist. So kann der Arbeitgeber aus der Analyse nicht ersehen, ob die Kommunikation betrieblichen Zwecken diente oder eine private Unterhaltung stattfand. Lediglich in Einzelfällen könnte eine solche Auswertung private Verbindungen aufdecken, beispielsweise wenn zwei fachfremde Arbeitnehmer einen sehr häufigen Chat-Kontakt haben, weil sie beispielsweise eine Liebesbeziehung pflegen. Der erhöhte Kontakt wäre in einem Netzwerkgraphen auffällig, wobei der Hintergrund dieser engen Beziehung durch die Analyse ebenfalls nicht offengelegt wird.

Zu beachten ist allerdings, dass aufgrund der notwendigen Information der Arbeitnehmer vor Einsatz eines solchen Systems diese die Möglichkeit haben, auf einen Kontakt über das Firmennetzwerk zu verzichten. Auf der sicheren Seite ist der Arbeitgeber jedenfalls, wenn er die private Kommunikation verbietet. Insbesondere aufgrund der unklaren Rechtslage zur Anwendbarkeit des TKG auf den Arbeitgeber bei erlaubter Privatnutzung sollte dieser, wenn Auswertungen der Verbindungsdaten stattfinden sollen, eine solche verbieten.[1430]

(3) Anlassbezogenheit und Dauer der Überwachung

Bei jeglicher Überwachungsmaßnahme – und eine solche stellt der Enterprise Social Graph ebenfalls dem Grunde nach dar – ist für die Beantwortung der Frage der Eingriffsintensität die Frage nach dem Überwachungsanlass sowie der Dauer der Überwachung zu stellen. Ein maßgeblicher Faktor ist die Anzahl der überwachten (unbeteiligten) Personen.[1431]

1430 Siehe hierzu bereits **D. § 3 I. 2**. Zwar fallen im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherte Daten zwar grundsätzlich nicht unter § 88 TKG, dennoch ist dies als Kriterium im Rahmen der Abwägung zu berücksichtigen, vgl. *Stück*, CCZ 2016, 285 (287) m.w.N.

1431 BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (1190) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54.

Schlussendlich sind diese Kriterien nichts anderes als eine strikte Anwendung des Verhältnismäßigkeitsgrundsatzes. Je eher ein Betroffener Anlass zur Überwachung gegeben hat, desto mehr muss er eine Einschränkung seiner persönlichen Rechte in Kauf nehmen. Für Personen, die keinen Anlass zur Überwachung gesetzt haben, ist eine solche von größerer Intensität.[1432]

Zur nicht-repressiven Netzwerkanalyse, die hier im Fokus der Untersuchung steht, haben die Betroffenen keinen Anlass geboten. Vielmehr möchte ein Arbeitgeber mehr über das betriebliche, informelle Netzwerk erfahren, um unbekannte Verbindungen zu erkennen und möglicherweise vorhergesehene Kommunikationskanäle zu verbessern (siehe bereits oben). Betroffen sind alle Arbeitnehmer des Betriebs, die digitale Kollaborationstools des Arbeitgebers nutzen (müssen).

Hinzu kommt, dass die Überwachung nicht nur stichprobenhaft und über begrenzte Zeiträume erfolgen kann, wenn ein tatsächliches Abbild über einen zeitlichen Verlauf erstellt werden soll. Die Überwachung der Kommunikation (und z.B. des Kalenders) zur Erstellung eines Enterprise Social Graphs muss dauerhaft erfolgen, damit sie überhaupt geeignet ist, den erstrebten Zweck zu erfüllen (siehe bereits oben **b**) und **c**)).

Dennoch ist ein Unterschied zu den vielfach vor den Gerichten ausgefochtenen Video-Überwachungsfällen herauszuheben. Während dort die Arbeitnehmer in ihrem gesamten Verhalten überwacht werden, mitunter sogar der Kommunikationsinhalt, sofern eine Audio-Aufzeichnung ebenfalls stattfindet, erfasst die Netzwerkanalyse nur einen marginalen Teil des betrieblichen Lebens (im durchschnittlichen Unternehmen etwa 50 % der Kommunikationsvorgänge[1433] und hiervon nur die Verbindungsdaten [„Metadaten"]). Die Gefahr eines „Gefühls des Überwachtwerdens"[1434] ist demnach auch ungemein geringer, wenn die Betroffenen ordnungsgemäß nach Art. 13 DSGVO informiert wurden. Transparente und klar kommu-

1432 St. Rspr.; vgl. statt aller BVerfG, Urt. v. 11.03.2008 – 1 BvR 2074/05, 1 BvR 1254/07, BVerfGE 120, 378 (402) = NJW 2008, 1505 – Automatische Kennzeichenerfassung m.w.N.

1433 *Hanke*, Datenschutzprobleme und Gestaltungsmöglichkeiten in der Praxis, 2018, abrufbar unter: https://www.arbeitnehmerkammer.de/fileadmin/user_upload/Veranstaltungen/Veranstaltungsdokumentation/Downloads/Datenschutzrecht_20180221_Hanke.pdf (letzter Abruf am: 31.03.2020).

1434 BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, BVerfGE 115, 320 (354 f.) = NJW 2006, 1939 – Rasterfahndung II; Urt. v. 11.03.2008 – 1 BvR 2074/05, 1 BvR 1254/07, BVerfGE 120, 378 (403) = NJW 2008, 1505 – Automatische Kennzeichenerfassung.

nizierte Regelungen zum eingesetzten Verfahren, zur Gewährleistung der Datensicherheit und Protokollierung verringern die Eingriffsintensität.[1435]

Ein Vergleich lässt sich vor allem zur Überwachung von Telefon- und E-Mail-Verbindungsdaten ziehen. Diese wurde in der Rechtsprechung und Literatur schon umfassend behandelt.[1436] Während nach hiesiger Auffassung das TKG auf Arbeitgeber keine Anwendung findet, sind die Abwägungskriterien auch beim allgemeinen Datenschutzrecht dieselben.

Im Bereich der Telefonie ist anerkannt, dass Arbeitgeber – bei verbotener Privatnutzung – die Verbindungsdaten, also Datum, Uhrzeit, Gesprächsdauer und Uhrzeit auch anlasslos aufzeichnen dürfen:

> „*Unter dem Gesichtspunkt des Persönlichkeitsrechts problematisch ist allein die Erfassung der vollständigen Zielnummer, und zwar ohne Differenzierung nach dienstlichen und privaten Gesprächen. Da es aber um Telefonate vom Dienstapparat geht, vom Arbeitnehmer aber erwartet werden kann, daß er seine privaten Angelegenheiten außerhalb der Arbeitszeit regelt, ist der Eingriff in das Persönlichkeitsrecht eng begrenzt.*“[1437]

Als problematisch wird in der Rechtsprechung vor allem die (vollständige) Erfassung der Zielrufnummer angesehen, da es sich dort auch um personenbezogene Daten des Empfängers handelt und für diese Speicherung eine eigenständige Legitimationsgrundlage erforderlich wäre.[1438] Aber auch im Innenverhältnis des Betriebs kann eine vollständige Erfassung im Hinblick auf das Behinderungsverbot des § 78 BetrVG problematisch sein, wenn die Gefahr besteht, dass Betriebsratsmitglieder bei ihrer Arbeit behindert werden. Dies wäre der Fall, wenn Kontakte zu einzelnen Arbeitnehmern minutiös aufgezeichnet würden.[1439]

Die zitierte Rechtsprechung behandelte im Kern immer die Erfassung der Verbindungsdaten zur Kostenkontrolle, nicht zur Auswertung im Rah-

---

1435 BAG, Beschl. v. 15.04.2014 – 1 ABR 2/13 (B), NZA 2014, 551 (553 f.) = BAGE 148, 26 = AP BetrVG 1972 § 29 Nr. 9.

1436 Einen Überblick geben *Thüsing/Traut*, § 9. Speicherung und Sichtung von E-Mails und E-Mail-Logfiles, in: Thüsing, Beschäftigtendatenschutz und Compliance, Rn. 31 ff. sowie *Thüsing/Traut*, § 10. Überwachung von Telefonverbindungsdaten, in: Thüsing, Beschäftigtendatenschutz und Compliance, Rn. 1 ff.

1437 LAG Niedersachsen, Urt. v. 13.01.1998 – 13 Sa 1235/97, NZA-RR 1998, 259 (260).

1438 Offen gelassen von BAG, Beschl. v. 27.05.1986 – 1 ABR 48/84, AP BetrVG 1972 § 87 Überwachung Nr. 15 = NZA 1986, 643 unter B. II. 2. e) der Gründe.

1439 Vgl. zum äquivalenten § 8 BPersVG BAG, Beschl. v. 01.08.1990 – 7 ABR 99/88, AP ZA-Nato-Trupppenstatus Art. 56 Nr. 20 unter B. II. 3. der Gründe.

men von People Analytics. Hierbei wurde das Interesse des Arbeitgebers zur Missbrauchskontrolle mit den Interessen der Arbeitnehmer bzw. Arbeitnehmervertretung abgewogen.[1440] Die Zulässigkeitsprüfung der Überwachung des (kostenlosen) E-Mail-Verkehrs hingegen erfolgte in Literatur und Rechtsprechung v.a. unter dem Aspekt der Fehlerbehebung sowie der rechtswidrigen Inanspruchnahme sowie wirtschaftlichen Schädigung im Sinne von „*fraud prevention*".[1441] Bei beiden Fällen ist ein sehr hohes (wirtschaftliches) Interesse des Arbeitgebers anzuerkennen, welches bspw. im Falle der internen Kommunikation der Betriebsratsmitglieder nicht bestand.

Im Rahmen von Netzwerkanalysen besteht ebenfalls ein wirtschaftliches Interesse des Arbeitgebers, jedoch nicht im Sinne der Kosten- und Missbrauchskontrolle, sondern der Effektivierung seiner Betriebsabläufe. Auf der anderen Seite steht das Persönlichkeitsrecht bzw. das Recht auf Privatheit der Arbeitnehmer.

Umfassende, anlasslose Aufzeichnungen der Verbindungsdaten sind bereits aufgrund § 78 BetrVG problematisch; jedenfalls müsste die Kommunikation der Betriebsratsmitglieder aus den Analysen ausgenommen werden, da hier das Interesse an einer ungestörten Betriebsratsarbeit überwiegt. Je höher der Konzern digitalisiert ist, desto mehr analysierbare Kommunikation findet statt und desto genauer kann das erzeugte Abbild werden. Für die Betriebsratsarbeit kann dies hochproblematisch sein, wenn Arbeitnehmer davor zurückschrecken, mit ihren Problemen den Betriebsrat zu kontaktieren, da sie befürchten müssen, dass der Arbeitgeber diese Kommunikation analysiert und dies negative Folgen für sie haben könnte.

Auch unter dem Aspekt der oben zitierten Rechtsprechung des LAG Niedersachsen müsste sichergestellt sein, dass private Kommunikation bei erlaubter Privatnutzung nicht erfasst wird.[1442]

1440 *Thüsing/Traut*, § 10. Überwachung von Telefonverbindungsdaten, in: Thüsing, Beschäftigtendatenschutz und Compliance, Rn. 2 ff.

1441 Hierzu m.w.N. *Thüsing/Traut*, § 9. Speicherung und Sichtung von E-Mails und E-Mail-Logfiles, in: Thüsing, Beschäftigtendatenschutz und Compliance, Rn. 58 ff. - der Begriff "fraud prevention" stammt aus der Vorauflage, dort Rn. 100 ff.

1442 Siehe hierzu aber bereits oben (**2**).

(4) Folgen

Die Folgen einer Überwachungsmaßnahme sind von entscheidender Bedeutung für die Eingriffsintensität. Hat ein Arbeitnehmer negative Folgen zu befürchten, kann das Gefühl des Überwachtwerdens vielfach Einschüchterungseffekte hervorrufen, welche Arbeitnehmer daran hindern könnten, ihre Grundrechte wahrzunehmen.[1443] So hat auch das BVerfG festgestellt, dass die Intensität des Grundrechtseingriffs in das allgemeine Persönlichkeitsrecht u.a. davon beeinflusst wird, welche nachteiligen sonstigen Folgen aufgrund der Maßnahme drohen oder nicht ohne Grund zu befürchten sind.[1444]

Hierbei stehen, wie sich in der Rechtsprechung des BVerfG zeigt, nicht die datenschutzrechtlichen Folgen im Fokus wie im Rahmen der Zweckänderung (vgl. **E. § 1 I. 2. d) dd)**), sondern es sind jegliche tatsächliche negative Folgen mit gleicher Gewichtung zu berücksichtigen, die Arbeitnehmer daran hindern könnten, ihre grundrechtlichen Freiheitsrechte auszuüben. Selbstverständlich dürfen – da es um immer noch eine datenschutzrechtliche Abwägung geht – die datenschutzrechtlichen Folgen auch nicht außer Acht gelassen werden.

Mögliche Folgen der Netzwerkanalyse könnten sein, dass (bei erlaubter Privatnutzung) private Beziehungen zwischen Mitarbeitern aufgedeckt werden und Kontakte zum Betriebsrat sichtbar werden (und Arbeitnehmer daher davon zurückschrecken, diesen zu kontaktieren) bis hin zu negativen personellen Maßnahmen, wenn beispielsweise ein Nachrichtenaufkommen registriert wird, das deutlich über dem betrieblichen Durchschnitt liegt und daher vermutet wird, dass private Chats während der Arbeitszeit stattfinden. Zwar handelt der konkrete Arbeitnehmer in letzterem Fall vertragswidrig und seine Interessen sind daher nur in geringem Maße schutzwürdig. Die durch die Netzwerkanalyse statuierte Überwachung selbst erfasst aber auch legale Verhaltensweisen (wie beispielsweise Chats in den Pausen bei erlaubter Privatnutzung sowie Kontaktierung des Betriebsrats) und könnte Arbeitnehmer davon abhalten, ihre Rechte wahrzunehmen. Um solche geschützten Interessen nicht zu beeinträchtigen

1443 BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (1191) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54.

1444 Vgl. statt vieler BVerfG, Urt. v. 11.03.2008 – 1 BvR 2074/05, 1 BvR 1254/07, BVerfGE 120, 378 (403) = NJW 2008, 1505 – Automatische Kennzeichenerfassung Rn. 80; Beschl. v. 04.04.2006 – 1 BvR 518/02, BVerfGE 115, 320 (351 ff.) = NJW 2006, 1939 – Rasterfahndung II Rn. 107 ff.

und negative Folgen zu vermeiden oder minimieren, kann der Arbeitgeber beim Einsatz dieser Technologie entsprechende juristische Garantien vorsehen. Diese könnten beispielsweise Verarbeitungsverbot oder die Zusicherung, dass aus der Analyse keine bzw. nur in sehr eng begrenzten Fällen negative Folgen entstehen. Für die Garantien gelten dieselben Maßstäbe wie bei der Zweckvereinbarkeitsprüfung.[1445]

cc) Zwischenergebnis

Netzwerkanalysen sind aufgrund der hohen Eingriffsintensität und dauerhaften, anlasslosen Überwachung datenschutzrechtlich problematisch. Hieraus darf jedoch nicht geschlussfolgert werden, dass solche grundsätzlich unzulässig bzw. nur im Rahmen von § 26 Abs. 1 S. 2 BDSG möglich sind.[1446] Vielmehr bedarf es einer präzisen Regelung aller typischerweise in einem Unternehmen stattfindenden Kommunikationsvorgänge und einer Abwägung der dort widerstreitenden Interessen.

Keinesfalls darf eine Überwachungs-/Drucksituation – wie beispielsweise bei einer dauerhaften Videoüberwachung des Arbeitsplatzes – geschaffen werden. Auch die Privatnutzung betrieblichen Kommunikationsplattformen sollte (insbesondere unter dem Aspekt der unklaren Rechtslage zur Anwendbarkeit des TKG auf Arbeitgeber) verboten werden. Jedenfalls müssen die Arbeitnehmer im Vorfeld darauf hingewiesen werden, dass die Verbindungsdaten der Kommunikation überwacht und Analysen zugeführt werden. Im Hinblick auf die private Nutzung der Plattformen scheint es denkbar, dass eine Einwilligung gem. § 26 Abs. 2 S. 1 BDSG eingeholt wird, da die Arbeitnehmer keiner Drucksituation unterliegen; sie können auch schlicht auf (ggf. unzulässige) private Konversationen über das Firmennetzwerk verzichten, wenn sie eine Aufdeckung von Beziehungen vermeiden möchten. Auch aus diesem Blickwinkel dürfte eine Angemessenheit bei erlaubter Privatnutzung nicht ausgeschlossen sein.

Sofern die betriebliche Kommunikation im Zentrum der Analyse steht, ist die Eingriffsintensität in das Persönlichkeitsrecht der Arbeitnehmer – anders als bei der Videoüberwachung – eng begrenzt, sodass von einem Überwiegen der Arbeitgeberinteressen auszugehen ist.

Zur Absicherung können auch juristische Garantien durch den Arbeitgeber (entweder in Betriebsvereinbarungen oder durch eine Generalzusa-

1445 Siehe hierzu bereits **E. § 1 III. 2. b**) (**2**).
1446 So aber *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 81.

ge) abgegeben werden, die im Rahmen der Folgenabwägung sich ebenfalls zugunsten einer Analyse auswirken.

e) Abschließende Bewertung

Grundsätzlich sind innerbetriebliche Netzwerkanalysen – mit Einschränkungen – zulässig. Es bedarf jedoch einer differenzierten Bewertung im Einzelfall, die – gerade im Hinblick auf die volle richterliche Überprüfbarkeit der Abwägung nach § 26 Abs. 1 S. 1 BDSG – immer mit Rechtsunsicherheiten belastet sind.

Aufgrund der Einschätzungsprärogative der Betriebspartner im Rahmen einer Regelung gem. § 26 Abs. 4 BDSG, Art. 88 Abs. 1 DSGVO[1447] ist zu empfehlen, eine die Datenverarbeitung legitimierende Betriebsvereinbarung abzuschließen. Hierdurch können bei Einhaltung der Datenschutzgrundsätze des Art. 88 Abs. 2, Art. 5 DSGVO (vgl. § 26 Abs. 4 S. 2 BDSG) Rechtsstreitigkeiten und insbesondere Bußgelder vermieden werden.

Eine umfassende Information der Arbeitnehmer vor der Datenerhebung und -verarbeitung ist nicht zuletzt aufgrund von Art. 13 DSGVO in jedem Falle erforderlich. Werden die Maßnahmen heimlich durchgeführt, so führt dies nicht nur zu einer Verletzung der Informationspflicht, sondern auch im Rahmen der Abwägung nach § 26 Abs. 1 S. 1 BDSG zu einer Unzulässigkeit der Datenverarbeitung.

2. Betriebsverfassungsrechtlicher Kontext

Nicht nur aus datenschutzrechtlichen, sondern auch aus betriebsverfassungsrechtlichen Gründen ist der Abschluss einer Betriebsvereinbarung erforderlich. Bei der Netzwerkanalyse bzw. bereits bei der Erhebung der Daten für eine solche, handelt es sich um eine Überwachungsmaßnahme nach § 87 Abs. 1 Nr. 6 BetrVG. Da Netzwerk-Graphen, wie bereits oben aufgeführt, insbesondere auch im Rahmen der (weit zu verstehenden[1448]) Personalplanung gem. § 92 BetrVG eingesetzt werden, muss der Arbeitgeber den Betriebsrat bereits in der Planungsphase („*rechtzeitig*“) darüber informieren. Zur Vermeidung von Wiederholungen wird auf die Ausführungen unter **E. § 1 IV. 2** verwiesen.

1447 Siehe hierzu bereits **E. § 1 III. 1. c) aa)**; allgemein **D. § 1 V. 2.**
1448 Zu § 92 BetrVG siehe bereits **D. § 2 II. 4.**

III. Zusammenfassung

Netzwerk-Graphen stellen ein mächtiges Mittel dar, um die informelle Organisation im Unternehmen darzustellen und zu analysieren. Im Grundsatz gibt es zwei Ansätze: Einerseits die Analyse anhand standardisierter Fragebögen, die darauf abzielen, ganz bestimmte Fragestellungen zu beantworten und einen bestimmten Typus von Netzwerk aufzudecken. Andererseits den Enterprise Social Graph, der die gesamte digitale Kommunikation innerhalb eines Unternehmens in Echtzeit abdecken kann.

Während ersteres aus datenschutzrechtlicher Sicht, bei korrekter Formulierung der Fragen (siehe **E. § 4 I. 1**) unproblematisch ist, bestehen bei letzterem schon erheblich größere Probleme, da eine anlasslose, dauerhafte Überwachung statuiert wird (siehe **E. § 4 II. 1**). Nichtsdestotrotz kann dieser zulässig sein; so überwiegen auch dort in vielen Fällen die Arbeitgeberinteressen. Aufgrund der Vielzahl der erfassbaren Kommunikationssituationen bedarf es einer präzisen und detaillierten Regelung. In jedem Fall müssen Analysen von Betriebsratskommunikationen gänzlich ausgeschlossen werden, da Arbeitnehmer sonst von der Wahrnehmung ihrer Rechte zurückschrecken könnten, wenn sie Repressalien des Arbeitgebers zu befürchten haben. Ebenso müssen eine Regelung für private Kommunikation über betriebliche Netzwerke getroffen und beispielsweise Einwilligungen von Arbeitnehmern eingeholt werden.

Dennoch lassen sich Netzwerkanalysen optimal in bereits vorhandene People Analytics integrieren, wenn Unternehmen ihre Arbeit weitgehend digitalisiert haben. Gerade bei der Nutzung von Kollaborationssuites wie Office 365 bedarf es nur eines geringen technischen Aufwandes zur Implementierung, da solche Funktionen von Haus aus integriert sind. Über APIs können die Daten aus der Software so in das Personalmanagementsystem integriert und ein noch größerer Nutzen erzeugt werden.

In jedem Fall muss ein vorhandener Betriebsrat aufgrund der betriebsverfassungsrechtlichen Mitspracherechte im Vorfeld informiert und bei der Planung und Einführung eingebunden werden. In diesem Zusammenhang empfiehlt es sich – zur Vermeidung von Rechtsunsicherheiten – eine gleichzeitig die Datenverarbeitung legitimierende Betriebsvereinbarung abzuschließen.

F. Entwicklung einer Muster-Betriebsvereinbarung

An vielen Stellen dieser Arbeit wurde darauf hingewiesen, dass der Abschluss einer Betriebsvereinbarung nicht nur aus betriebsverfassungsrechtlicher Sicht notwendig, sondern auch aus datenschutzrechtlichem Blickwinkel geboten ist, um Rechtsunsicherheiten bei der Auslegung des offenen Begriffs der „Erforderlichkeit" zu vermeiden.

Nach Art. 88 Abs. 1 DSGVO sowie § 26 Abs. 4 S. 1 BDSG kann eine Betriebsvereinbarung die Datenverarbeitung legitimieren, sofern die in Art. 5 DSGVO genannten Datenschutzgrundsätze eingehalten werden.[1449]

Unter **D. § 1 IV** sowie **D. § 1 V. 2** wurde ausführlich dargelegt, warum die Betriebspartner mit Hilfe einer Betriebsvereinbarung kein eigenständiges Datenschutzregime erzeugen können, sondern sich im Grundsatz an das vorgegebene Datenschutzniveau der DSGVO und des BDSG halten müssen, jedoch für Einzelfälle Spezialregelungen schaffen dürfen, die bei gerichtlichen Streigikeiten nicht vollumfassend am Begriff der Erforderlichkeit gemessen werden (Einschätzungsprärogative der Betriebspartner). Die Verhandlungspartner bei der Abwägung der Grundrechte nach § 75 Abs. 2 BetrVG einen Beurteilungsspielraum, der Rechtssicherheit schafft.[1450]

Nachfolgend soll ein möglicher Aufbau einer Betriebsvereinbarung dargestellt werden, die die Einführung von People Analytics sowie damit zusammenhängende datenschutzrechtliche Legitimationsfragen regelt. Es soll aufgezeigt werden, wo die Verhandlungspartner einen Regelungsspielraum besitzen und wie dieser ausgestaltet werden kann. Die Orientierung erfolgt an den in dieser Arbeit genannten Beispielen. Eine konsolidierte Fassung der hier erarbeiteten Betriebsvereinbarung findet sich im **Anhang II**.

1449 Unter altem Recht (§ 4 Abs. 1 BDSG a.F.) war dies aufgrund der Formulierung „andere Rechtsvorschriften" zunächst umstritten, aber letztlich h.M., vgl. *Körner*, NZA 2019, 1389 (1390); *Klösel/Mahnhold*, NZA 2017, 1428, jeweils m.w.N.

1450 Bejahend einen Beurteilungsspielraum im Hinblick auf die Erforderlichkeit der Datenverarbeitung (im Rahmen von § 75 Abs. 2 BetrVG) bei der Abwägung nationaler Grundrechte, BAG, Beschl. v. 29.06.2004 – 1 ABR 21/03, NZA 2004, 1278 (1280) = BAGE 111, 173 = AP BetrVG § 87 1972 Überwachung Nr. 41 (m. Anm. Ehmann); siehe bereits **E. § 1 III. 1. c) aa)**.

§ 1 Allgemeines

§ 26 Abs. 6 BDSG regelt, dass die Beteiligungsrechte der Interessensvertretungen der Beschäftigten unberührt bleiben, d.h. auf Basis der bislang aufgezeigten Mitbestimmungsrechte (insbesondere § 87 Abs. 1 Nr. 1 und 6 sowie §§ 94 f. BetrVG) kann der Betriebsrat Betriebsvereinbarungen zum Beschäftigtendatenschutz initiieren. § 88 BetrVG ermöglicht dem Betriebsrat auch den Abschluss (freiwilliger) Betriebsvereinbarungen in mitbestimmungsfreien Regelungsbereichen.[1451] Im Übrigen verhält sich das Datenschutzrecht nicht zu Mitbestimmungsrechten.

Aufgrund der Informations- und Transparenzanforderungen, aber auch der weitergehenden Beteiligungsrechte müssen insbesondere in bereits vorhandenen Betriebsvereinbarungen weitgehendere und detaillierte Regelungen getroffen werden als früher.[1452] Dies ergibt sich bereits Art. 88 Abs. 2 DSGVO selbst, wonach geeignete und besondere Maßnahmen im Hinblick auf die Transparenz der Verarbeitung in einer solchen Vereinbarung enthalten sind.[1453]

Unterschieden wird grundsätzlich hinsichtlich des Regelungsgehalts zwischen Rahmen- und Einzelbetriebsvereinbarungen.[1454]

§ 2 Anforderungen an eine datenschutzrechtliche Betriebsvereinbarung

I. Transparenzerfordernis des Art. 88 Abs. 2 DSGVO

Aufgrund von Art. 88 Abs. 2 DSGVO sollten Betriebsvereinbarungen in jedem Falle Regelungen zur Transparenz der Datenverarbeitung enthalten. Diese erfüllen entweder die Anforderungen der Art. 12 ff. DSGVO oder spezifizieren die Anforderungen weiter. Bisweilen wird empfohlen (spezifische) Regelungen zur Unterrichtung und Information der betroffenen Arbeitnehmer zu treffen.[1455]

Es ist umstritten, ob sich die Vorgabe zur Transparenz der Datenverarbeitung auf die inhaltliche Ausgestaltung und oder auch die formalen Regelungen selbst bezieht, letztere also in klarer und verständlicher Sprache

1451 Hierzu allgemein *Körner*, NZA 2019, 1389 (1391).
1452 *Körner*, NZA 2019, 1389 (1391 f.).
1453 Wie hier wohl *Dzida/Grau*, DB 2018, 189 (191).
1454 *Klösel/Mahnhold*, NZA 2017, 1428.
1455 Hierzu *Wybitul*, ZD 2016, 203 (207).

gefasst sein müssen. Teilweise wird vertreten, dass das Transparenzgebot auch für die Regelungen selbst gilt.[1456] Als Grundlage werden der Transparenzgrundsatz aus Art. 5 Abs. 1 lit. a DSGVO sowie Erwägungsgrund 58 herangezogen. In letzterem heißt es: „*Der Grundsatz der Transparenz setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist […]*". Die Gegenauffassung[1457] stützt sich auf den Wortlaut des Art. 88 Abs. 2 DSGVO („*Transparenz der Verarbeitung*"), erkennt aber teilweise[1458] gleichwohl eine Sinnhaftigkeit einer klaren und verständlichen Regelung unter Rückgriff auf Erwägungsgrund 41 S. 2 („[…] *sollten jedoch klar und präzise sein*") an. Eine Adressierung an juristische Laien sei aber aufgrund der notwendig hoch technischen und präzisen Regelung nicht möglich. Eine Lösung, die wiederum von anderen Autoren hierzu vorgeschlagen wird, ist die Betriebsvereinbarung mit einem Dokument zu „häufig gestellten Fragen (FAQ)" zu ergänzen, um Regelungstransparenz herzustellen.[1459]

Als „Minimallösung" wird teilweise eine Wiedergabe oder Bezugnahme auf die Transparenzvorschriften der Art. 12 - 15 DSGVO akzeptiert[1460], aber detailliertere Regelungen bzw. alternative Informationsmechanismen (z.B. Information des Betriebsrats statt des Einzelnen) als zweckmäßig erachtet.[1461] Eine weitere Ansicht verzichtet hingegen vollständig auf die Bezugnahme auf Pflichten nach Art. 12 ff. DSGVO, da der „Verantwortliche" ohnehin zuständig ist und daher eine (weitere) Regelung mit dem Betriebsrat bei Erfüllung dieser Pflichten nicht erforderlich sei.[1462] Über-

1456 Paal/Pauly/*Pauly*, Art. 88 DSGVO Rn. 14; Sydow/*Tiedemann*, Art. 88 DSGVO Rn. 20; *Grimm*, ArbRB 2018, 78 (80): "Kein IT-Deutsch"; *Korinth*, ArbRB 2018, 47 (49).

1457 BeckOK DatenSR/*Riesenhuber*, Art. 88 DSGVO Rn. 85; *Klösel/Mahnhold*, NZA 2017, 1428 (1431); *Wybitul*, ZD 2016, 203 (207 f.); wohl auch *Maschmann*, DB 2016, 2480 (2484).

1458 BeckOK DatenSR/*Riesenhuber*, Art. 88 DSGVO Rn. 85.1.

1459 *Dzida/Grau*, DB 2018, 189 (192); *Tiedemann*, ArbRB 2016, 334 Fn. 15; *Wybitul/Sörup/Pötters*, ZD 2015, 559 (561).

1460 *Tiedemann*, ArbRB 2016, 334 (336); *Kort*, DB 2016, 711 (714).

1461 *Wybitul*, ZD 2016, 203 (208); *Klösel/Mahnhold*, NZA 2017, 1428 (1431): Bloße Wiedergabe ausreichend, Betriebsvereinbarung hat allerdings auch Vorschriften zu enthalten, die die Transparenzanforderungen erfüllen.

1462 *Dzida/Grau*, DB 2018, 189 (193).

wiegend wird allerdings vertreten, dass eine bloße Wiedergabe des Gesetzestexts nicht ausreichend sei,[1463] um den Anforderungen zu entsprechen.

Gibt es mehrere Betriebsvereinbarungen im Unternehmen, so ist im Hinblick auf den Transparenzgrundsatz eine Erläuterung des Regelungszusammenhangs zwischen den einzelnen Betriebsvereinbarungen (z.B. einer Rahmenbetriebsvereinbarung und einer spezifischen Einzelbetriebsvereinbarung); eine solche Erläuterung an einer für alle Arbeitnehmer leicht zugänglichen Stelle (z.B. das Intranet) ist ausreichend.[1464]

Letztlich lässt sich die Lösung im den Datenschutzprinzipien selbst finden: Art. 5 Abs. 1 lit. a DSGVO bestimmt, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise, ebenfalls aber nach lit. b auch für festgelegte, eindeutige Zwecke verarbeitet werden müssen. Muss die Kollektivvereinbarung selbst sprachlich einfach gehalten werden, so sind präzise Regelungen („*Juristendeutsch*“) kaum möglich. Aus diesem Grund würde das Transparenzerfordernis somit anderen Regelungen zuwiderlaufen. Vielmehr muss es ausreichend sein, dass Betroffene anhand von FAQs oder sonstigen Erläuterungen klar nachvollziehen, für welche Zwecke ihre Daten genau verarbeitet werden. Hierdurch lässt sich auch die Form der Information nach Art. 12 ff. bzw. Art. 88 Abs. 2 DSGVO bestimmen: Die notwendigen Informationen müssen dabei nicht selbst im Normtext aufgenommen werden, sondern können an einer für alle Beschäftigten gut einsehbaren Stelle (z.B. das Intranet) veröffentlicht werden. Selbstverständlich muss bei mehreren Regelungen auch das Verhältnis zueinander klar dargestellt werden, um Normenklarheit zu schaffen.[1465] Eine Aufnahme aller Informationen in den Normtext würde diesen hingegen überfrachten und der Transparenz entgegenwirken. Möglich bleibt es aber selbstverständlich, technische Ausführungen noch durch eine – wenn auch unpräzisere – Erläuterung für den juristischen Laien beispielsweise als (nicht-normative) „Informationsbox“ in den Normtext aufzunehmen. Die in Art. 88 Abs. 2 DSGVO geforderten Transparenz-Maßnahmen kön-

1463 *Düwell/Brink*, NZA 2017, 1081 (1082); *Haußmann/Brauneisen*, BB 2017, 3065 (3066); Sydow/*Tiedemann*, Art. 88 DSGVO Rn. 20; *Grimm*, ArbRB 2018, 78 (80); *Wurzberger*, ZD 2017, 258 (262).

1464 *Korinth*, ArbRB 2018, 47 (49); *Tiedemann*, ArbRB 2016, 334 (336).

1465 Ein aktuelles Beispiel von einer unklaren Rechtslage zeigten die Corona-Verordnungen der Länder in Zusammenhang mit den Allgemeinverfügungen der Landkreise. Viele juristische Laien, aber auch Experten wussten nicht mehr, wie die aktuelle Rechtslage ist. Aus diesem Grund muss die Transparenz bei vielen Betriebsvereinbarungen unbedingt durch eine klare Auflistung sowie Darstellung der Hierarchie klar gemacht werden.

nen daher spezifische Regelungen zur Veröffentlichung der in Art. 12 ff. DSGVO geforderten Informationen sein.[1466] Eine reine Wiedergabe des Normtextes (z.B. in verändertem Wortlaut) wäre nicht zweckmäßig; ein Verweis hingegen unschädlich.

Für diese Sichtweise spricht auch die Umsetzung des Art. 88 Abs. 2 DSGVO im nationalen Beschäftigtendatenschutzrecht. So finden sich auch dort keine bloßen Wiederholungen der Art. 12 ff., weil dies (außer für „bestimmte Punkte", sofern dies aufgrund ihres inneren Zusammenhangs und für ihre Verständlichkeit für die Adressaten notwendig ist) sogar europarechtswidrig wäre.[1467]

II. Bezeichnung als datenschutzrechtliche Rechtfertigungsgrundlage

In jedem Falle ist es aber unter Berücksichtigung der Transparenzvorgaben erforderlich, dass in der Betriebsvereinbarung ausdrücklich klargestellt wird, dass eine Regelung nicht nur die Ausübung der betriebsverfassungsrechtlichen Mitbestimmungsrechte des Betriebsrats, sondern auch die datenschutzrechtliche Ermächtigungsgrundlage auf Basis von Art. 88 DSGVO bzw. § 26 Abs. 4 DSGVO darstellt.[1468] Nur so können Beschäftigte erkennen, dass die Rechtsgrundlage für die Verarbeitung nicht das „allgemeine" Datenschutzrecht ist, sondern der Arbeitgeber bei der Verarbeitung ihrer personenbezogenen Daten von einer Spezialermächtigung in Form einer Betriebsvereinbarung Gebrauch macht.

III. Regelung zur Konzerndatenübermittlung (Art. 88 Abs. 2 DSGVO)

Sofern Daten innerhalb eines Konzerns übermittelt werden, ist nach Art. 88 Abs. 2 DSGVO erforderlich, dass die Betriebspartner hierfür eine Regelung in der Betriebsvereinbarung treffen, um die Wahrung der menschlichen Würde, der berechtigten Interessen sowie der Grundrechte der betroffenen Arbeitnehmer sicherzustellen. Zwar ist die Vorschrift im Wortlaut deutlich weiter gefasst und könnte so zu verstehen sein,

---

1466 So auch *Haußmann/Brauneisen*, BB 2017, 3065 (3066).

1467 EuGH, Urt. v. 28.03.1985 – C-272/83, BeckRS 2004, 72839, 28 – Kommission/Italien; *Maschmann*, NZA-Beilage 2018, 115 (119).

1468 So auch *Grimm*, ArbRB 2018, 78 (79); *Klösel/Mahnhold*, NZA 2017, 1428 (1432).

dass zwingend Regelungen zur Konzerndatenübermittlung enthalten sein müssen; dies würde allerdings den Zweck der „Spezifizierungsklausel" verfehlen. Nur dort, wo auch tatsächlich eine Konzerndatenübermittlung stattfindet, müssen nach Art. 88 Abs. 2 DSGVO auch Regelungen dazu getroffen werden; insofern muss die Vorschrift teleologisch reduziert werden.[1469]

Obwohl das Thema „Konzerndatenübermittlung" in der Praxis, insbesondere bei People Analytics eine große Rolle spielt, da HR-Daten oftmals nicht nur beim Unternehmen selbst, sondern im Konzern in einer HR-Gesellschaft oder bei der Konzernmutter verarbeitet werden, ist dies nicht Gegenstand dieser Arbeit, die die Datenverarbeitung für Analysezwecke selbst in ihrer Zulässigkeit untersucht. Eine ausführliche Betrachtung der Einzelheiten zur Datenübermittlung in EU-Staaten sowie Drittstatten (mit und ohne Abkommen) würde den Rahmen sprengen und bleibt daher außen vor. In der nachfolgend aufgestellten Muster-Betriebsvereinbarung wird daher ausschließlich die Verarbeitung innerhalb eines Unternehmens betrachtet und geregelt.

IV. Schutzmaßnahmen bei Überwachungssystemen am Arbeitsplatz

Als dritten Aspekt, der von einer datenschutzrechtlichen Beschäftigtendatenschutzspezialregelung aufgegriffen werden muss, nennt Art. 88 Abs. 2 DSGVO die Überwachungssysteme am Arbeitsplatz. In diesem Bereich hat der Betriebsrat auch ein zwingendes Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG.[1470] Soweit in einer Betriebsvereinbarung also Regelungen zu Überwachungssystemen am Arbeitsplatz getroffen, bedarf es zwingend auch Schutzmaßnahmen nach Art. 88 Abs. 2 DSGVO aufgrund der hohen Gefahren für das Persönlichkeitsrecht der Betroffenen. Erfasst werden aufgrund des Wortlauts („Überwachungs*systeme*") nur automatisierte Kontrollverfahren.[1471] Diese bergen – im Vergleich zu nicht-automatisierten Verfahren wie beispielsweise dem Einsatz eines Detektivs – im Einzelfall ein weitaus höheres Gefahrenpotential für die Daten und Rechte der betroffenen Arbeitnehmer.

1469 BeckOK DatenSR/*Riesenhuber*, Art. 88 DSGVO Rn. 88; *Klösel/Mahnhold*, NZA 2017, 1428 (1432).

1470 Siehe bereits ausführlich **D. § 2 II. 1. b**).

1471 Paal/Pauly/*Pauly*, Art. 88 DSGVO Rn. 17; BeckOK DatenSR/*Riesenhuber*, Art. 88 DSGVO Rn. 91; *Wybitul*, ZD 2016, 203 (208).

Bei den untersuchten Advanced People Analytics-Methoden handelt es sich allesamt um Überwachungssysteme im Sinne dieser Vorschrift, da jedes elektronische Gerät, das dazu bestimmt ist, personenbezogene Daten über den Arbeitnehmer zu erheben, davon erfasst ist.[1472] Entsprechende Schutzmaßnahmen für die Rechte der Arbeitnehmer sind daher zwingend in einer legitimierenden Betriebsvereinbarung aufzunehmen.

§ 3 Rahmen- und Einzelbetriebsvereinbarung

Grundsätzlich ist es möglich, neben Einzelbetriebsvereinbarungen zu spezifischen Regelungsbereichen (z.B. Betriebsvereinbarung zum Home-Office, Betriebsvereinbarung zur Nutzung von SAP im Rahmen der Buchhaltung etc.) auch Rahmenbetriebsvereinbarungen zu schließen. Diese legen Bestimmungen für eine Vielzahl von Sachverhalten fest, ohne jedoch die Sachverhalte spezifisch zu regeln.[1473] Mangels abschließender Regelung sind Rahmenbetriebsvereinbarungen zwar nicht erzwingbar[1474], dennoch gerade im Informations- und Kommunikationsbereich von hoher Bedeutung, um beispielsweise Mindeststandards für (jegliche) Datenverarbeitungen im Betrieb, Unternehmen oder Konzern festzulegen.[1475]

Hierdurch lassen sich auch Einzelbetriebsvereinbarungen entzerren, indem beispielsweise Regelungen für Auskunfts- und Informationspflichten nach Art. 12 ff. DSGVO nicht in jeder Einzelbetriebsvereinbarung erneut aufgenommen werden müssen, sondern können mit Hilfe einer Rahmenvereinbarung „vor die Klammer" gezogen werden. Dies trägt u.a. auch zu der teilweise geforderten Transparenz der Regelungen[1476] bei.

Vielfach wird aus diesem Grund der Abschluss von Rahmenbetriebsvereinbarungen empfohlen.[1477]

Überdies können mit dem Instrument der Rahmenbetriebsvereinbarung – bei Bestehen eines Gesamt- oder Konzernbetriebsrats – auch Regelungen

---

1472 BeckOK DatenSR/*Riesenhuber*, Art. 88 DSGVO Rn. 17; insofern besteht eine Parallele zum Wortlaut des § 87 Abs. 1 Nr. 6 BetrVG.

1473 *Oberthür*, A. II. Arten von Betriebsvereinbarungen, in: Oberthür/Seitz, Betriebsvereinbarungen, Rn. 5.

1474 *Oberthür*, A. II. Arten von Betriebsvereinbarungen, in: Oberthür/Seitz, Betriebsvereinbarungen, Rn. 8.

1475 *Schulze/Pfeffer*, ArbRAktuell 2017, 358.

1476 Hierzu **F. § 2 I**.

1477 So etwa in jüngeren Zeitschriftenbeiträgen *Wybitul*, NZA 2017, 1488; *Körner*, NZA 2019, 1389 (1393); *Schulze/Pfeffer*, ArbRAktuell 2017, 358.

auf Unternehmens- bzw. Konzernebene getroffen werden, die für alle Betriebe gelten und konkrete Regelungen den örtlichen Betriebsräten überlassen werden, sofern die gesetzliche Zuständigkeitsverteilung gewahrt bleibt; eine Delegation von Kompetenzen ist dabei nicht möglich.[1478]

Im Bereich von People Analytics werden hingegen kaum Regelungen „nur" auf Betriebsebene getroffen werden, da die HR-Abteilung in aller Regel auf Unternehmens-, wenn nicht sogar auf Konzernebene angesiedelt ist und gerade Analysen zentral durchgeführt werden, sofern es das Datenschutzrecht (im Hinblick auf das fehlende Konzernprivileg) zulässt. Dennoch werden auch hier Rahmen- und Einzelbetriebsvereinbarungen eingesetzt, um allgemeine datenschutzrechtliche Standards für alle Datenverarbeitungen festzulegen und wiederum Einzelbereiche in spezifischen Betriebsvereinbarungen zu regeln.

Im Nachfolgenden werden zur Veranschaulichung auch Regelungen, die üblicherweise in einer Rahmenbetriebsvereinbarung geregelt würden, in der Einzelbetriebsvereinbarung aufgenommen, um eine vollständige Abdeckung der notwendigen Regelungen für eine „*People Analytics-BV*" zu erzielen.

Bevor jedoch auf die einzelnen Aspekte der Regelung eingegangen wird, wird zuvor noch aufgezeigt, welche Bereiche typischerweise in der Rahmenbetriebsvereinbarung und welche in der Einzelbetriebsvereinbarung „People Analytics" geregelt würden.

I. Rahmenbetriebsvereinbarung „IKT"

Wie bereits dargestellt, kommen in die Rahmenbetriebsvereinbarung vor allem Regelungen, die auf alle Datenverarbeitungen anwendbar sind und nicht anwendungsspezifisch für eine bestimmte Applikation oder Datenverarbeitungssituation sind. Hierzu zählen insbesondere Regelungen zu Auskunfts- und Informationsansprüchen (etwaige Konkretisierungen der Pflichten aus Art. 12 ff. DSGVO), allgemeine Bestimmungen zur Zweckbestimmung und -bindung, Vorgaben zur Systemdokumentation, ein etwaiger Ausschluss von Leistungs- und Verhaltenskontrollen, Vorgaben zur Auftragsverarbeitung (z.B. Unterrichtung des Betriebsrats, Gestaltungsvorgaben für Auftragsverarbeitungsverträge), Vorgaben zu sonstigen Über-

1478 *Oberthür*, A. II. Arten von Betriebsvereinbarungen, in: Oberthür/Seitz, Betriebsvereinbarungen, Rn. 7; zur Unzulässigkeit der Delegierung von Kompetenzen, BAG, Beschl. v. 21.01.2003 – 3 ABR 26/02, NJOZ 2003, 2274 f. Os. 2.

mittlungen an Dritte, ein Berechtigungskonzept, Bestandsverzeichnis (als Anlage) sowie das Verfahren bei Streitigkeiten.[1479]

Auch Vorgaben zur (wirksamen) Einwilligung von Arbeitnehmern im Beschäftigungskontext können Eingang in eine solche Rahmenbetriebsvereinbarung finden.[1480]

II. Einzelbetriebsvereinbarung „People Analytics“

In der Einzelbetriebsvereinbarung „*People Analytics*“ hingegen werden alle Spezifika für die geplanten Analytics geregelt. Wie sich bereits aus der bisherigen Untersuchung ergibt, gibt es an vielen Stellen „Einfallstore“ für betriebliche Sonderregelungen bzw. machen Spezialregelungen an vielen Stellen Sinn, um den unbestimmten Begriff der „Erforderlichkeit“ (für die Entscheidung über die Begründung bzw. Durchführung des Beschäftigungsverhältnisses) weiter zu konkretisieren bzw. eine Subsumtion unter den gesetzlichen Begriff zu vermeiden und hierdurch Rechtsunsicherheiten gar nicht erst entstehen zu lassen. Ebenfalls sinnvoll ist es auch in diesem Rahmen die Möglichkeit, spezieller Einwilligungen von Arbeitnehmern (z.B. für „persönliche Dashboards“) unter Beachtung des grundsätzlichen Prinzips der Freiwilligkeit der Einwilligung näher zu regeln.

Unter Rückgriff auf die untersuchten People Analytics-Anwendungsszenarien sollten folgende Punkte in einer Einzelbetriebsvereinbarung geregelt werden: Nutzung von IT-Logdaten für Analytics-Zwecke, zulässige Zweckänderungen, Profiling und Scoring, automatisierte (Einzelfall-)Entscheidungen, Einsatz von Dashboards und Netzwerk-Graphen/-Analysen.

Weiterhin – jedoch hier außer Betracht bleibend –müssen zwingend die Übermittlung von Daten innerhalb eines Konzerns geregelt und in diesem Rahmen Grenzen sowie Schutzmaßnahmen klar festgelegt werden, falls eine solche stattfinden soll.

§ 4 Einzelregelungen einer „People Analytics-BV“

Im Nachfolgenden sollen die (notwendigen) Regelungen einer Betriebsvereinbarung mit Schwerpunkt People Analytics untersucht und dabei die Regelungsspielräume der Betriebsparteien aufgezeigt werden. Der Fokus

1479 Siehe hierzu *Schulze/Pfeffer*, ArbRAktuell 2017, 358.
1480 Vgl. *Grimm*, ArbRB 2018, 122 (123).

wird auf die unter **F. § 3** aufgezählten Regelungsbereiche – auch im Rahmen von Rahmenbetriebsvereinbarungen – gelegt, sodass im Endeffekt eine schlüssige Gesamtregelung zu People Analytics in einem Unternehmen entsteht.

Es wird davon ausgegangen, dass keine Übermittlung innerhalb eines Konzerns stattfindet und die Daten ausschließlich im Unternehmen verarbeitet werden, also auch keine Auftragsverarbeitung (z.B. durch die Nutzung von Cloud-Anbietern) stattfindet. Insbesondere ersterer Aspekt bedürfte aufgrund von Art. 88 Abs. 2 DSGVO einer Regelung in einer Betriebsvereinbarung. Bei der Auftragsverarbeitung hingegen muss zunächst mit dem jeweiligen Drittanbieter verhandelt werden, inwiefern eine Anpassung auf die betrieblichen Gegebenheiten möglich ist; aus diesem Grund kann an dieser Stelle keine pauschale Aussage getroffen werden, sodass dieser Bereich ebenfalls außer Betracht bleibt.[1481]

I. Präambel

In einem ersten Schritt ist – nicht zuletzt aufgrund des Transparenzerfordernisses – jeder Betriebsvereinbarung eine Präambel voranzustellen, die festlegt, dass die geschlossene Betriebsvereinbarung gleichzeitig auch eine Legitimationsgrundlage für die Datenverarbeitung darstellt.[1482] Für eine *People Analytics*-Betriebsvereinbarung (im Folgenden: PA-BV) könnte diese wie folgt lauten:

> *Bereits aus der Bezeichnung „Human Ressources" geht hervor, dass das Humankapital eines Unternehmens – im Gegensatz zu den Anfängen der Personalarbeit – ein wesentlicher Faktor für den Erfolg eines Unternehmens ist. Entscheidend prägen also die fachlichen und sozialen Fähigkeiten der Mitarbeiter den wirtschaftlichen Erfolg unseres Unternehmens XY. Gerade in der aktuellen Zeit, in welcher Arbeit in hohem Maße digitalisiert wird und der persönliche Kontakt auch unter den Kollegen abnimmt sowie die Unternehmensstrukturen immer komplexer werden, ist es von entscheidender Bedeutung für die Zufriedenheit der Arbeitnehmerschaft, dass innerbetriebliche Prozesse möglichst effizient ablaufen und Probleme frühzeitig erkannt*

1481 Zu den Vorgaben der Auftragsdatenverarbeitung (noch unter altem Recht) bei der Nutzung von Persönlichkeitsanalysetools, vgl. *Eckhardt/Kramer*, DuD 2016, 144.

1482 Hierzu bereits **F. § 2 II**.

*und behoben werden. Hierfür setzt XY die Methode **People Analytics** ein, die den Entscheidungsträgern ermöglichen soll, etwaige Ungereimtheiten im Betriebsablauf bereits frühzeitig zu erkennen und gegensteuern zu können. Eine niedrige Reaktionszeit ist erforderlich, um mit den Maßnahmen nicht immer einen Schritt hinterherzuhinken, sondern eine Steuerung in Echtzeit zum Vorteil der Arbeitnehmerschaft zu ermöglichen.*

*XY setzt im Rahmen von People Analytics auf die **Auswertung von IT-Nutzungsdaten** und nutzt die Techniken des **Profilings und Scorings**, um den Arbeitnehmern und Entscheidungsträgern im Unternehmen in verständlicher Form alle für sie wesentlichen Informationen in **Dashboards** darzustellen und rasche Entscheidungen zu ermöglichen. Um Kommunikationsabläufe zu verbessern, wird die **Netzwerk-Analyse** eingesetzt.*

Alltägliche Prozesse sollen durch automatisierte Entscheidungen beschleunigt und vereinfacht, somit das Human Resources Management entlastet und schnelle Entscheidungen ermöglicht werden.

*Damit diese Form des modernen und evidenzbasierten Personalmanagements ermöglicht werden kann, wird folgende Vereinbarung geschlossen, die gleichzeitig auch als **datenschutzrechtliche Legitimationsgrundlage** für die hierfür erforderlichen Verarbeitungsvorgänge nach Art. 88 Abs. 1 DSGVO, § 26 Abs. 4 BDSG gilt. Um die gesetzlichen Vorgaben der DSGVO und des BDSG einzuhalten, regelt diese Vereinbarung die betriebsverfassungsrechtlichen und datenschutzrechtlichen Rahmenbedingungen für den Einsatz von People Analytics **abschließend**.*

Eine Präambel muss nicht die dargestellte Ausführlichkeit und Präzision besitzen, dennoch empfiehlt es sich – in „einfachem Deutsch“ – in der Präambel voranzustellen, welche Bereiche die Betriebsvereinbarung regelt, sodass ein interessierter Mitarbeiter einen schnellen Überblick über den Regelungsgegenstand bekommt, ohne sich durch den vollständigen, mitunter technisch und sprachlich sehr komplexen Regelungsbereich durcharbeiten zu müssen. Insbesondere wenn die Betriebsvereinbarung auch als datenschutzrechtliche Legitimationsgrundlage gilt, ist die PA-BV die Haupterkenntnisquelle dafür, ob eine Datenverarbeitung rechtmäßig ist oder nicht.

In der Information nach Art. 13 DSGVO ist diese daher auch als Legitimationsgrundlage aufzuführen.

II. Gegenstand und allgemeine Grundsätze der Datenverarbeitung

Im normativen Bereich der Betriebsvereinbarung sind in weiterer Folge der Anwendungsbereich und Gegenstand der Regelung klar abzugrenzen und notwendige Begriffe zu bestimmen. Hierbei sollte aufgrund von Art. 88 Abs. 2 DSGVO statuiert werden, dass die Regelung eine angemessene und besondere Maßnahme zur Wahrung der berechtigten Interessen, der menschlichen Würde und Grundrechte sowie des Schutzes der Persönlichkeit der beschäftigten Arbeitnehmer darstellt:

> ***§ 1 Anwendungsbereich, Gegenstand und allgemeine Grundsätze der Datenverarbeitung***
>
> *(1) Diese Betriebsvereinbarung gilt für alle Arbeitnehmer im Sinne des § 5 Abs. 1 BetrVG, mit Ausnahme der leitenden Angestellten, und für jegliche Datenverarbeitungen, die im Zusammenhang mit der Analyse von personenbezogenen Daten von Arbeitnehmern zum Zwecke des Personalmanagements (People Analytics) stattfinden. Die Begriffsdefinitionen, soweit nicht ausdrücklich anders definiert, entsprechen denjenigen aus Art. 4 DSGVO.*

Nota bene: Der Sprecherausschuss kann gem. § 28 Abs. 1 SprAuG mit dem Arbeitgeber Richtlinien über den Inhalt, Abschluss oder die Beendigung von Arbeitsverhältnissen der leitenden Angestellten schriftlich vereinbaren; dieser Inhalt gilt gem. Abs. 2 unmittelbar und zwingend. In diesem Zusammenhang könnte beispielsweise zwischen Arbeitgeber und Sprecherausschuss vereinbart werden, dass die Regelungen der Betriebsvereinbarung auch für leitende Angestellte gelten. Besteht kein Sprecherausschuss, muss eine individuelle Bezugnahme auf die PA-BV im Arbeitsvertrag oder einer Zusatzvereinbarung erfolgen.

> *(2) Gegenstand dieser Vereinbarung ist die Regelung angemessener und besonderer Maßnahmen zur Wahrung der berechtigten Interessen, der menschlichen Würde und der Grundrechte sowie des Schutzes der Persönlichkeit der Arbeitnehmer gem. Art. 88 Abs. 2 DSGVO beim Einsatz von People Analytics.*

Werden in der Vereinbarung bestimmte Begrifflichkeiten verwendet, die gesetzlich nicht definiert sind, empfiehlt es sich zur Vermeidung von Streitigkeiten auch diese in einer Norm zu Beginn zu definieren und bei mehrfacher Verwendung auf Definitionen in einzelnen Klauseln zu verzichten.

Dies erhöht die Lesbarkeit der Vereinbarung und schafft weitere Transparenz:

> ***§ 2 Begriffsbestimmungen***
>
> 1. *„Scoring“ ist die Verwendung eines Wahrscheinlichkeitswertes, welcher über ein wissenschaftlich-anerkanntes, mathematisches Verfahren berechnet wird, über ein bestimmtes zukünftiges Verhalten einer natürlichen Person im Hinblick auf die Untersuchungsfrage.*
>
> 2. *„Score“ ist das Ergebnis eines Scoring-Vorgangs und stellt einen bestimmten Wahrscheinlichkeitswert über ein bestimmtes zukünftiges Verhalten einer natürlichen Person im Hinblick auf die Untersuchungsfrage dar. Dieser kann entweder in Prozent oder in Form einer Punktezahl im Rahmen eines vorgegebenen Schemas in Erscheinung treten.*
>
> 3. *„Ranking“ ist ein Verfahren, bei welchem in einer abschließenden Liste die Inhalte der Liste nach einem vorgegebenen, wissenschaftlich-anerkannten, mathematischen Verfahren mit Blick auf die Passgenauigkeit zur Untersuchungsfrage gereiht werden. Das zugrundeliegende Verfahren stellt in der Regel ein „Scoring“ bzw. eine Kombination verschiedener Score-Werte dar.*
>
> 4. *„Dashboard“ ist eine Visualisierungsform für Daten. Dashboards werden im Rahmen dieser Betriebsvereinbarung dazu eingesetzt, um die aus People Analytics gewonnenen Daten für die jeweilige Zielperson der Analyse übersichtlich darzustellen.*
>
> 5. *„Netzwerk-Graph“ ist ein grafisches Tool zur Darstellung der informellen Hierarchie im Unternehmen. Er basiert auf der Auswertung von Kommunikationsdaten der Arbeitnehmer im Unternehmen.*

III. Datenschutzrechtliche Grundsätze für die Datenverarbeitung und Überwachungsmaßnahmen

Neben der Bezugnahme auf die allgemeinen datenschutzrechtlichen Grundsätze (in § 1 PA-BV) sollten auch noch spezifische Grundsätze für die Datenverarbeitung im Rahmen von People Analytics getroffen werden. Hierzu gehören besondere Regelungen zur Zweckbindung und -vereinbar-

keit sowie zu Überwachungsmaßnahmen[1483]. Insbesondere letztere sind – wie unter **E. § 1 III. 2. a**) und **E. § 4 II. 1** dargestellt – grundsätzlich ebenfalls Überwachungsmaßnahmen, sodass der nicht-repressive Einsatz aufgrund von Art. 88 Abs. 2 BDSG einer besonderen Regelung bedarf.

> ***§ 3 Datenschutzrechtliche Grundsätze für die Anwendung von People Analytics***
>
> *(1) Die in Art. 5 Abs. 1 lit. a bis f DSGVO festgelegten Datenschutzgrundsätze sind Inhalt dieser Vereinbarung und gelten für jegliche Verarbeitungen personenbezogener Daten der Arbeitnehmer und Beschäftigten nach § 26 Abs. 8 BDSG für die Zwecke von People Analytics (vgl. § 1 Abs. 1 dieser Vereinbarung).*
>
> *(2) Personenbezogene Daten aus informationstechnischen Systemen, die nicht für die Zwecke von People Analytics erhoben wurden, dürfen – außer im Rahmen einer anonymisierten Verarbeitung – nicht für diesen Zweck verarbeitet werden. Ein Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO findet nicht statt. Ausnahmen sind gesondert unter Bezugnahme zu dieser Regelung spezifizieren.*

Obwohl insbesondere im Bereich der *Simple People Analytics* eine Zweckvereinbarkeit oftmals gegeben ist, empfiehlt es sich, eine solche Regelung aufzunehmen. Hierdurch werden Streitigkeiten über eine Zweckvereinbarkeit der Nutzung von IT-Daten für People Analytics-Zwecke vermieden. Zudem ist sichergestellt, dass die Arbeitnehmer bereits zum Zeitpunkt der Erhebung informiert sind und nicht befürchten müssen, dass etwaige Daten später mit dem Argument der Zweckkompatibilität für Auswertungen heranzogen werden. Für *Advanced People Analytics* ist nach hiesiger Auffassung ist eine Zweckkompatibilität ohnehin nicht gegeben,[1484] sodass in diesem diese Klausel nur deklaratorisch ist und keinen weitergehenden Regelungsgehalt besitzt. Sie kann dennoch zu einer höheren Akzeptanz bei den Beschäftigten bzw. der Interessensvertretung sorgen. Mangels rechtlicher Gefahren für die Arbeitnehmer werden allerdings zweckkompati-

1483 *Grimm*, ArbRB 2018, 122 (124).
1484 Siehe **E. § 1 III. 2. b**) (**3**).

ble Anonymisierungsvorgänge für anonymisierte APA-Maßnahmen vom strengen Zweckbindungsgrundsatz ausgenommen.[1485]

> *(3) Zur Gewährleistung der Transparenz der Datenverarbeitung werden die Arbeitnehmer bei der Nutzung von IT-Daten in einfacher und verständlicher Sprache über die Kategorien der über sie erhobenen IT-Daten in regelmäßigen Abständen (monatlich) per E-Mail informiert. Die Spezifizierung der Kategorie hat so ausführlich wie möglich zu erfolgen.*

Mögliche Kategorien sind beispielsweise bei E-Mail-Daten: Empfänger (sofern intern), Absender (sofern intern) Sendedatum/-zeit; bei Instant-Messaging (intern): Empfänger bzw. Sender sowie Übermittlungszeit; Office-Auswertungen: Dateiname, Zeitstempel der Dateiöffnung, Zeitstempel der Speicherung.

Eine Information des Betroffenen ist nach Art. 13 DSGVO nur bei der Erhebung notwendig. Dabei ist es ausreichend, dass der Verarbeiter dem Betroffenen die Information auf einer Website bereitstellt.[1486] Sofern die betroffene Person allerdings bereits über die Information der Verarbeitung verfügt, ist keine Information erforderlich (Art. 13 Abs. 4 DSGVO). Zu einer regelmäßigen Information ist der Arbeitgeber nicht verpflichtet. Dennoch kann eine solche sinnvoll sein, um das Bewusstsein über die erfolgende Datenverarbeitung zu stärken, damit eine solche nicht in „Vergessenheit“ gerät. Werden die Daten nicht bei der betroffenen Person erhoben, so muss der Verantwortliche nach Art. 14 Abs. 3 DSGVO unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer angemessenen Frist nach Erlangung, jedoch spätestens nach einem Monat den Betroffenen informieren. Auch hier entfällt die Informationspflicht – analog der Regelung bei der Direkterhebung – nach Art. 14 Abs. 5 lit. a DSGVO, wenn und so weit die betroffene Person bereits über die Information verfügt.[1487] Insofern gilt das soeben Gesagte.

1485 Diese bedürften aufgrund der Statistik-Ausnahme in Art. 5 Abs. 1 lit. b DSGVO ohnehin keinem Kompatibilitätstest.

1486 EuArbRK/*Franzen*, Art. 5 DSGVO Rn. 5; einschränkend BeckOK DatenSR/*Schmidt-Wudy*, Art. 13 DSGVO Rn. 85: nur wenn die Daten ausschließlich für den Betroffnen abrufbar sind; a.A. *Bäcker*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 13 DSGVO Rn. 59: aktive Unterrichtung erforderlich; Bereitstellung auf Website nicht ausreichend.

1487 *Bäcker*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 14 DSGVO Rn. 52.

(4) Soweit es die Auswertungsziele zulassen, werden keine personenbezogenen Daten durch die Systeme der XY erhoben. Ist eine anonyme Datenerhebung nicht möglich, so werden die Daten unverzüglich nach der Erhebung in größtmöglichem Maße aggregiert bzw. anonymisiert. In jedem Falle findet eine Pseudonymisierung der Daten statt.

Aufgrund des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) müssen die Daten auf das für die Zwecke der Verarbeitung erforderliche Maß beschränkt sein; selbiges ergibt sich auch aus § 26 Abs. 1 S. 1 BDSG. Sofern also personenbezogene Auswertungen (wie beispielsweise bei Netzwerk-Graphen) nicht erforderlich sind, sondern aggregierte Daten (z.B. auf Abteilungsebene) ausreichen, sind die Daten zu anonymisieren bzw. – soweit möglich – bereits anonymisiert zu erheben. Die Pseudonymisierung hingegen ist eine technisch-organisatorische Maßnahme zur Datensicherung[1488] und wirkt für den Verarbeiter selbst daher nicht pauschal legitimierend. Im Rahmen der Interessensabwägung kann sie jedoch ermöglichende Wirkung haben, sofern hierdurch weniger Gefahren für die Rechte der Arbeitnehmer bestehen.[1489] Dies wäre der Fall, wenn der Zuordnungsschlüssel gesondert aufbewahrt wird und daher sichergestellt ist, dass eine zufällige Re-Identifizierung des Betroffenen ausscheidet. Der Schlüssel kann beim selben Verantwortlichen liegen, sofern er ausreichend vor unbefugten Zugriffen geschützt ist; eine Einschaltung eines Datentreuhänders ist nicht erforderlich.[1490]

(5) Sofern für die Analysen keine Zuordnung zu einer bestimmbaren Person notwendig ist, sondern eine Auswertung unter einem Pseudonym ausreichend ist, wird der Zuordnungsschlüssel durch eine doppelte Verschlüsselung gesichert. In diesem Rahmen ist es erforderlich, dass die Geschäftsführung von XY und der (Gesamt-)Betriebsrat nur gemeinsam die Entschlüsselung vornehmen können. Die Verschlüsselung muss dem Stand der Technik entsprechen. Eine Entschlüsselung darf nur im Falle eines Straftatverdachts oder einer groben Pflichtverletzung durch den Arbeitnehmer erfolgen.

1488 *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 5 Rn. 2; *Article 29 Data Protection Working Party*, WP 203, S. 3; weitere Nachweise in Fn. 277.

1489 Hierzu **D. § 1 I. 4. c) bb)**.

1490 Vgl. Erwägungsgrund 29; ausführlich unter **D. § 1 I. 4. d)**.

Durch die doppelte Absicherung des Zuordnungsschlüssels wird, sollten Daten bei etwaigen Straftaten oder groben Pflichtverletzungen für repressive Zwecke erforderlich sein, sichergestellt, dass kein einseitiger Missbrauch der Daten stattfindet. Die Voraussetzungen sind geringer als die die des § 26 Abs. 1 S. 2 BDSG, da dort eine grobe Pflichtverletzung nicht ausreichend, sondern ein Straftatverdacht erforderlich ist. Durch klar festgelegte Situationen, in denen eine Dekodierung erfolgen darf, werden die personenbezogenen Daten der Arbeitnehmer besonders gesichert und die Pseudonymisierung entfaltet im Rahmen der Interessenabwägung für Analytics eine privilegierende Wirkung.

IV. Transparenzvorgaben sowie Informations- und Auskunftsrechte der Arbeitnehmer

Im Nachfolgenden werden in Bezug auf verschiedene Anwendungsszenarien mögliche und sinnvolle (allgemeine) Regelungen zur Transparenz dargestellt sowie Konkretisierungsansätze für die allgemeinen Informations- und Auskunftspflichten aus Art. 13 ff. DSGVO aufgezeigt.

§ 4 Datenschutzrechtliche Information

(1) In Form einer „Datenschutzrechtlichen Information zur Erhebung von Beschäftigtendaten“[1491] *wird den Arbeitnehmern eine leicht zugängliche Information über die Pflichten des Arbeitgebers nach dieser Betriebsvereinbarung, dem BDSG und der DSGVO sowie über die Rechte der Arbeitnehmer in Form einer PDF zur Verfügung gestellt. Diese Information wird laufend aktualisiert und die Arbeitnehmer bei Änderungen per E-Mail informiert. Die Information ist in einer verständlichen, klaren und einfachen Sprache zu verfassen. In der in § 3 Absatz 3 genannten zyklischen Information ist diese Information mit einem Hyperlink zu verknüpfen.*

(2) In der Information nach Absatz 1 ist zu erläutern, in welchem Regelungszusammenhang diese Betriebsvereinbarung zu anderen Betriebsvereinbarungen sowie sonstigen betrieblichen Vorgaben und Regelungen steht. Die Normenhierarchie ist grafisch darzustellen.

1491 Beispiel aus *Grimm*, ArbRB 2018, 122 (124).

Die Arbeitnehmer sollen zusätzlich zur monatlichen Information über ihre verarbeiteten Daten allgemeine datenschutzrechtliche Informationen erhalten, um sich einen schnellen Überblick über ihre Rechte und deren Wahrnehmung verschaffen zu können. Dies dient der formellen Transparenz.[1492]

§ 5 Einrichtung einer FAQ-Seite

Zusätzlich zur Veröffentlichung des Normtextes dieser Betriebsvereinbarung wird im Intranet eine „Frequently Asked Questions (FAQ)"-Seite eingerichtet, auf welcher der Normtext dieser Vereinbarung in leichter und verständlicher Sprache erläutert wird. Ergeben sich (allgemeine) Fragen von Arbeitnehmern zu dieser Vereinbarung, sind diese inklusive Beantwortung in den Katalog aufzunehmen. Die FAQ gelten nicht normativ, dienen jedoch aus Auslegungshilfe für die Regelungen in dieser Vereinbarung.

Diese Regelung erfolgt ebenfalls in Erfüllung des Transparenzgebots.[1493]

§ 6 Verzeichnis der Verarbeitungstätigkeiten

Der Arbeitgeber erstellt – zusätzlich zu einem Verzeichnis nach Art. 30 DSGVO – ein Verzeichnis der Verarbeitungstätigkeiten für die einzelnen Verarbeitungsvorgänge nach dieser Betriebsvereinbarung. Es sind die Vorgaben des Art. 30 DSGVO einzuhalten und das Verzeichnis dieser Betriebsvereinbarung anzuhängen.

Das spezifische Verzeichnis der Verarbeitungstätigkeiten dient dazu, einen schnellen Überblick über die nach dieser Betriebsvereinbarung legitimierten Verarbeitungsvorgänge, Kategorien und Empfängern von Daten sowie Löschfristen und technisch-organisatorische Sicherungsmaßnahmen zu erhalten.

§ 7 Informations- und Auskunftsrechte der Arbeitnehmer

(1) Es gelten die gesetzlichen Informations- und Auskunftsrechte gem. Art. 13 ff. DSGVO und §§ 32 ff. BDSG.

1492 *Grimm*, ArbRB 2018, 122 (124).
1493 Siehe hierzu bereits **F. § 2 I.**

(2) In Ergänzung zu den gesetzlichen Informations- und Auskunftsrechten erfolgen in dieser Vereinbarung Konkretisierungen zur Information durch den Arbeitgeber im Rahmen der einzelnen Verarbeitungssituationen.

(3) Die Informationserteilung erfolgt per E-Mail an die dienstliche E-Mail-Adresse des Arbeitnehmers. In begründeten Fällen kann der Arbeitnehmer vom Arbeitgeber eine schriftliche Information verlangen. In jedem Fall ist die Information unentgeltlich zur Verfügung zu stellen. Eine mündliche Information scheidet aus.

§ 7 PA-BV dient zur Konkretisierung der datenschutzrechtlichen Informationspflichten. Da Art. 12 Abs. 1 DSGVO für die Information die Schriftform oder eine andere Form, „gegebenenfalls auch elektronisch“, vorschreibt, ist eine Konkretisierung nach Art. 88 Abs. 2 DSGVO zulässig. Die mündliche Informationserteilung hingegen ist nach Art. 12 Abs. 1 S. 3 DSGVO zwar grundsätzlich ebenfalls zulässig, aufgrund der Komplexität der Analytics-Sachverhalte aber nicht zweckdienlich. Aus diesem Grund wird eine solche Informationserteilung ausgeschlossen. Art. 12 Abs. 1 S. 3 DSGVO ermöglicht lediglich eine mündliche Informationserteilung, falls der Betroffene dies verlangt. Es wird jedoch keine Pflicht des Verantwortlichen statuiert, sodass in einer Betriebsvereinbarung abweichende Regelungen möglich sind.

V. Datenschutzrechtliche Legitimationen

Zusätzlich zur Bezeichnung als datenschutzrechtliche Legitimationsgrundlage in der nicht-normativen Präambel ist es erforderlich, dass die datenschutzrechtlichen Legitimationen für die einzelnen Anwendungsfelder von People Analytics klar festgelegt werden, um den Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. a DSGVO) sowie der Rechtmäßigkeit und Verarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. b DSGVO) einzuhalten.

Im Folgenden werden einige im Rahmen der Untersuchung genannten Szenarien für zulässige People Analytics beispielshaft geregelt.

1. Advanced People Analytics

In einem ersten Schritt sollte die Erhebung bestimmter IT-Systemdaten zur Nutzung für People Analytics legitimiert werden. Pauschale Aussagen verbieten sich an dieser Stelle, sodass verschiedene mögliche Szenarien für den Einsatz von People Analytics dargestellt sowie Regelungsvorschläge aufgezeigt werden sollen.

Szenario 1: Das Unternehmen XY ist ein Versicherungsunternehmen und möchte wissen, wie viele Versicherungsanträge, Policenanpassungen und Beschwerden ein Sachbearbeiter pro Niederlassung im Schnitt pro Tag verarbeitet. Die eingesetzte Software lässt hierbei jeden Vorgang, den ein Sachbearbeiter vornimmt, in diese drei Kategorien einordnen und speichert zu jedem Vorgang den Bearbeiter sowie einen Zeitstempel. Bei der Einführung des Systems war eine Auswertung der Daten für Analysezwecke nicht geplant.

Zu beachten ist hier, dass das Unternehmen lediglich eine Auswertung auf Niederlassungsebene wünscht, die Daten im System aber auf Bearbeiterebene gespeichert werden. Diese Daten werden für die Zuordnung der Vorgänge für Kundenrückfragen sowie Missbrauchsfälle gespeichert. Für die Nutzung in People Analytics müssen diese also aggregiert werden.

§ 8 Vorgangsanalyse von Versicherungsfällen pro Niederlassung

(1) XY ist es gestattet, die personenbezogenen Daten der Arbeitnehmer für die Zwecke der Vorgangsanalyse von Versicherungsfällen auf Niederlassungsebene auszuwerten.

(2) Als Vorgangsanalyse von Versicherungsfällen wird die Berechnung einer durchschnittlichen Anzahl von bearbeiteten Fällen pro Sachbearbeiter und Niederlassung verstanden. Es erfolgt eine Untergliederung der Daten in die Kategorien „Gesamt", „Versicherungsanträge", „Policenanpassungen" und „Beschwerden".

(3) Vor einer Weiterverarbeitung sind die aus dem System ABC verwendeten Daten auf Niederlassungsebene zu aggregieren. Die Bearbeiterkennung des Sachbearbeiters ist aus dem Datensatz zu entfernen. Darüber hinaus hat XY sicherzustellen, dass keine Identifizierbarkeit eines Sachbearbeiters möglich ist. Die Verknüpfung mit weiteren Daten zu weite-

ren Verarbeitungszwecken ist vorbehaltlich einer gesonderten Regelung verboten.

Im vorliegenden Fall ist eine rückwirkende Verarbeitung der Daten nach § 3 Abs. 2 PA-BV möglich, da es sich um anonymisierte Daten handelt. Aufgrund der Anonymität der Daten sind diese nach erfolgter Anonymisierung nicht mehr vom Datenschutzrecht erfasst. Zur Sicherstellung, dass nicht durch Verknüpfung mit anderen Daten diese wieder unbemerkt personenbezogen werden, wird ein Verknüpfungsverbot für die Daten festgelegt.

Szenario 2: Im Unternehmen XY beschwert sich eine Vielzahl von Arbeitnehmern beim Betriebsarzt über Kopf- und Rückenschmerzen. Der Betriebsarzt vermutet als Ursache zu lange Bildschirmarbeitszeiten, verbunden mit zu wenig Pausen. Er möchte seine Vermutung durch eine Auswertung der täglichen PC-Arbeitszeiten der betroffenen Arbeitnehmer bekräftigen und hierdurch auch andere potenziell gefährdete Arbeitnehmer identifizieren, um bei diesen gezielt ein Programm zur Gesundheitsprävention durchführen zu können.

In diesem Szenario ist es nicht die HR-Abteilung, die personenbezogene Daten für People Analytics nutzen möchte, sondern der Betriebsarzt. Die tägliche Bildschirmzeit des jeweiligen Arbeitnehmers stellt kein sensitives Datum im Sinne des Art. 9 Abs. 1 DSGVO dar.

Insbesondere handelt es sich nicht um Gesundheitsdaten gem. Art. 4 Nr. 15 DSGVO, da die Kenntnis der Bildschirmarbeitszeit noch keine Rückschlüsse auf den Gesundheitszustand des Beschäftigten zulässt. Werden diese im Rahmen der betriebsärztlichen Untersuchung mit den Daten vom Betriebsarzt verknüpft, werden diese allerdings zu sensitiven Daten, da diese dann in den Kontext zur Gesundheit gestellt werden. Spätestens zu diesem Zeitpunkt schreibt das Gesetz in § 22 Abs. 1 Nr. 1 lit. b BDSG vor, dass die Verarbeitung durch das ärztliche Personal selbst oder unter deren Verantwortung erfolgt. Der Datenbestand muss also von Zugriffen durch den Arbeitgeber geschützt werden und von den sonstigen Daten abgesondert werden.[1494]

Unabhängig von einer etwaig gesetzlich vorgeschriebenen Absonderung sind die Daten zur Bildschirmnutzung unter dem Aspekt der Erforderlich-

1494 Siehe hierzu bereits **E. § 1 III. 2. c) dd) (2) (d)**.

keit der Datenverarbeitung auch schon vor einer Verknüpfung mit Gesundheitsdaten vor Zugriffen durch den Arbeitgeber zu schützen, da sich hierdurch eine Überwachung der Arbeitnehmer statuieren ließe, die im Rahmen der Bewertung der Eingriffsintensität zu berücksichtigen ist.[1495] Da bei der Verarbeitung (auch durch die Betriebsärztin) Beschäftigungszwecke verfolgt werden, kann eine solche (anders als beispielsweise reine Gesundheits-Apps zur Aufrechterhaltung der Fitness der Arbeitnehmer) in einer Betriebsvereinbarung geregelt werden.

§ 9 Erfassung der Bildschirmarbeitszeit zur Gesundheitsvorsorge

(1) Die Betriebsärztin Maxi Musterfrau erfasst im Rahmen des Arbeitsschutzes und der Gesundheitsvorsorge die Bildschirmarbeitszeiten der Arbeitnehmer. Die Verarbeitung und Erfassung dieser personenbezogenen Daten wird für die Auswertung zur Vermeidung von Überbelastungen durch diese Betriebsvereinbarung legitimiert.

(2) Der Datenbestand ist gesondert vom sonstigen Datenbestand der XY zu erfassen und insbesondere vor Zugriffen durch den Arbeitgeber durch geeignete Maßnahmen nach dem Stand der Technik zu schützen. Verantwortliche Verarbeiterin ist allein Maxi Musterfrau; eine Weitergabe der Daten an Dritte, auch an den Betriebsrat, ist nicht gestattet.

(3) Jeder Arbeitnehmer hat jederzeit die Möglichkeit der Datenverarbeitung für den in Absatz 1 genannten Zweck zu widersprechen. Im Falle eines Widerspruchs ist der gesamte Datensatz zu diesem Arbeitnehmer, der im Rahmen von Absatz 1 erhoben wurde, unverzüglich zu löschen und der Arbeitnehmer über die erfolgte Löschung zu informieren.

(4) Die Betriebsärztin verarbeitet diese Daten ausschließlich zur Gesundheitsvorsorge und Prävention sowie im Rahmen von Behandlungen der betroffenen Arbeitnehmer.

Hierbei sollte der Betriebsarzt in der Betriebsvereinbarung explizit erwähnt werden, sodass eine Weitergabe der Daten an einen (Folge-)Betriebsarzt ausscheidet bzw. nur mit Einwilligung der Arbeitnehmer erfolgen kann. Hintergrund hierfür ist, dass in der Regel ein besonderes Vertrauensverhältnis zum Arzt besteht, welches Grundlage für das Unterlassen

1495 Vgl. zu den Kriterien bei Überwachungsmaßnahme **E. § 4 II. 1. d) bb)**.

eines Widerspruchs sein kann. Im Rahmen der Interessensabwägung sind etwaige Widerspruchsrechte zu berücksichtigen.[1496]

Zu beachten ist, dass einem Arbeitnehmer eine nicht-gewünschte Gesundheitsvorsorge, die nur zu seinem eigenen Schutz dient, nicht aufgedrängt werden kann. So lässt sich auch die gesetzliche Wertung des Art. 9 Abs. 2 lit. b DSGVO verstehen, wonach eine Datenverarbeitung zum Schutz lebenswichtiger Interessen ohne Einwilligung nur möglich ist, wenn der Betroffene zur Abgabe einer solchen außerstande ist. Im Kontext der Betriebsvereinbarung bedeutet dies allerdings nicht, dass eine Verarbeitung nur aufgrund einer Einwilligung erfolgen kann, weil der Arbeitgeber durchaus auch ein zu berücksichtigendes Interesse an der Gesundheit seiner Arbeitgeber hat. Vielmehr hat er Fürsorgepflichten nach § 62 HGB sowie insbesondere § 618 BGB.[1497] Insofern sind bei dieser Verarbeitungssituation die Besonderheiten im Beschäftigungskontext zu berücksichtigen, sodass die Betriebspartner in einer Betriebsvereinbarung eine legitimierende Sonderregelung treffen dürfen, die die Rechte der Arbeitnehmer nach § 75 Abs. 2 BetrVG wahrt.

Gleichwohl wäre hier statt einer Erlaubnis mit Widerspruchsvorbehalt aufgrund der gleichlaufenden Interessen nach § 26 Abs. 2 S. 2 BDSG auch eine Einwilligung des Arbeitnehmers denkbar, deren Spezifika in der BV geregelt werden könnten.

Szenario 3: Das Unternehmen XY hat in der Hauptniederlassung eine Abteilung, die sich mit der Nachstellung und Überprüfung von Versicherungsfällen beschäftigt. Dort ist es in der Vergangenheit gehäuft zu Unfällen gekommen, da PKWs für längere Zeit in der geschlossenen Halle betrieben und Arbeitnehmer aufgrund einer hohen CO-Konzentration durch Abgase ohnmächtig wurden. Um weitere Unfälle zu vermeiden, schafft der Arbeitgeber Wearables an, die den CO-Gehalt der Luft sowie die Vitalparameter der in diesem Bereich beschäftigten Arbeitnehmer überwachen und bei einer Überschreitung gewisser Grenzwerte einen weiteren Arbeitnehmer in der Nähe alarmieren und ggf. bei auffälligen Vitalparametern den Betriebsarzt informieren.

1496 Vgl. zur Vorgängerregelung *Article 29 Data Protection Working Party*, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), S. 55 f.

1497 *Hoffmann*, in: Pielow, Beck'scher Online-Kommentar Gewerbeordnung, § 105 GewO Rn. 182 ff.

In diesem Szenario werden zwei verschiedene Kategorien von Daten verarbeitet: Einerseits werden die Daten zum (groben) Aufenthaltsort eines Arbeitnehmers, verbunden mit dem CO-Gehalt der Luft erfasst, andererseits sensitive Daten in Form der Vitalparameter des Beschäftigten zur schnellen Information des Betriebsarztes im Notfall. Für letztere bedarf es einer besonderen Legitimation, da diese Kategorie von Daten durch Art. 9 Abs. 1 DSGVO einen erweiterten Schutz erhält. Gem. § 26 Abs. 4 S. 1 BDSG können solche Daten jedoch auf Grundlage einer Kollektivvereinbarung verarbeitet werden, sofern die Datenschutzgrundsätze eingehalten werden. Aus § 26 Abs. 3 S. 1 BDSG ergibt sich, dass die Verarbeitung von sensitiven Daten, die zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht – hier: Arbeitsschutz – erforderlich sind und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt, zulässig ist. Besondere Schutzmaßnahmen müssen nach § 22 Abs. 2 BDSG getroffen werden. Diese Regelung entspricht dem in Art. 9 Abs. 2 lit. b DSGVO statuierten Grundsatz. Da in einer Kollektivvereinbarung das Recht nur spezifiziert werden darf, müssen diese Grundsätze (Erforderlichkeit zur Erfüllung einer rechtlichen Pflicht sowie kein Überwiegen der Interessen des Arbeitnehmers) auch in einer Betriebsvereinbarung eingehalten werden.[1498]

Aus dem Grundsatz der Datenminimierung lässt sich ableiten, dass – insbesondere – die Daten zu den Vitalparametern nicht dauerhaft im Datenbestand des Betriebsarztes (zum gesonderten Datenbestand siehe bereits **Szenario 2**) erfasst, sondern nur im Alarmfall übermittelt werden dürfen. Sofern eine Momentaufnahme der erfassten Vitalparameter bei der Überschreitung eines Grenzwertes nicht ausreichend zur Beurteilung des Gesundheitszustandes ist, kann auch eine Übermittlung von Daten in einem Zeitfenster von beispielsweise 15 oder 30 Minuten vor der Überschreitung stattfinden. Dies kann dadurch datenschutzfreundlich implementiert werden, indem die Daten zunächst immer nur für einen gewissen Zeitraum lokal auf dem Wearable gespeichert und erst im Alarmfall an den Betriebsarzt übermittelt werden.

Für die Alarmierung eines nahen Beschäftigten hingegen gibt es mehrere Ansatzpunkte, wie eine solche datenschutzfreundlich und datenminimierend erfolgen kann. Einerseits könnte mit einer Kurzreichweiten-Technologie wie Bluetooth eine Alarmierung der in der Nähe befindlichen Arbeitnehmer erfolgen; bei dieser Lösung besteht allerdings das Problem,

1498 Zur Reichweite des Art. 88 DSGVO bzw. § 26 Abs. 4 BDSG, siehe **D. § 1 V. 2.**

dass die Reichweite in vielen Fällen nur wenige Meter beträgt[1499] und daher eine Alarmierung von Kollegen mitunter nicht sichergestellt werden kann, also keine ausreichende Sicherheit bietet und daher möglicherweise nicht geeignet zur Erfüllung des verfolgten Ziels ist. Ebenfalls unsicher wäre die Speicherung des letzten Bluetooth-Gerätes in der Nähe und Alarmierung dessen, da sich der alarmierte Arbeitnehmer bereits auf dem Heimweg oder an einer anderen Stelle im Unternehmen befinden könnte, sodass andere Arbeitnehmer näher sind und schneller Hilfe leisten könnten. Eine dauerhafte Erfassung der Position von allen Arbeitnehmern im Unternehmen ist aber ebenfalls unter dem Aspekt der Überwachungsvermeidung unzulässig.

Die Lösung, die im Unternehmen XY angewandt wird, ist daher die Folgende: In der Halle des Unternehmens befindet sich ein Empfänger, welcher die in der Nähe befindlichen Wearables registriert. Kein Wearable wird einem konkreten Arbeitnehmer zugeordnet, sondern es meldet sich mit einer zufälligen und regelmäßig neu generierten ID an diesem Empfänger an. Die Reichweite des Empfängers ist so eingestellt, dass immer mindestens ein weiteres Wearable registriert wird. Falls dies nicht möglich ist, erfolgt eine Verstärkung des Signals des Empfängers, bis ein Signal erfasst wird. Sollten trotz Verstärkung keine Wearables registriert werden, erfolgt eine Alarmierung über einen vordefinierten E-Mail- und SMS-Notfall-Verteiler.

Sobald das Wearable einen Alarm auslöst, wird neben der zufälligen ID auch der auf dem Wearable gespeicherte Name des betroffenen Arbeitnehmers an den Empfänger übermittelt.

§ 10 Einsatz von Wearables im Hochrisikobereich

(1) XY stellt seinen Arbeitnehmern, die in der Versicherungsfall-Werkstatt arbeiten, Wearables zur Verfügung, die den CO-Wert der Luft sowie die Herzfrequenz und die Sauerstoffsättigung des Bluts erfassen.

(2) Arbeitnehmer, die sich im Hochrisikobereich aufhalten, sind während der Zeit des Aufenthalts verpflichtet, ein Wearable zu tragen. XY hat für die Einhaltung dieser Pflicht durch geeignete Maßnahmen zu sorgen.

1499 *Möckel*, Bluetooth: Wie hoch ist die Reichweite?, 2019, abrufbar unter: https://www.heise.de/tipps-tricks/Bluetooth-Wie-hoch-ist-die-Reichweite-4523661.html (letzter Abruf am: 28.05.2020).

(3) XY verarbeitet die Daten zum CO-Gehalt der Luft und des Standorts des Wearables zum Zwecke des Arbeitsschutzes. Das Wearable generiert hierbei alle zehn Minuten eine neue, zufällige ID zur Anmeldung am Access Point. Die generierte ID darf nicht einem bestimmten Arbeitnehmer zuordenbar sein. Es erfolgt keine dauerhafte Speicherung der registrierten IDs.

(4) Der Access Point muss so positioniert und eingestellt werden, dass er alle Wearables im Hochrisikobereich sowie mindestens zwei, aber maximal vier weitere Wearables außerhalb dieses Bereiches zur Alarmierung erfasst.

(5) Überschreitet der CO-Wert[1500] des Raumes 30 ppm, so wird der Träger des Wearables vor einer hohen Konzentration gewarnt. Überschreitet der Wert 500 ppm, wird der Träger zum sofortigen Verlassen des Raumes aufgefordert. Bei einem Überschreiten des Grenzwertes von 6.400 ppm erfolgt eine erneute Warnung des Arbeitnehmers und eine Alarmierung aller nach Absatz 4 erfassten Personen. Im letzten Fall übermittelt das Wearable den Namen des Beschäftigten an die alarmierten Personen, um eine rasche Hilfe zu gewährleisten. Werden nach Absatz 4 keine weiteren Personen erfasst, so erfolgt eine Alarmierung über den Verteiler notfall@xy.com.

(6) Bei Überschreiten eines CO-Wertes von 10.000 ppm wird zusätzlich die Betriebsärztin über den Vorfall informiert und neben dem Namen und des konkreten CO-Werts auch die Herzfrequenz sowie die Sauerstoffsättigung der letzten 15 Minuten in ihren Datenbestand übermittelt; die Verarbeitung der Gesundheitsdaten des betroffenen Arbeitnehmers für diesen Zweck wird durch diese Vorschrift legitimiert. Die Übertragung der Daten muss über einen verschlüsselten Kanal nach dem aktuellen Stand der Technik erfolgen.

Die dargestellte Regelung könnte eine Mindestregelung für das **Szenario 3** darstellen. Die Absätze 1 bis 3 regeln hierbei die Verpflichtung des Arbeitgebers, entsprechende Geräte für jeden Arbeitnehmer zur Verfügung zu stellen sowie die Sicherstellung der Verpflichtung der Arbeitnehmer zum

1500 Die im nachfolgenden aufgeführten CO-Grenzwerte wurden an die Grenzwerte der Tabelle auf der Website https://www.kohlenmonoxidmelder.com/kohlenmonoxid/ (letzter Abruf am 28.05.2020) angelehnt.

Tragen solcher. Im Übrigen wird die Datenverarbeitung zum Zwecke des Arbeitsschutzes legitimiert. Um ein Überwachungspotential zu vermeiden, vereinbaren die Betriebspartner die Generierung zufälliger, nicht-zuordenbarer IDs und eine Sendebegrenzung des Empfängers sowie Schwellen für Datenübermittlungen (Absätze 4 und 5). In Absatz 6 wird die Verarbeitung sensitiver Daten durch den Betriebsarzt legitimiert und geregelt, wobei ein deutlich höherer, extrem gesundheitsschädigender Grenzwert für die Übermittlung von Vitaldaten angesetzt wird, um dem besonderen Schutz von Gesundheitsdaten Rechnung zu tragen.

Die zugrunde zulegende Interessenabwägung spricht indes auch nicht gegen derartige eine Verarbeitung dieser Daten: Durch das System wird das höchste Rechtsgut des Arbeitnehmers, das Leben, geschützt und der Eingriff in das Persönlichkeitsrecht durch die Begrenzung der Verarbeitungsvorgänge personenbezogener Daten auf Grenzwertüberschreitungen minimiert. Da der Arbeitgeber zum Gesundheitsschutz verpflichtet ist (§ 618 BGB) und ein enorm hohes Gefahrpotential besteht, gibt es kein Widerspruchsrecht der Arbeitnehmer. Auch die Festlegung einer bestimmten Betriebsärztin für die Datenübermittlung erfolgt aufgrund der Notwendigkeit eines schnellen Handelns (im Gegensatz zum **Szenario 2**) bewusst nicht.

2. Scoring von Bewerbern / Automatisiertes Bewerbermanagement

Eine datenschutzrechtliche Legitimation von Datenverarbeitungen im Bewerbungskontext ist mangels Zuständigkeit des Betriebsrats für Bewerber (vgl. § 5 BetrVG) nicht möglich; da etwaige Betriebsvereinbarungen keine normative Wirkung entfalten, können diese eine Datenverarbeitung nach § 26 Abs. 4 BDSG bzw. Art. 88 DSGVO nicht legitimieren; der Arbeitgeber muss eine etwaige Datenverarbeitung im Rahmen § 26 Abs. 1 S. 1 BDSG legitimieren.[1501]

Dennoch hat der Betriebsrat ein Mitbestimmungsrecht nach §§ 94 Abs. 2, 95 BetrVG (Allgemeine Beurteilungsgrundsätze, Auswahlrichtlinien), wenn ein Scoring durchgeführt wird, da hierfür die Bewerber nach

1501 Siehe **E. § 1 III. 2. c) dd) (3)**; zur Zulässigkeit des Scorings von Bewerbern nach § 26 Abs. 1 BDSG, **E. § 1 III. 2. c) dd) (2) (a)**.

bestimmten, vorgegebenen Kriterien bewertet und ggf. sortiert werden.[1502] Dies sollte ebenfalls in einer Betriebsvereinbarung geregelt werden; da dies jedoch kein spezifisch datenschutz-rechtliches Problem ist und die Auswahlrichtlinien und Beurteilungskriterien vom Einzelfall abhängen, wird an dieser Stelle nicht näher darauf eingegangen.

3. Scoring von Arbeitnehmern / Dashboards

§ 94 Abs. 2 BetrVG gibt dem Betriebsrat bei der Aufstellung allgemeiner Beurteilungsgrundsätze ein Mitbestimmungsrecht. Hat der Arbeitgeber also die Absicht, seine Mitarbeiter zu scoren, so ist es zunächst erforderlich, allgemeine Beurteilungsgrundsätze festzulegen, die Grundlage des Scorings sein sollen.[1503]

In diesem Zusammenhang sollte gleichzeitig die datenschutzrechtliche Legitimation in der Betriebsvereinbarung geregelt werden, auch wenn sich nach hiesiger Auffassung die meisten Auswertungen bereits auf § 26 Abs. 1 S. 1 BDSG stützen lassen.[1504]

Unterschieden werden muss zwischen dem Scoring der Arbeitsleistung und des (sonstigen) betrieblichen Verhaltens. Zwar hat der Arbeitgeber ein berechtigtes Interesse an einer Überwachung der Primärleistungspflicht, andererseits darf diese unter Berücksichtigung des Persönlichkeitsrechts der Arbeitnehmer nicht lückenlos ausgestaltet werden, da ansonsten ein Überwachungsdruck aufgebaut werden könnte, der die Arbeitnehmer daran hindern könnte, ihre Freiheitsrechte wahrzunehmen.[1505] Bei der Überwachung des betrieblichen Verhaltens hingegen ist die Gefahr der Erzeugung eines Leistungsdrucks geringer, sodass sich hier eher längerfristige Überwachungsmaßnehmen für People Analytics statuieren lassen. Streng darauf geachtet werden muss allerdings, dass wirklich nur das arbeitsbezogene Verhalten ausgewertet wird, da andernfalls der Eingriff in das Persönlichkeitsrecht der Arbeitnehmer nicht mehr zu rechtfertigen ist.[1506]

1502 *Göpfert/Dußmann*, NZA-Beilage 2016, 41 (45); *Lützeler/Kopp*, ArbRAktuell 2015, 491 (493); *Fitting*, § 95 Rn. 11; allgemein zu § 95 BetrVG, oben **D. § 2 II. 3**.

1503 Zum Mitbestimmungsrecht des § 94 Abs. 2 BetrVG, vgl. **D. § 2 II. 2. b**).

1504 Siehe **E. § 1 III. 2. c**) **dd**) (**2**) (**b**) und (**c**).

1505 Hierzu bereits **E. § 1 III. 2. a**) **cc**) (**4**).

1506 Zum Scoring des betrieblichen Verhaltens, siehe oben **E. § 1 III. 2. c**) **dd**) (**2**) (**c**).

Szenario 1: Das Unternehmen XY setzt seine neue Kollaborationssoftware *Collabo* ein. Dieses Tool bietet über *AnalyzeIt* eine Schnittstelle an, die es Arbeitnehmern erlaubt, ihre tägliche Arbeitszeit zu analysieren. Die Analysen zeigen jeweils auf, wie viele Minuten täglich ein Arbeit-nehmer mit dem Beantworten von E-Mails verbracht hat, wie viele geschriebene E-Mails tatsächlich beantwortet werden, welcher Anteil der täglichen Arbeitszeit in Meetings verbracht wird und wieviel davon tatsächliche „Focus-Time“ ist, in welcher der Arbeitnehmer ungestört an seinen Projekten arbeiten kann. Die persönlichen Auswertungen sollen nur dem Arbeitnehmer angezeigt werden. Die Team-, Abteilungs- und Unternehmensführung soll hingegen jeweils aggregierte Auswertungen auf Team-, Abteilungs- und Unternehmensebene erhalten.

Ausgangspunkt der Betrachtung sind verschiedene Datenverarbeitungsvorgänge: Einerseits der Auswertungsvorgang mit personenbezogenen Daten für den Arbeitnehmer selbst, andererseits die Anonymisierung und Aggregation der Daten auf Team-, Abteilungs- und Unternehmensebene, um eine Übersicht zu generieren. Die Darstellung erfolgt in Dashboards und in wöchentlichen E-Mails mit einer Zusammenfassung der letzten Woche, in welcher die Veränderung zur Vorwoche aufgezeigt werden soll.

Die Datenverarbeitung für das Arbeitnehmerdashboard kann nicht auf eine Betriebsvereinbarung oder eine gesetzliche Legitimationsgrundlage gestützt werden.[1507] Möglich ist es aber, die Rahmenbedingungen für eine (wirksame) Einwilligung des Arbeitnehmers in der Betriebsvereinbarung festzulegen, wie sich aus Erwägungsgrund 155 ergibt.[1508]

Die Verarbeitung zum Zwecke der Aggregation hingegen kann in einer Betriebsvereinbarung geregelt werden. Dort muss insbesondere festgelegt werden, welcher k-Faktor[1509] notwendig ist, um den Datenschutz der einzelnen Arbeitnehmer wirksam zu realisieren. Sofern eine ausreichende Anonymisierung gesichert ist, überwiegen die Interessen des Arbeitgebers am Anonymisierungsvorgang, sodass dieser auch in einer Betriebsvereinba-

1507 Es mangelt an bereits der Geeignetheit der Datenverarbeitung für das erstrebte Ziel, vgl. **E. § 3 I. 1.**

1508 Zu einer möglichen Regelung der Einwilligung von Arbeitnehmern in einer Betriebsvereinbarung, vgl. *Grimm*, ArbRB 2018, 122 (123).

1509 Anonymisierungsgrad, der angewendet werden muss, um eine tatsächliche Anonymität der Daten und somit Nicht-Anwendbarkeit des Datenschutzrechts sicherzustellen, vgl. **E. § 3 III.**

rung legitimiert werden kann. Aufgrund der „Statistik-Ausnahme“ (vgl. bereits **E. § 1 I. 2. c**)) wäre auch eine Zweckänderung bereits erfasster Daten unproblematisch ohne weiteren Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO möglich.

Durch den Einsatz von Scoring-Technologien erfolgt eine Zweckänderung der ursprünglich zu einem anderen Zwecke erhobenen IT-Daten, für welche eine Regelung durch die Betriebspartner getroffen werden sollte.[1510]

§ 11 Nutzung von AnalyzeIt

(1) XY setzt zur Optimierung der Arbeitsabläufe im Unternehmen AnalyzeIt ein. AnalyzeIt ermöglicht es, Auswertungen des täglichen (digitalen) Arbeitstages auf Arbeitnehmerbasis zu erstellen. Zur Sicherung des Datenschutzes werden individualisierte Auswertungen nur aufgrund einer Einwilligung von Arbeitnehmern erstellt.

(2) In diesem Rahmen wird die Technik des Scorings eingesetzt. Unter Ausnahme von § 3 Abs. 2 dieser Vereinbarung ist die zweckändernde Nutzung der hierfür erforderlichen Daten auf Grundlage einer Einwilligung für das persönliche Dashboard möglich.

(3) AnalyzeIt verarbeitet folgende Kategorien von Daten: Einträge im persönlichen Kalender des Arbeitnehmers, E-Mail-Sender und -Empfänger sowie Versende- und Empfangszeitpunkt, Speicherdatum eines E-Mail-Entwurfs. Es erzeugt einen individuellen, täglichen Produktivitätsscore auf Basis dieser Daten.

(4) Bei der Erstellung des Produktivitätsscores ist sicherzustellen, dass ein wissenschaftliches, mathematisch-anerkanntes Verfahren eingesetzt wird, das zu aussagekräftigen Ergebnissen führt. Auf der AnalyzeIt-Plattform muss die Berechnung des Scores gegenüber dem Arbeitnehmer in Grundzügen erläutert werden. In jedem Falle muss es dem Arbeitnehmer möglich sein, den berechneten Score nachvollziehen zu können.

1510 So bereits oben **E. § 1 I. 1. b**) **bb**); in Bezug auf Leistungsdaten, jedoch ohne spezifisch auf Scoring einzugehen, ebenso *Lambrich/Cahlik*, RDV 2002, 287 (290 f.).

(5) Es ist durch technisch-organisatorische Maßnahmen sicherzustellen, dass nur der Arbeitnehmer selbst Zugriff auf seine individualisierten Auswertungen hat.

(6) Für die Einwilligung des Arbeitnehmers gilt § 26 Abs. 2 BDSG. Die Einwilligung hat durch eine elektronische Zustimmung des Arbeitnehmers mittels einer Check-Box auf der Analytics-Plattform zu erfolgen. Die Freiwilligkeit der Einwilligung wird vermutet. Es ist ausdrücklich darauf hinzuweisen, dass der Arbeitnehmer jederzeit seine Einwilligung widerrufen kann. Abweichend von Art. 7 Abs. 3 S. 2 DSGVO gilt, dass die aufgrund der Einwilligung verarbeiteten personenbezogenen Daten für das persönliche Dashboard rückwirkend und unverzüglich gelöscht werden. Der Arbeitnehmer kann seine Einwilligung jederzeit widerrufen. Die Widerrufserklärung kann im AnalyzeIt-Dashboard direkt oder per E-Mail an widerruf@xy.com erklärt werden.

(7) XY ist gestattet, aggregierte Auswertungen der in Absatz 2 genannten Daten auf Team-, Abteilungs- und Unternehmensebene für Zwecke der People Analytics zu erstellen. Personelle Maßnahmen mit einer negativen Auswirkung auf Arbeitnehmer aufgrund dieser Daten sind ausgeschlossen.

(8) Bei der Aggregation der Daten ist sicherzustellen, dass die Daten nicht mehr einer bestimmbaren Person zuordenbar sind. Im Allgemeinen wird bei einer Aggregation von Daten von mindestens vier Arbeitnehmern von einer Anonymität ausgegangen. Sollte im Einzelfall eine Zuordnung zu einer bestimmbaren Person möglich sein, so sind der Betriebsrat und der betroffene Arbeitnehmer unverzüglich zu informieren und weitere Maßnahmen vorzunehmen, dass weitere Identifizierungen nicht stattfinden. Die individualisierbaren Daten sind unverzüglich zu löschen.

(9) Die aggregierten Auswertungen des eigenen Teams-, der eigenen Abteilung und des Unternehmens sind den Arbeitnehmern zur Verfügung zu stellen. Dies soll, wenn möglich, im persönlichen Dashboard des Arbeitnehmers erfolgen.

Da § 3 Abs. 2 PA-BV regelt, dass die zweckändernde Verarbeitung von personenbezogenen Daten für People Analytics nicht zulässig ist, wird in Abs. 2 dieser Regelung eine Ausnahme von diesem Grundsatz für die

Datenauswertungen für das persönliche Dashboard festgelegt. Aufgrund der Anonymisierung dürfen im Rahmen der aggregierten Darstellung die Daten ohnehin weiterverarbeitet werden, sodass es einer weiteren Ausnahme an dieser Stelle nicht bedarf. In Erweiterung zu den gesetzlichen Vorgaben zur Transparenz von Scoring-Verfahren[1511] wird in Absatz 5 geregelt, dass dem Arbeitnehmer die Berechnung des Score-Werts erläutert werden und der Arbeitnehmer das Ergebnis zumindest nachvollziehen können muss. In Absatz 6 werden die gesetzlichen Vorgaben zur Einwilligung spezifiziert und das Vorliegen einer Freiwilligkeit vermutet. Eine unwiderlegliche Vermutung an dieser Stelle würde die Berücksichtigung des Einzelfalls nicht mehr erlauben und somit gegen den Grundsatz in Art. 7 Abs. 4 DSGVO verstoßen.

In Absatz 7 wird ein individueller k-Faktor als Regel herangezogen; der Arbeitgeber bleibt aber dennoch verpflichtet, die Daten wirksam zu anonymisieren. Diese Regelung legitimiert die Verarbeitung bei einer k-Anzahl von vier Personen, auch wenn hierbei im Einzelfall später festgestellt wird, dass die Gruppengröße für die wirksame Anonymisierung zu klein war. Für diesen Fall wird durch § 7 Abs. 8 PA-BV sichergestellt, dass der Arbeitgeber für den Zeitraum bis zur Anpassung der Gruppengröße eine Legitimationsgrundlage besitzt und hierdurch keinen Datenschutzverstoß begeht. Aufgrund der geringen Wahrscheinlichkeit eines Eingriffes in das Persönlichkeitsrecht einzelner Arbeitnehmer und der eng begrenzten Zeit des Eingriffs, überwiegt das Interesse des Arbeitgebers an der Datenverarbeitung. Notwendig ist diese Regelung, da es schwierig ist, sicherzustellen, dass Auswertungen möglichst präzise sind, gleichzeitig aber keine Rückschlüsse auf einzelne Personen Rückschlüsse zulassen.

Szenario 2: Das Unternehmen XY setzt eine neue Personalverwaltungssoftware ein. In dieser werden die Stammdaten, die betrieblichen Fortbildungen, jährliche Zielvereinbarungen und das Ergebnis halbjährlicher Mitarbeitergespräche erfasst. Ein neues Plugin *ScoreIt* ermöglicht es nun die Mitarbeiter zu scoren und die Passgenauigkeit mit den Anforderungen der Stelle mit einem Punktewert von 0 bis 10 anzeigen zu lassen. Zur Verbesserung der Effizienz sollen mit Hilfe des Scores Entwicklungspotentiale aufgezeigt bzw. Perso-

1511 Diese sind als sehr gering einzustufen, zumal auch Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g und Art. 15 Abs. 1 lit. h DSGVO Informationen über die involvierte Logik nur bei einer automatisierten Einzelfallentscheidung fordern; hierzu bereits **E. § 1 III. 2. c) bb)**.

nalmaßnahmen vorgeschlagen werden. Automatisierte Entscheidungen, z.B. in Form von Anmeldungen für Fortbildungen oder Seminare erfolgen nicht.

Dieses Szenario ist ein mögliches Beispiel für die in **E. § 3 II. 1** erfolgte Untersuchung. Mangels kontinuierlicher Leistungserfassung liegen keine Überwachungsmaßnahmen vor, sodass diese Art der Datenverarbeitung – im Vergleich zu anderen Advanced People Analytics – eher unproblematisch ist.

Auch hier steht aus rechtlicher Sicht zunächst die Problematik einer Zweckänderung im Raum: Im vorliegenden Fall wäre zwar vertretbar, dass auch das weitergehende Scoring für die Durchführung des Arbeitsverhältnisses erforderlich ist, da die Zweckbestimmung des § 26 Abs. 1 S. 1 BDSG sehr weit gefasst ist. Sollen möglicherweise auch noch andere Daten daraus gewonnen werden (z.B. der zukünftige Personalbedarf), die nicht in unmittelbarem Zusammenhang mit der Durchführung des *konkreten* Arbeitsverhältnisses stehen, so ist eine Zweckänderung zwingend erforderlich.[1512] Auch ist nicht sicher, ob ein Gericht das Scoring als vom Erhebungszweck gedeckt beurteilen würde, sodass in jedem Falle Regelungen zur Zweckänderung bzw. -kompatibilität getroffen werden sollten.

Sofern der weitergehende Zweck ebenfalls im Beschäftigungskontext anzusiedeln ist, dürfen die Betriebsparteien aufgrund Art. 88 DSGVO spezifischere Vorschriften zur Zweckkompatibilität treffen.[1513] Voraussetzung ist allerdings, dass die Datenschutzgrundsätze, in diesem Zusammenhang insbesondere die in Art. 6 Abs. 4 DSGVO festgelegten Grundsätze zur Zweckänderung wahren. Insbesondere darf keine Lockerung dieses Gebots stattfinden.[1514]

Mitspracherechte des Betriebsrats bestehen vor allem in § 94 Abs. 2 BetrVG, also in den allgemeinen Beurteilungsgrundsätzen, die dem Scoring zugrunde liegen.

§ 12 Nutzung von ScoreIt

(1) XY setzt in Ergänzung der Personalverwaltungssoftware PersoPlus das Plugin ScoreIt ein. ScoreIt ermöglicht es, die vorhandenen Stammdaten der Arbeitnehmer, Zielvereinbarungen und unterjährigen Mitarbeiterge-

1512 Siehe **E. § 1 I. 1. b) dd)**.
1513 So wohl auch *Körner*, NZA 2019, 1389 (1392).
1514 *Kort*, NZA-Beilage 2016, 62 (64); siehe hierzu bereits **D. § 1 V. 2.**

spräche auszuwerten, mit den Stellenbeschreibungen abzugleichen und verschiedene Punktewert von 0 bis 10 für Entwicklungspotential, Passgenauigkeit auf die Stelle, Passgenauigkeit auf Beförderungsstellen sowie den Gesamteindruck über den Arbeitnehmer zu generieren. Dieser Score dient der Unterstützung der Personalverantwortlichen bei Personalmaßnahmen.

(2) Bei der Verwendung von ScoreIt ist darauf zu achten, dass ein wissenschaftlich-anerkanntes, mathematisches Verfahren verwendet wird, das nachvollziehbare Punktewerte generiert. Es muss XY zu jedem Zeitpunkt möglich sein, den konkreten Punktewert zu erläutern.

(3) XY ist, in Ausnahme des Grundsatzes von § 3 Abs. 2 dieser Vereinbarung, legitimiert, die Daten auf PersoPlus für das Scoring durch ScoreIt in zweckverändernder Weise weiterzuverarbeiten. Hierbei wird davon ausgegangen, dass eine Zweckkompatibilität im Sinne des Art. 6 Abs. 4 DSGVO besteht. Der Arbeitgeber darf keine besonderen Kategorien von Daten im Sinne des Art. 9 DSGVO verwenden. Durch technisch-organisatorische Maßnahmen muss sichergestellt werden, dass die Daten entsprechend dem aktuellen Stand der Technik gegen unbefugte Zugriffe Dritter abgesichert werden.

(4) Die generierten Scorewerte dürfen nicht als alleinige Grundlage für Personalmaßnahmen herangezogen werden. Automatisierte Einzelfallentscheidungen sind verboten. Jede vorgeschlagene Maßnahme muss inhaltlich durch einen entscheidungsbefugten Vorgesetzten überprüft und genehmigt werden. Jede benachteiligende Maßnahme, die auf einem Scorewert beruht, ist unter Zugrundelegung der für den Score erheblichen Datenbasis gegenüber dem Arbeitnehmer und dem Betriebsrat zu begründen.

(5) Der betroffene Arbeitnehmer hat den Anspruch, jederzeit Einblick in seinen Scorewert zu nehmen und eine Begründung zur Zusammensetzung in Textform zu fordern. Ebenfalls hat er die Möglichkeit gegen den generierten Wert Widerspruch einzulegen und seinen Standpunkt darzustellen. XY ist verpflichtet, den Scorewert unter Berücksichtigung der Stellungnahme des Arbeitnehmers zu überprüfen und ihm das Ergebnis der Überprüfung schriftlich mitzuteilen.

Im ersten Absatz wird die Verwendung des Plugins *ScorteIt* geregelt sowie die verschiedenen Kategorien von Daten, die Grundlage für das Scoring sind, benannt. Absatz 2 regelt in Anlehnung an – den unionsrechtswidrigen[1515] – § 31 BDSG die Vorgaben für das Scoring, wobei – über die Vorgaben hinaus – noch sichergestellt wird, dass der Arbeitgeber den Score jederzeit erläutern können muss. Dies erfolgt auch gegenüber dem Arbeitnehmer in Textform (Absatz 5). Ersteres wird bereits durch das Transparenzerfordernis des Art. 5 Abs. 1 lit. a DSGVO gefordert; letzteres erfolgt – jedenfalls im Hinblick auf das SCHUFA-Urteil des BGH[1516] zur Vorgängerreglung – wohl überschießend zur aktuellen Rechtslage nach DSGVO und BDSG und zum Vorteil des Arbeitnehmers.[1517] Die Legitimation in Absatz 3 zur Zweckänderung basiert auf einer Einschätzung der Zweckkompatibilität nach Art. 6 Abs. 4 DSGVO und ist durch Art. 88 DSGVO gedeckt. Dass von einer Zweckkompatibilität ausgegangen wird, soll eine Beweislastumkehr statuieren. Ob und inwiefern dies im Hinblick auf die nach h.M.[1518] geltende Beweislastregelung in Art. 5 Abs. 2 DSGVO rechtlich zulässig ist, ist in Wissenschaft und Literatur noch nicht geklärt. Ein Scoring von Gesundheitsdaten hingegen scheidet aufgrund der strengen Voraussetzungen des § 26 Abs. 3 S. 1 BDSG aus.[1519] Absatz 4 der Regelung sichert, dass keine (verbotene) automatisierte Einzelfallentscheidung nach Art. 22 DSGVO vorliegt. Zuletzt wird in § 8 Abs. 5 DSGVO noch ein weitgehendes Widerspruchsrecht statuiert, welches es in dieser Form nach Art. 22 Abs. 3 DSGVO nur bei der automatisierten Einzelfallentscheidung gibt, nicht jedoch, wenn ein menschlicher Entscheider die Entscheidung unter Berücksichtigung eines Scores trifft.[1520]

1515 Ausführlich oben **E. § 1 III. 2. c) bb) (1)**.

1516 BGH, Urt. v. 28.01.2014 – VI ZR 156/13, ZD 2014, 306.

1517 So wird von einem großen Teil der Literatur die Rechtsprechung weiterhin für anwendbar erachtet, vgl. *Klar*, BB 2019, 2243 (2251); *von Lewinski/Pohl*, ZD 2018, 17 (23); kritisch BeckOK DatenSR/*Schmidt-Wudy*, Art. 15 DSGVO Rn. 78.3.

1518 Zum Regelungsgehalt von Art. 5 Abs. 2 DSGVO: Beweislastregelung zulasten des Verantwortlichen: *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 5 DSGVO Rn. 186; *Pötters*, in: Gola, Datenschutz-Grundverordnung, Art. 5 DSGVO Rn. 34; Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 32; *Wolff*, D. I. Grundsätze der Datenverarbeitung, in: Schantz/Wolff, Das neue Datenschutzrecht, Rn. 449; wohl auch *Hamann*, BB 2017, 1090 (1092); keine Beweislastregelung: Sydow/*Reimer*, Art. 5 DSGVO Rn. 53; *Veil*, ZD 2018, 9 (10): Beweislastregel "nur" i.R.d. Haftung.

1519 Hierzu **E. § 1 III. 2. c) dd) (2) (d)**.

1520 Zum Inhalt des Rechts nach Art. 22 Abs. 3 DSGVO vgl. bereits **D. § 1 V. 3. e)**.

4. Automatisierte Entscheidungen im laufenden Beschäftigungsverhältnis

Während im vorherigen Szenario automatisierte Einzelfallentscheidungen explizit ausgeschlossen wurden, soll im Nachfolgenden ein Regelungsbeispiel für automatisierte Entscheidungen auf Basis des durch das fiktive Tool *ScoreIt* generierten Scores dargestellt werden. Die Untersuchung beschränkt sich auf automatisierte Entscheidungen im laufenden Beschäftigungsverhältnis, da der Betriebsrat für Bewerber mangels Zuständigkeit keine datenschutzrechtliche Regelungskompetenz besitzt.[1521]

Da der Anwendungsbereich für automatisierte Einzelfallentscheidungen nach Art. 22 DSGVO im laufenden Beschäftigungsverhältnis sehr begrenzt ist,[1522] wird im Nachfolgenden ein Beispiel für eine Automatisierung aufgezeigt, welches mangels rechtlicher Wirkung aber nicht von Art. 22 Abs. 1 DSGVO erfasst ist.

> **Szenario:** Auf Basis von *ScoreIt* sollen die Scores zum Entwicklungspotential sowie der Passgenauigkeit auf die jetzige Stelle und Beförderungsstellen zur Grundlage für Fortbildungsvorschläge genommen werden. Der Schulungsanbieter bietet eine standardisierte Schnittstelle bereit, die von der Personalsoftware genutzt werden kann, um Schulungen und deren einzelne Lernziele automatisiert auszuwerten und mit Arbeitnehmerprofilen abzugleichen. Eine Datenübermittlung an den Anbieter findet nicht statt. Werden bei einem Arbeitnehmer Defizite in bestimmten Bereichen erkannt, kann über diese Schnittstelle eine passende Schulung gefunden werden, um den Arbeitnehmer in diesen Bereichen fortzuentwickeln. XY möchte nun automatisiert den Arbeitnehmern entsprechende Schulungen anbieten.

Das genannte Szenario zeigt ein mögliches Anwendungsbeispiel für eine in **E. § 2 II. b**) untersuchte automatisierte Einzelfallentscheidung. Da es sich lediglich um einen Vorschlag handelt und die Entscheidung daher keine rechtliche Wirkung entfaltet, fällt dieses Szenario nicht unter Art. 22 Abs. 1 DSGVO. Dennoch sollte aufgrund der betriebsverfassungsrechtlichen Mitbestimmungsrechte des Betriebsrats und des zugrundeliegenden Scorings eine kollektivrechtliche Regelung getroffen werden, die das Szenario regelt.

1521 Im Detail **E. § 1 III. 1. c**) **bb**) sowie **E. § 1 III. 2. c**) **dd**) (**3**).
1522 Vgl. **E. § 2 III**.

§ 13 Automatisierte Fortbildungsvorschläge auf Basis von ScoreIt

(1) ScoreIt soll neben dem in § 12 genannten Anwendungsszenario auch dafür genutzt werden, Arbeitnehmern auf Basis ihres Entwicklungsscores und der Passgenauigkeitsscores maßgeschneiderte Fortbildungen vorzuschlagen, um die fachlichen und persönlichen Kompetenzen weiter zu fördern.

(2) In diesem Zusammenhang ist XY legitimiert, die durch ScoreIt generierten Daten, in Ausnahme von § 3 Abs. 2 dieser Vereinbarung, für Fortbildungszwecke zu verarbeiten.

(3) Der Arbeitnehmer erhält hierzu eine E-Mail mit einem Fortbildungsvorschlag und entsprechenden Terminen für die Fortbildung. In dieser E-Mail ist dem Arbeitnehmer die Entscheidungsgrundlage für den Vorschlag auf Basis ihres Scores darzustellen. Ferner soll, nach Möglichkeit, die durch die Maßnahme zu erzielende Scoreverbesserung aufgezeigt werden. In keinem Fall wird der Arbeitnehmer durch einen automatisierten Vorschlag zur Teilnahme an einer Fortbildung verpflichtet.

(4) Soll ein Arbeitnehmer zu einer Fortbildung auf Basis von ScoreIt verpflichtet werden, so ist sicherzustellen, dass ein Vorgesetzter den generierten Vorschlag unter Zugrundelegung bisheriger Personalgespräche und Erfahrungswerten überprüft und die Teilnahme zur Fortbildung unter Ausübung des Direktionsrechts persönlich anordnet.

(5) Bei begrenzten Ausbildungskapazitäten ist dem Betriebsrat vor Übermittlung der Vorschläge die Vorschlagsliste des Systems vorzulegen. Dieser hat nach Erhalt der Liste eine Woche Zeit, um die Liste zu überprüfen und eigene Vorschläge einzubringen. XY und Betriebsrat einigen sich unter Beachtung des von ScoreIt generierten Scores auf eine gemeinsame Liste.

(6) In jedem Falle ist dem Betriebsrat eine Liste der geplanten Fortbildungen zu übermitteln, sodass dieser eigene Vorschläge einbringen kann. Unter Berücksichtigung des von ScoreIt generierten Werts entscheiden Arbeitgeber und Betriebsrat über die Teilnahme der Vorschläge des Betriebsrats an den angebotenen Fortbildungen. Die betroffenen Arbeitnehmer werden nach dem in Absatz 3 geregelten Verfahren über die Fortbildung informiert.

Die Absätze 1 und 2 regeln, für welche Zwecke die Scores – neben den in § 13 PA-BV bereits geregelten Verarbeitungssituationen – genutzt werden dürfen. Zwar könnte die Verarbeitung für Fortbildungszwecke womöglich bereits unter die weite Formulierung der „Personalmaßnahmen" subsumiert werden; sicherheitshalber sollte dieser Zweck aber nochmals explizit erwähnt werden, da durch einen reinen Vorschlag noch keine Personalmaßnahme stattfindet. In Absatz 3 wird die Einbeziehung und Information des Arbeitnehmers geregelt und sichergestellt, dass die Verarbeitung und der generierte Vorschlag der in Art. 5 Abs. 1 lit. a DSGVO geforderten Transparenz entspricht. Zum Ausschluss einer – möglicherweise verdeckten – automatisierten Einzelfallentscheidung nach Art. 22 Abs. 1 DSGVO regelt Absatz 4, dass eine Anordnung einer Fortbildung (nachteilige rechtliche Wirkung) nur auf Basis der Datengrundlage und nicht allein des Scores erfolgen darf.[1523] Zur Sicherung der in §§ 96 ff. BetrVG geregelten Mitbestimmungsrechte des Betriebsrats dienen die Absätze 5 und 6 der Regelung.[1524]

5. Netzwerk-Analysen

Netzwerk-Analysen stellen ein besonderes Anwendungsfeld von Advanced People Analytics dar, insbesondere wenn diese in Form eines „Enterprise Social Graph" aus Echtzeitdaten generiert werden sollen. Aufgrund der zu regelnden Feinheiten und dem kritischen Spannungsfeld zwischen (zulässiger) Netzwerk-Analyse und unzulässiger Überwachung der Beschäftigten ist die präzise Regelung einer solchen Technik in einer Betriebsvereinbarung geboten.

Hinweis: Vorweg wird auf die unsichere Rechtslage im Hinblick auf die Anwendbarkeit der Regelungen des TKG auf Arbeitgeber, die ihren Arbeitnehmern die Privatnutzung der betrieblichen Kommunikation erlauben, hingewiesen.[1525] Obwohl nach hiesiger Auffassung die §§ 88 ff. TKG auf Arbeitgeber nur beschränkt Anwendung finden, ist aufgrund

---

1523 Andernfalls hat inhaltlich bereits der Algorithmus die Entscheidung getroffen und es liegt ein Fall des Art. 22 Abs. 1 DSGVO vor; siehe hierzu **D. § 1 V. 3. c) aa)**.

1524 Zu den Beratungs- und Mitbestimmungsrechten des Betriebsrats vgl. bereits **E. § 2 II. b) bb)**.

1525 Inzwischen dürfte die Rechtsprechung dazu tendieren, die §§ 88 ff. TKG nicht mehr auf Arbeitgeber anzuwenden, dennoch ist dies bislang nicht höchstrichterlich geklärt. Hierzu im Detail **D. § 3 I. 2.**

der strafrechtlichen Risiken sowie der anderslautenden Auffassung der Datenschutzbehörden eine private Nutzung der betrieblichen Telekommunikation durch Arbeitgeber zu untersagen, wenn der Kommunikationsverkehr (auch lediglich Verbindungsdaten) überwacht und einer Analyse zugeführt werden soll.

Regelungen zur Netzwerkanalyse und Privatnutzung betrieblicher IT ist aufgrund der Mitbestimmungsrechte des Betriebsrats nach § 87 Abs. 1 Nr. 1 und 6 BetrVG optimalerweise in einer Betriebsvereinbarung zu regeln.[1526]

Szenario: Neben einem Textverarbeitungsprogramm, Tabellenkalkulationsprogramm und Präsentationsprogramm beinhaltet die obige Kollaborationssoftware *Collabo* des Unternehmens XY auch ein E-Mail-Programm, wobei die E-Mails ebenfalls durch den *Collabo*-Server verarbeitet werden. Daneben gibt es ein Instant-Messaging-Programm *TeamIt*, über welches sich Chat-Nachrichten und Dateien versenden lassen und Videokonferenzen veranstaltet werden können. Die Arbeitnehmer nutzen zur innerbetrieblichen Kommunikation – auch über die vom Arbeitgeber zur Verfügung gestellten Mobiltelefone – vor allem *TeamIt* zur Kommunikation. Das Management von XY stellt fest, dass innerbetriebliche Kommunikationsabläufe nicht über die vor-gesehenen Hierarchien erfolgen. Es wird vermutet, dass verteilt im Unternehmen einzelne Arbeitnehmer immer wieder als Experten in Anspruch genommen werden. Das Management möchte diese identifizieren.

Eine mögliche Regelung dieses Sachverhalts könnten die folgenden Ausführungen darstellen:

§ 14 Verbot der Privatnutzung der betrieblichen Kommunikation und Durchführung von Netzwerk-Analysen

(1) Die Nutzung der betrieblichen Kommunikationsplattformen (E-Mail, Telefonie und TeamIt) für private Zwecke ist verboten.

(2) XY nutzt die Verbindungsdaten der betrieblichen Kommunikationsplattformen für Netzwerk-Analysen durch den Einsatz eines Enterprise Social Graph. Ziel der Analysen ist es, das informelle Netzwerk des

1526 Zu letzterem *Müller*, öAT 2019, 1 (3).

Netzwerks darzustellen und hierdurch die formale Hierarchie des Unternehmens zu optimieren.

(3) Nach Information der Arbeitnehmer über die Zweckerweiterung der Verarbeitung der Verbindungsdaten ist XY legitimiert, die personenbezogenen Verbindungsdaten für Netzwerkanalysen zu nutzen. Die Arbeitnehmer sind mindestens eine Woche vor Aktivierung des Enterprise Social Graph umfassend in Textform per E-Mail sowie durch deutlich sichtbaren Hinweis im Intranet zu informieren. Diese Information umfasst auch die Warnung, dass hierdurch bei unerlaubter Privatnutzung private Beziehungen zwischen einzelnen Arbeitnehmern aufgedeckt werden können.

(4) Personelle Maßnahmen auf Basis der durch den Enterprise Social Graph gewonnen Erkenntnisse dürfen nicht zum Nachteil der Arbeitnehmer angewandt werden. Ausnahme sind repressive Maßnahmen, die unter den Voraussetzungen des § 26 Abs. 2 BDSG ergriffen werden.

(5) Der Zugriff auf den Enterprise Social Graph ist auf das erforderliche Minimum zu beschränken; jeder Zugriff auf das System ist zu dokumentieren.

(6) Dem Betriebsratsvorsitzenden und seinem Stellvertreter sind unter den Voraussetzungen des Absatz 5 Einsicht in den Enterprise Social Graph zu gewähren; die hierdurch erlangten Kenntnisse unterliegen der Geheimhaltungspflicht.

(7) Die Daten der Netzwerkanalyse sind spätestens nach einem Jahr nach Erhebung zu löschen; wurde das mit der Verarbeitung erstrebte Ziel vorher erreicht, sind die Daten nach Zielerreichung unverzüglich zu löschen.

Wie bereits eingangs aufgeführt, wird in Absatz 1 aufgrund der Rechtsunsicherheit die Privatnutzung verboten. In Absatz 2 wird das verfolgte Ziel statuiert und in Absatz 3 die hierfür notwendige Datenverarbeitung nach vorheriger Information der Arbeitnehmer legitimiert.

Über die gesetzlichen Vorgaben nach Art. 13 f. DSGVO hinaus ist wegen der grundsätzlichen hohen Eingriffsintensität der Maßnahme aufgrund einer „Dauerüberwachung“ bei (unerlaubter) Privatnutzung noch eine zu-

sätzliche Warnung aufzunehmen, welche Folgen eine solche haben könnte.

Absatz 4 stellt eine Garantie dar, dass die Analysen in aller Regel keine negativen Folgen für Arbeitnehmer haben werden; dies ist ein Kriterium, das im Rahmen einer Güterabwägung ebenfalls von entscheidender Bedeutung ist.[1527] Lediglich bei Straftatverdacht dürfen die Daten für repressive Maßnahmen verwendet werden. In den Absätzen 5 und 6 wird zur Vermeidung von Missbrauch der Zugriff auf das Minimum beschränkt (auch auf Betriebsratsebene) und eine Dokumentationspflicht für Zugriffe statuiert.

Zuletzt wird eine Speicherbegrenzung in überschießender Tendenz zum Grundsatz nach Art. 5 Abs. 1 lit. e DSGVO von höchstens einem Jahr festgelegt. Somit scheidet aus, dass die Daten unter dem Vorwand der Erforderlichkeit nahezu unbegrenzt gespeichert werden.

VI. Technische und organisatorische Sicherungsmaßnahmen

Ferner sollten in der Betriebsvereinbarung Regelungen zu technischen und organisatorischen Sicherungsmaßnahmen nach Art. 25 DSGVO aufgenommen werden, die konkret auf das jeweilige Unternehmen bzw. den jeweiligen Betrieb abgestimmt sind.[1528]

> ***§ 15 Spezifische technische und organisatorische Sicherungsmaßnahmen***
>
> *(1) Es ist sicherzustellen, dass alle aufgrund dieser Vereinbarung verarbeiteten Daten nach dem Stand der Technik verschlüsselt werden. Beim Einsatz eines symmetrischen Verschlüsselungsverfahrens ist (Stand: Mai 2021) mindestens AES-256 einzusetzen.*
>
> *(2) Die Daten sind darüber hinaus, soweit möglich, zu pseudonymisieren. Eine Rückführung zum Klarnamen darf erst im Rahmen der Anzeige der Daten für den Endanwender erfolgen.*
>
> *(3) Es ist ein Berechtigungskonzept zu erarbeiten, in welchem alle Arbeitnehmer mit Zugriff auf die personenbezogenen Daten in dieser Betriebs-*

1527 Siehe hierzu **E. § 4 II. 1. d) bb) (4)**.
1528 Vgl. *Körner*, NZA 2019, 1389 (1392).

vereinbarung konkret benannt werden und begründet wird, weshalb ein Zugriff auf die Daten erforderlich ist. Über jede Berechtigungsvergabe ist der Betriebsrat zu informieren. Alle Personen mit einem Zugriff auf die personenbezogenen Daten nach dieser Vereinbarung sind zur Geheimhaltung zu verpflichten.

(4) Ferner ist ein Löschkonzept zu entwickeln, welches dieser Betriebsvereinbarung angehängt wird und verpflichtend ist. In diesem müssen für jede Kategorie der im Rahmen dieser Vereinbarung erhobenen Daten Speicherfristen sowie der konkrete Vorgang der Löschung und dessen Dokumentation festgelegt werden. Des Weiteren sollen Überprüfungsmöglichkeiten des Betriebsrats hinsichtlich einer sicheren Löschung festgelegt werden. Dieses Löschkonzept dient der Sicherstellung der Datenminimierung und Speicherbegrenzung und ist mit dem Betriebsrat abzustimmen. Es ist an geeigneter Stelle im Intranet zu veröffentlichen.

Die Regelungen der Absätze 1 und 2 dienen dem technischen Datenschutz. Durch die Sicherstellung einer Verschlüsselung sowie weitgehender Pseudonymisierung der Daten werden die Risiken für die Betroffenen bei Datenpannen minimiert. Im Falle eines Datenlecks ist dann zwar gem. Art. 33 DSGVO die Datenschutzbehörde zu informieren, bei ausreichender Sicherung gem. Art. 34 Abs. 3 lit. a DSGVO jedoch nicht der Betroffene. Das Berechtigungs- und Löschkonzept ist eine organisatorische Maßnahme zum Datenschutz; durch einen möglichst geringen Zugriffskreis an (internen) Datenempfängern sowie der Verpflichtung zur Geheimhaltung wird sichergestellt, dass keine unbefugten Dritten Kenntnis der Daten erlangen.

VII. Verfahren bei Streitigkeiten

Zur Vermeidung von Streitigkeiten über die Reichweite eines Mitbestimmungsrechts und darüber, ob es sich bei den einzelnen Klauseln um freiwillige Vereinbarungen nach § 88 BetrVG handelt, empfiehlt es sich, die Anrufung einer Einigungsstelle durch jede Seite sowie die Verbindlichkeit der Entscheidung dieser vorzusehen.[1529] Hierdurch lässt sich vermeiden, dass mitunter hochkomplexe IT-Fragen vor Gericht ausgefochten werden müssen; die Parteien können stattdessen eine Einigungsstelle anrufen, die

1529 *Körner*, NZA 2019, 1389 (1393).

sich auf IT-Betriebsvereinbarungen spezialisiert und somit für die Entscheidung die notwendige Fachkompetenz hat.

§ 16 Verfahren bei Streitigkeiten / Einigungsstelle

(1) Bei Streitigkeiten über die Anwendung, Auslegung oder Reichweite dieser Vereinbarung sind sowohl XY als auch der Betriebsrat berechtigt, die Einigungsstelle anzurufen.

(2) Die Entscheidung der Einigungsstelle ist verbindlich.

VIII. Sonstiges

Die weiteren zu treffenden Regelungen betreffen das Inkrafttreten, die Laufzeit der Vereinbarung sowie Kündigungsfristen, Nachwirkung, eine Neuverhandlungspflicht bei Kündigung sowie eventuelle Anpassungspflichten bei Änderungen von Rahmenbedingungen. Schlussendlich sollten noch in den Schlussbestimmungen der Ausschluss mündlicher Nebenabreden sowie eine salvatorische Klausel vorgesehen werden.[1530] Von Abdruck dieser wird abgesehen.

1530 Formulierungsvorschläge bei *Grimm*, ArbRB 2018, 122 (127).

G. Zusammenfassung und Thesen

§ 1 Zusammenfassung der wesentlichen Untersuchungsergebnisse

Die vorliegende Untersuchung zeigt, dass sich die aufgezeigten Problemstellungen immer wieder auf dieselbe Frage zurückführen lassen: Überwiegen die Interessen des Arbeitgebers an der Datenverarbeitung jene des Arbeitnehmers, nicht überwacht zu werden bzw. seine Daten für sich zu behalten?

Hierbei ist gleichgültig, in welchem rechtlichen Tatbestand die Prüfung erfolgt: Art. 6 Abs. 1 lit. f DSGVO, § 26 Abs. 1 S. 1 BDSG oder § 75 Abs. 2 BetrVG. In allen Fällen steht das berechtigte Interesse des Arbeitgebers an der Datenverarbeitung im Mittelpunkt. Dies gilt unabhängig davon, ob europäische Grundrechte, wie bei der Prüfung von Art. 6 Abs. 1 lit. f DSGVO und § 26 Abs. 1 S. 1 BDSG abgewogen werden müssen oder (ergänzungsweise) nationale im Rahmen von § 75 Abs. 2 BetrVG.

In datenschutzrechtlicher Hinsicht wird dies am Kriterium der Erforderlichkeit festgemacht, welches genau diese beschriebene Interessensabwägung statuiert. Der Datenverarbeiter hat jedoch keinen eigenen Einschätzungsspielraum und das Kriterium ist sehr vage bestimmt. Es bestehen – nicht zuletzt aufgrund der hohen Bußgeldandrohungen in Art. 83 DSGVO – hohe Unsicherheiten bei der Anwendung dieser unbestimmten Legitimationsgrundlagen.

Die untersuchten People Analytics sind von diesem Problem besonders betroffen: Einerseits ist noch nicht abschließend geklärt, wie weit die DSGVO im Bereich des Beschäftigtendatenschutzes Regelungsspielräume für nationale Regelungen und Kollektivvereinbarungen eröffnet[1531], andererseits verhält sich auch das neue Datenschutzrecht im normativen Teil in keiner Weise zu aktuellen Techniken wie Big Data oder künstliche Intelligenz. Auch das Profiling hat in Art. 4 Nr. 4 der Datenschutzgrundverordnung lediglich eine Legaldefinition erhalten; eine konkrete Regelung dieser Technik ist – abseits von Nebenpflichten – jedoch nicht erfolgt. Zu Recht wird die neue Verordnung daher als defizitär bezeichnet und dem Gesetzgeber vorgeworfen, dass er das Prinzip der Technikneutralität

1531 *Dammann*, ZD 2016, 307 (310) bezeichnet die Regelung des Art. 88 DSGVO als konturlos.

missverstanden und hierdurch eine Risikoneutralität geschaffen hat.[1532] Die spezifischen Risiken der neuen Technologien werden in der DSGVO schlicht nicht adressiert.

Fatal wäre es, solche Techniken pauschal als unzulässig bzw. nicht erforderlich für die Durchführung des Beschäftigungsverhältnisses oder die Wahrnehmung berechtigter Interessen zu betrachten.[1533] Dies verhindert nicht nur technologischen Fortschritt, sondern wird auch den berechtigten Interessen der Parteien im Einzelfall nicht gerecht.

Insbesondere im Bereich der Simple People Analytics, also in jenem Bereich, wo nur einfache mathematische und statistische Verfahren eingesetzt werden, bestehen datenschutzrechtlich kaum Bedenken, diese Weiterverarbeitung von Arbeitnehmerdaten für Auswertungen als „erforderlich für die Durchführung des Beschäftigungsverhältnisses" anzusehen.

Im Bereich der Advanced People Analytics hingegen muss besonders darauf geachtet werden, dass durch die aktive Datenerhebung kein unzulässiger Überwachungs- und Anpassungsdruck erzeugt wird und die Verarbeitung transparent gestaltet wird. Die zweckverändernde Datenverarbeitung personenbezogener Daten ist nur bei Anonymisierung der Daten zulässig, andernfalls muss bereits bei Erhebung der Daten der Zweck entsprechend weit festgelegt werden.

Werden diese Voraussetzungen eingehalten, können People Analytics in aller Regel rechtskonform ausgestaltet werden. Aufgrund einer vorhandenen Einschätzungsprärogative und der aus betriebsverfassungsrechtlichen Gründen ohnehin vorhandenen Notwendigkeit einer innerbetrieblichen Regelung, ist es geboten eine die Datenverarbeitung legitimierende Betriebsvereinbarung über People Analytics abzuschließen.

§ 2 Kernthesen

Die Ergebnisse dieser Untersuchung sowie die vorgestellten Lösungsansätze zum rechtskonformen Einsatz von People Analytics im Betrieb bzw. Unternehmen lassen sich anhand folgender Kernthesen zusammenfassen:

1532 *Roßnagel*, DuD 2017, 290.

1533 So aber beispielsweise BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 118.3: nur auf Basis einer Einwilligung möglich; für den Enterprise Social Graph *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 81.

I. People Analytics-Verfahren für das konkrete Arbeitsverhältnis können auf § 26 Abs. 1 S. 1 BDSG gestützt werden; bei allgemeinen Analysen findet Art. 6 Abs. 1 lit. f DSGVO Anwendung.

Sofern die Daten, die durch People Analytics generiert werden, der Entscheidung über oder Durchführung des konkreten Beschäftigungsverhältnisses dienen, ist § 26 Abs. 1 S. 1 BDSG die einschlägige Legitimationsgrundlage. Werden personenbezogene Daten von Bewerbern oder Arbeitnehmern für andere betriebliche Zwecke genutzt, ist Art. 6 Abs. 1 lit. f DSGVO einschlägig.

Beiden Normen ist gemein, dass sie eine Verhältnismäßigkeitsprüfung, verbunden mit einer Interessensabwägung im Einzelfall erfordern. Sofern durch Analyse-Verfahren kein unzulässiger Überwachungs- und Anpassungsdruck erzeugt wird (etwa durch eine lückenlose Überwachung der Primärleistungspflicht oder des gesamten Verhaltens des Arbeitnehmers), sind diese in der Regel zulässig.

Eine Ausnahme gilt nur, wenn die Ergebnisse ausschließlich dem Arbeitnehmer zur Verfügung gestellt werden sollen, der Arbeitgeber aber keinen Einblick erhält. In diesem Fall muss auf die Einwilligung nach § 26 Abs. 2 BDSG zurückgegriffen werden.

II. Profiling- und Scoring-Techniken sind unter den allgemeinen Voraussetzungen der Datenverarbeitung zulässige Mittel zur Verarbeitung personenbezogener Daten.

Der Begriff des *Profiling*s wird in Art. 4 Nr. 4 DSGVO definiert. Vermissen lässt sich jedoch eine konkrete Regelung für die Zulässigkeit dieser Verfahrensart. Die Datenschutz-Grundverordnung knüpft hieran lediglich weitere Folgen (wie beispielsweise die Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung) und Rechte (erweiterte Informationsrechte sowie ein Widerspruchsrecht). Die Formulierung des Art. 22 Abs. 1 DSGVO ist missglückt. Zurückzuführen ist dies auf die kontroversen Auffassungen von Kommission und Europäischem Parlament. Letztlich unterliegen Profiling-Technologien den allgemeinen Verarbeitungsvoraussetzungen nach Art. 6 DSGVO bzw. § 26 Abs. 1 BDSG im Bereich des Beschäftigtendatenschutzes, wobei die höhere Eingriffsintensität durch solche Verfahren im Rahmen der Abwägung zu berücksichtigen ist. Der Begriff des *Scoring*s hingegen ist ein rein nationaler Begriff, den der deutsche Gesetzgeber in § 31 BDSG näher definiert. Trotz Unionsrechtswidrigkeit der nationalen Regelung sind die dort statuierten Grundsätze für

diese Technik einzuhalten, da sie bereits durch die Datenschutzgrundverordnung vorgegeben werden. Eine (grundsätzlich) verbotene automatisierte Entscheidung nach Art. 22 Abs. 1 DSGVO liegt aber vor, wenn nur noch auf Basis der durch Profiling oder Scoring erzeugten Ergebnisse entschieden wird.

III. Im Rahmen eines Arbeitnehmer-Scorings ist der Einsatz künstlicher Intelligenz zulässig.

Der Einsatz künstlicher Intelligenz bei der Verarbeitung personenbezogener Daten wird von einer Unbehaglichkeit begleitet. Denn die innere Logik eines solchen Systems stellt für den Menschen eine Art „Black Box" dar und die enorme Anzahl der entscheidungsrelevanten Datenpunkte in einem neuronalen Netz ist für einen Menschen nicht mehr überblickbar.

Aus diesem Grund darf ein neuronales Netz auch nicht mit personenbezogenen Daten genährt werden. Zulässig bleibt es aber, mit Hilfe von anonymen Daten und künstlicher Intelligenz Faktoren und Gewichtungen für (Personal-)Entscheidungen zu untersuchen und hieraus eine transparente Formel zu schaffen, die bestimmte Eigenschaften von Bewerbern oder Arbeitnehmern mit bestimmten Faktoren gewichtet.

Das Scoring erfordert keine vollständige Transparenz der Entscheidungskriterien, sondern eine Basisrationalität und hierausfolgend grundsätzlich nachvollziehbare Entscheidungen. Wie bei menschlichen Entscheidungen kann einem solchen System aber nicht abverlangt werden, die Gewichtung jedes Faktors bis ins kleinste Detail für einen Menschen verständlich begründen zu müssen. Dies ist nicht Aufgabe des Datenschutzrechts. Ausreichend ist es daher, wenn beispielsweise feststeht, dass die Durchschnittsnote der Arbeitszeugnisse im Rahmen einer Bewerbung mit 23 % in die Gesamtbewertung einfließt, um eine ausreichende Transparenz zu gewährleisten. Dies ist bereits mehr als bei einer menschlichen Entscheidung, die „aus dem Bauch heraus" gefällt wird, vorhanden ist.

IV. Nicht jede Profilerstellung im Arbeitsverhältnis ist eine gesondert legitimationsbedürftige Profiling-Maßnahme.

Profiling erfordert eine Bewertung persönlicher Merkmale eines Betroffenen durch automatisierte Verfahren. Dies liegt mangels automatisierter Bewertung bei der Sammlung und Zusammenführung von Arbeitnehmerdaten in einer digitalen Personalakte noch nicht vor. Dies gilt selbst dann, wenn durch diese Art der Speicherung Filterungen, Sortierungen und

Suchen oder gar Trendanalysen mit Hilfe der linearen Regression möglich sind.

Ebenso handelt es sich nicht um eine Profiling-Maßnahme, wenn in einem Assessment-Center Daten über einen Arbeitnehmer erhoben werden, die nicht von einem Computer verarbeitet und bewertet werden, sondern von einem Psychologen. In diesem Fall wird letztendlich die Bewertung des Menschen durch einen Menschen vorgenommen und der Computer stellt allenfalls ein Hilfsmittel zur Datenverarbeitung dar.

V. Automatisierte Entscheidungen auf Basis von People Analytics sind in vielen Fällen mangels rechtlicher Wirkung zulässig. Bei nachteiligen Folgen können solche in begrenzten Einzelfällen auf die Ausnahme von Art. 22 Abs. 2 lit. a DSGVO gestützt werden.

Art. 22 Abs. 1 DSGVO statuiert ein generelles Verbot automatisierter Einzelfallentscheidungen. Dies gilt allerdings nur insofern als dass hierdurch ein Nachteil für den Betroffenen entsteht. Von diesem Verbot macht Absatz 2 Ausnahmen, u.a. wenn dies für den Abschluss oder die Erfüllung eines Vertrags erforderlich ist. Diese Ausnahme statuiert eine Verhältnismäßigkeitsprüfung, wobei der Maßstab aufgrund des Ausnahmecharakters deutlich strenger ist als die Erforderlichkeit der Datenverarbeitung nach allgemeinen Grundsätzen. Eine automatisierte Entscheidung im Beschäftigungskontext ist demnach zulässig, wenn die vorhandenen Ressourcen nicht ausreichend sind, alle Vorschläge, die ein Bewertungssystem generiert, noch einzeln zu überprüfen. Dies kann bei Bewerberfluten oder Massenentlassungen der Fall sein.

Außerhalb des Anwendungsbereiches des Verbots befinden sich mangels Entscheidung Vorgänge, die lediglich bereits zuvor festgelegte Entscheidungen, beispielsweise auf vertraglicher Basis, ausführen. Anwendungsfall wäre beispielsweise die Berechnung und Auszahlung einer umsatzabhängigen variablen Vergütung.

VI. Der Arbeitgeber unterliegt auch bei erlaubter Privatnutzung der betrieblichen IKT-Struktur nicht den strengen Vorgaben des Telekommunikationsrechts, wenn betriebsbezogene Daten verarbeitet werden.

Das Telekommunikationsrecht erfordert für seine Anwendbarkeit, dass der Arbeitgeber ein Diensteanbieter im Sinne des TKG ist. Aufgrund

des wettbewerbsrechtlichen Charakters des Gesetzes und dem mangelnden Entgeltcharakter einer solchen Dienstleistung für den Arbeitnehmer, ist dies zu verneinen. Dies gilt nur insofern als der Arbeitgeber keine am Markt typische Leistungen wie beispielsweise Hotspot-Dienste zur ausschließlichen Privatnutzung anbietet. Dienen die Netze vorwiegend betrieblichen Zwecken, dürfen die Verbindungsdaten unter allgemeinem Datenschutzrecht verarbeitet werden. Zur Sicherstellung der Grundrechte der Arbeitnehmer können technische Lösungen eingesetzt werden. Ein praktisches Beispiel wäre die Kennzeichnung von Nachrichten als „privat", um diese vor arbeitgeberseitigen Zugriffen zu schützen. Gängige, auf dem Markt angebotene Kommunikationslösungen bieten diese Funktionalität bereits seit Jahren an.

VII. Der Einsatz eines Enterprise Social Graph und entsprechenden Dashboards zur Darstellung des innerbetrieblichen Netzwerks mit Hilfe von Echtzeitauswertungen kann datenschutzkonform ausgestaltet werden.

Dashboards dienen vordergründig zur Anzeige der durch People Analytics generierten Daten in menschlich lesbarer Form. Sie sind daher keine datenschutzrechtlich besonders zu beurteilende Analyseform. Maßgeblich ist allerdings auch hier, dass die Empfänger von personenbezogenen Daten, also die zugriffsberechtigten Personen, auf das erforderliche Minimum beschränkt werden. Dies gilt insbesondere dann, wenn Echtzeitdaten wie beispielsweise beim Enterprise Social Graph oder der Auswertung von IT-Protokolldaten angezeigt werden sollen. Hier könnte bei einer zu großen Anzahl der Empfänger der Daten ein Überwachungsdruck statuiert werden, der die Verarbeitung unzulässig werden lässt. Für solche Auswertungen sollte, insbesondere, wenn Vorgesetze einen Zugriff erhalten, auf eine Datenaggregation mit hinreichend anonymisierter Wirkung zurückgegriffen werden.

VIII. Die lockere Zweckbindung der Datenschutzgrundverordnung ermöglicht in breitem Maße eine zweckfremde Weiterverarbeitung personenbezogener Daten für People Analytics.

Die Zweckbindung ist der absolute Kern des Datenschutzrechts; am Verarbeitungszweck wird die Rechtmäßigkeit jeglicher Datenverarbeitung gemessen. Dennoch verfolgt die Datenschutzgrundverordnung nicht mehr den strengen Zweckbindungsgrundsatz des BDSG a.F., sondern erlaubt

auch zweckfremde Verarbeitungen, soweit sie mit dem ursprünglichen Zweck kompatibel sind.

Die in der Praxis wichtigste Regelung findet sich in Art. 5 Abs. 1 lit. b DSGVO: Die sogenannte Statistik-Ausnahme legitimiert anonymisierte Big-Data-Auswertungen, auch im privaten Sektor mit kommerziellem Charakter, sofern das Ergebnis dieser keine personenbezogenen Daten sind. Für das Feld der People Analytics stehen damit weitgehende Analyse-Möglichkeiten offen. Mangels der Gefahr etwaiger Folgen ist auch der nach Art. 6 Abs. 1 lit. f DSGVO zu legitimierende Vorgang der Anonymisierung datenschutzrechtlich ohne Weiteres zulässig.

Eine Zweckentfremdung von technischen Protokolldaten für personenbezogene Analytics ist jedoch nicht erlaubt; hier werden die Kriterien des Kompatibilitätstests nach Art. 6 Abs. 4 DSGVO nicht erfüllt und der Arbeitgeber muss die Daten bereits für den spezifischen Zweck der Analytics erheben.

IX. Die Betriebspartner können in einer Betriebsvereinbarung ein eigenständiges Datenschutzregime für das Anwendungsfeld der People Analytics statuieren.

Die Regelungsmöglichkeiten im Bereich des Beschäftigtendatenschutzes werden durch Art. 88 DSGVO festgelegt. Eine Vollharmonisierung in diesem Bereich findet durch die Datenschutzgrundverordnung nicht statt, vielmehr werden durch Art. 88 Abs. 2 DSGVO Mindeststandards festgelegt, die auch im Bereich des Beschäftigtendatenschutzes eingehalten werden müssen. Daraus darf aber nicht geschlussfolgert werden, dass auf keinen Fall negative Abweichungen von den Regelungen der Verordnung stattfinden dürfen. Die Mitgliedsstaaten und Betriebspartner dürfen auf Basis von Art. 88 DSGVO ein eigenständiges Beschäftigtendatenschutzregime statuieren, das jedoch den Grundsätzen der DSGVO entsprechen muss. In diesem Sinne gehen nationale oder kollektivrechtliche Regelungen der DSGVO als *lex specialis* vor. Insbesondere für die Betriebspartner hat dies den Vorteil, dass ihnen insoweit (in den Grenzen des § 75 Abs. 2 BetrVG sowie Art. 88 Abs. 2 DSGVO) eine Einschätzungsprärogative darüber zusteht, inwiefern eine Datenverarbeitung erforderlich ist. Diese Möglichkeit der Regelung schafft für die Beteiligten Rechtssicherheit in einem Bereich, bei welchem die gesetzlichen Regelungen durch ihre Unterkomplexität und den hohen Bußgeldrisiken technologischen Fortschritt zu verhindern drohen.

Literaturverzeichnis

Abel, Ralf-Bernd, Automatisierte Entscheidungen im Einzelfall gem. Art. 22 DS-GVO. Anwendungsbereich und Grenzen im nicht-öffentlichen Bereich, ZD 2018, S. 304–307.

ders., Einmeldung und Auskunfteitätigkeit nach DS-GVO und § 31 BDSG. Frage der Rechtssicherheit im neuen Recht, ZD 2018, S. 103–108.

Ajunwa, Ifeoma/Freidler, Sorelle/Scheidegger, Carlos/Venkatasubramanian, Suresh, Hiring by Algorithm: Predicting and Preventing Disparate Impact, SSRN Electronic Journal 2016, DOI: 10.2139/ssrn.2746078.

Albrecht, Jan Philipp, Das neue EU-Datenschutzrecht - von der Richtlinie zur Verordnung. Überblick und Hintergründe zum finalen Text für die Datenschutz-Grundverordnung der EU nach der Einigung im Trilog, CR 2016, S. 88–98.

Albrecht, Jan Philipp/Jotzo, Florian, Das neue Datenschutzrecht der EU. Grundlagen, Gesetzgebungsverfahren, Synopse, Baden-Baden 2017.

Arning, Marian, Kapitel 6: Umgang mit Betroffenen, in: Moos/Schefzig/Arning (Hrsg.), Die neue Datenschutz-Grundverordnung. Mit Bundesdatenschutzgesetz 2018, Berlin 2018.

Arnold, Christian, § 316 Die Betriebsvereinbarung, in: Kiel/Lunk/Oetker/Richardi/Wlotzke/Wißmann (Hrsg.), Münchener Handbuch zum Arbeitsrecht, München 2019 [zitiert als: MHdB-ArbR/*Arnold*, § 316 Die Betriebsvereinbarung].

Arnold, Christian/Günther, Jens (Hrsg.), Arbeitsrecht 4.0. Praxishandbuch zum Arbeits-, IP- und Datenschutzrecht in einer digitalisierten Arbeitswelt, München 2018.

Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation (WP 203). Adopted on 02 April 2013, Brüssel 2013 [zitiert als: *Article 29 Data Protection Working Party*, WP 216].

dies., Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), Brüssel 2014 [zitiert als: *Article 29 Data Protection Working Party*, WP 217].

dies., Opinion 05/2014 on Anonymization Techniques (WP 216). Adopted on 10 April 2014, Brüssel 2014 [zitiert als: *Article 29 Data Protection Working Party*, WP 216].

Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff "personenbezogene Daten". Angenommen am 20. Juni 2007, Brüssel 2007 [zitiert als: *Artikel-29-Datenschutzgruppe*, WP 136].

dies., Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 "wahrscheinlich ein hohes Risiko mit sich bringt" (WP 248), Brüssel 2017 [zitiert als: *Artikel-29-Datenschutzgruppe*, WP 259].

dies., Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679 (WP 251). angenommen am 3. Oktober 2017, zuletzt überarbeitet und angenommen am 6. Februar 2018, Brüssel 2018 [zitiert als: *Artikel-29-Datenschutzgruppe*, WP 251].

dies., Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679 (WP 259). angenommen am 28. November 2017 zuletzt überarbeitet und angenommen am 10. April 2018, Brüssel 2018 [zitiert als: *Artikel-29-Datenschutzgruppe*, WP 259].

Ascheid, Reiner/Preis, Ulrich/Schmidt, Ingrid (Hrsg.), Kündigungsrecht. Großkommentar zum gesamten Recht der Beendigung von Arbeitsverhältnissen. 6. Aufl., München 2021 [zitiert als: APS/*Bearbeiter*].

Atabaki, Armita/Biemann, Torsten, Potenziale der Datenanalyse für HR (People Analytics), in: Petry/Jäger (Hrsg.), Digital HR. Smarte und agile Systeme, Prozesse und Strukturen im Personalmanagement, Freiburg, München, Stuttgart 2018, S. 125–136.

Athanas, Christoph, Big Data im HR: Sieben praktische Gedanken über ein Trendthema, abrufbar unter: https://blog.metahr.de/2015/02/05/big-data-im-hr-sieben-praktische-gedanken-ueber-ein-trendthema/ (letzter Abruf am: 27.09.2017).

Auer-Reinsdorff, Astrid/Conrad, Isabell (Hrsg.), Handbuch IT- und Datenschutzrecht. 3. Aufl., München 2019.

Bachner, Michael, Mitbestimmung des Betriebsrats bei der Auswahl technischer Überwachungseinrichtungen, DB 2006, S. 2518–2519.

Barman, Arup/Ahmed, Hussain, Big Data in Human Resource Management - Developing Research Context (letzter Abruf am: 29.09.2017).

Bausewein, Christoph, Bewerberauswahl und Personalentwicklung mittels psychologischer Eingungstests, DuD 2016, S. 139–143.

Benecke, Alexander/Wagner, Julian, Öffnungsklauseln in der Datenschutz-Grundverordnung und das deutsche BDSG - Grenzen und Gestaltungsspielräume für ein nationales Datenschutzrecht, DVBl 2016, S. 600–608.

Benkert, Daniel, Beschäftigtendatenschutz in der DS-GVO-Welt, NJW-Spezial 2018, S. 562–563.

Bersin, Josh, BigData in HR Why it's here and What it Means, 2012, abrufbar unter: http://blog.bersin.com/bigdata-in-hr-why-its-here-and-what-it-means/ (letzter Abruf am: 17.10.2017).

ders., The Geeks Arrive in HR: People Analytics Is Here, 2015, abrufbar unter: https://www.forbes.com/sites/joshbersin/2015/02/01/geeks-arrive-in-hr-people-analytics-is-here/ (letzter Abruf am: 17.10.2017).

ders., Why People Management is Replacing Talent Management, 2015, abrufbar unter: http://joshbersin.com/2015/01/why-people-management-is-replacing-talent-management/ (letzter Abruf am: 17.10.2017).

Betz, Christoph, Automatisierte Sprachanalyse zum Profiling von Stellenbewerbern. Überprüfung der datenschutzrechtlichen Zulässigkeit des Praxistrends, ZD 2019, S. 148–152.

Bissels, Alexander/Mayer-Michaelis, Isabel/Schiller, Jan, Arbeiten 4.0: Big Data-Analysen im Personalbereich, DB 2016, S. 3042–3049.

Bitkom e.V., Entscheidungsfindung mit Künstlicher Intelligenz. Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung, Berlin 2017.

ders., Risk Assessment & Datenschutz-Folgenabschätzung. Leitfaden, Berlin 2017.

Bitkom Research GmbH, Big Data im Personalmanagement. Ergebnisse Unternehmensbefragung, München, Berlin 2015, abrufbar unter: https://business.linkedin.com/content/dam/business/talent-solutions/regional/de-de/c/pdfs/BigDataimPersonalmanagement_LinkedIn_Bitkom.pdf (letzter Abruf am: 26.09.2019).

Bitkom Research GmbH/LinkedIn Deutschland, Österreich, Schweiz, "Big Data" verändert das Personalwesen nachhaltig. Studie von LinkedIn und Bitkom Research zeigt: Große Unternehmen setzen Big Data bereits verstärkt für Kernaufgaben ein / Erst unternehmensexterne Daten erschließen gesamtes Potenzial, München, Berlin 2015.

Bitkom Research GmbH/Personio GmbH, Woran scheitern Einstellungen? Eine Studie von Bitkom Research im Auftrag von Personio 2018.

Blinn, Nicole, Wearables und Arbeitnehmerdatenschutz - Vom freiwilligen Selbstoptimierer zum Kontrollinstrument des Arbeitgebers?, in: Taeger (Hrsg.), Smart world - smart law? Weltweite Netze mit regionaler Regulierung, Edewecht 2016, S. 519–534.

Block, Helga, 23. Datenschutz- und Informationsfreiheitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Düsseldorf 2017 [zitiert als: *Block*, 23. DIB LDI NRW].

Blum, Benjamin/Kainer, Friedemann, Rechtliche Aspekte beim Einsatz von KI in HR: Wenn Algorithmen entscheiden, PERSONALquarterly 2019, S. 22–27.

Bodie, Matthew T./Cherry, Miriam A./McCormick, Marcia L./Tang, Jintong, The Law and Policy of People Analytics, Colorado Law Review 2017, S. 961–1042.

Boehme-Neßler, Volker, Das Ende der Anonymität, DuD 2016, S. 419–423.

Böhm, Wolf-Tassilo, Anmerkung zu BAG, Beschl. v. 07.05.2019 - 1 ABR 53/17 - Einblicksrecht des Betriebsrats in Bruttoentgeltlisten, NZA-RR 2019, S. 530–532.

Bostrom, Nick, How long beforce Superintelligence?, 1998, abrufbar unter: https://nickbostrom.com/superintelligence.html (letzter Abruf am: 11.10.2019).

Brecht, Corinna/Steinbrück, Anne/Wagner, Manuela, Der Arbeitnehmer 4.0? Automatisierte Arbeitgeberentscheidungen durch Sensorik am smarten Arbeitsplatz, PinG 2018, S. 10–15.

Brink, Stefan/Schmidt, Stephan, Die rechtliche (Un-)Zulässigkeit von Mitarbeiterscreenings - Vom schmalen Pfad der Legalität, MMR 2010, S. 592–596.

Brink, Stefan/Schwab, Sabrina, Beschäftigtendatenschutz: Zwischen wirtschaftlicher Abhängigkeit und informationeller Selbstbestimmung, RDV 2017, S. 170–187.

Brisch, Klaus/Pieper, Fritz, Das Kriterium der "Bestimmbarkeit" bei Big Data-Analyseverfahren. Anonymisierung, Vernunft und rechtliche Absicherung bei Datenübermittlungen, CR 2015, S. 724–729.

Broy, Dominic/Heinson, Dennis, B. II. Die automatisierte Einzelfallentscheidung im Beschäftigungsverhältnis, in: Weth/Herberger/Wächter/Sorge (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis. Praxishandbuch zum Arbeitnehmerdatenschutz, München 2019 [zitiert als: WHWS/*Broy/Heinson*, B. II. Die automatisierte Einzelfallentscheidung im Beschäftigungsverhältnis].

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

ders., 2 Grundsätze des Datenschutzrechts, in: Tinnefeld/Buchner/Petri/Hof (Hrsg.), Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht, Berlin, Boston 2020, S. 215–330.

ders., 4 Datenverarbeitung im nicht-öffentlichen Bereich, in: Tinnefeld/Buchner/Petri/Hof (Hrsg.), Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht, Berlin, Boston 2020, S. 394–467.

Buchner, Benedikt/Kühling, Jürgen, Die Einwilligung in der Datenschutzordnung 2018, DuD 2017, S. 544–548.

Buchner, Herbert, Vom "gläsernen Menschen" zum "gläsernen Unternehmen". Zur rechtlichen Bindung der Datenerfassung und -verarbeitung im Betrieb, ZfA 1988, S. 449–488.

Buhl, Samir/Frieling, Tino/Krois, Christopher/Malorny, Friederike/Münder, Matthias/Richter, Barbara/Schmidt, Laura (Hrsg.), Der erwachte Gesetzgeber. Regulierung und Deregulierung im Arbeitsrecht : Dokumentation der 7. Assistentinnen- und Assistententagung im Arbeitsrecht vom 27.- 29.07.2017, Baden-Baden 2017.

Bundesministerium des Innern, Hintergrundpapier zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes. - Kabinettbeschluss vom 25.08.2010 - 2010, abrufbar unter: https://rsw.beck.de/docs/librariesprovider5/rsw-dokument e/Hintergrundpapier (letzter Abruf am: 07.11.2019).

Bundesministerium für Arbeit und Soziales (BMAS), "Grünbuch – Arbeit weiter denken" - Arbeiten 4.0, Berlin 2015 [zitiert als: *BMAS*, Grünbuch Arbeiten 4.0].

dass., "Weißbuch - Arbeit weiter denken" - Arbeiten 4.0, Berlin 2017 [zitiert als: *BMAS*, Weißbuch Arbeiten 4.0].

Byers, Philipp, B. VII. GPS-Ortung, in: Weth/Herberger/Wächter/Sorge (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis. Praxishandbuch zum Arbeitnehmerdatenschutz, München 2019 [zitiert als: WHWS/*Byers*, B. VII. GPS-Ortung].

Conrad, Isabell/Hausen, Dominik, § 37 Arbeitsrechtliche Bezüge, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, München 2019 [zitiert als: HdbIT-DSR/*Conrad/Hausen*, § 37 Arbeitsrechtliche Bezüge].

Conrad, Isabell/Licht, Susanna/Redeker, Helmut/Strittmatter, Marc, § 22 Cloud Computing, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, München 2019 [zitiert als: HdbIT-DSR/*Conrad et al.*, § 22 Cloud Computing].

Conrad, Isabell/Schneider, Jochen, § 14 Softwarepflege und Support, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, München 2019 [zitiert als: HdbIT-DSR/*Conrad/Schneider*, § 14 Softwarepflege und Support].

Conrad, Isabell/Treeger, Christina, § 34 Recht des Datenschutzes, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, München 2019 [zitiert als: HdbIT-DSR/*Conrad/Treeger*, § 34 Recht des Datenschutzes].

Conrad, Sebastian Conrad, Künstliche Intelligenz - Die Risiken für den Datenschutz, DuD 2017, S. 740–744.

Council of Europe, The protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/Rec(2010)13 and explanatory memorandum, Strasbourg 2011 [zitiert als: *Council of Europe*, CM/Rec(2010)13].

Culik, Nicolai, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung. Möglichkeiten und Grenzen für Big Data-Anwendungen im Personalwesen, Berlin 2018.

Dammann, Ulrich, Erfolge und Defizite der EU-Datenschutzgrundverordnung. Erwarteter Fortschritt, Schwächen und überraschende Innovationen, ZD 2016, S. 307–314.

Dammann, Ulrich/Simitis, Spiros (Hrsg.), EG-Datenschutzrichtlinie. Kommentar, Baden-Baden 1997.

Däubler, Wolfgang, Digitalisierung und Arbeitsrecht, AuR Sonderausgabe Juli 2016, S. 2–44.

ders., Digitalisierung und Arbeitsrecht. Internet, Arbeit 4.0 und Crowdwork. 6. Aufl., Frankfurt am Main 2018.

ders., Gläserne Belegschaften. Das Handbuch zum Beschäftigtendatenschutz. 8. Aufl., Frankfurt am Main 2019.

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter (Hrsg.), BetrVG Betriebsverfassungsgesetz. Mit Wahlordnung und EBR-Gesetz. 17. Aufl., Frankfurt am Main 2020 [zitiert als: DKW/*Bearbeiter*].

Däubler, Wolfgang/Wedde, Peter/Weichert, Thilo/Sommer, Imke (Hrsg.), EU-Datenschutz-Grundverordnung und BDSG-neu. Kompaktkommentar : EU-Datenschutz-Grundverordnung (EU-DSGVO), neues Bundesdatenschutzgesetz (BDSG-neu), weitere datenschutzrechtliche Vorschriften. 2. Aufl., Frankfurt am Main 2020.

Dauses, Manfred A./Ludwigs, Markus (Hrsg.), Handbuch des EU-Wirtschaftsrechts. 51. Aufl., München 2020.

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft Office 365 in hessischen Schulen, 09.07.2019, abrufbar unter: https://datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-f%C3%BCr-datenschutz-und (letzter Abruf am: 03.06.2020).

Deuster, Lisa, Automatisierte Entscheidungen nach der Datenschutz-Grundverordnung, PinG 2016, S. 75–78.

Deutscher Bundestag, Beschlussempfehlung und Bericht des Innenausschusses (4. Ausschuss), Berlin 2009 [zitiert als BT-Drs. 16/13657].

ders., Beschlussempfehlung und Bericht des Ausschusses für Inneres und Heimat (4. Ausschuss) zu dem Gesetzesentwurf der Bundesregierung - Drs. 19/4674, 19/5414 -. Entwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU - 2. DSAnpUG-EU), Berlin 2019 [zitiert als BT-Drs. 19/11181].

Deutscher Gewerkschaftsbund (DGB), Darum ist Microsoft Office 365 ein Fall für den Betriebsrat, 24.07.2017, abrufbar unter: https://www.dgb.de/themen/++co++0342f31e-6c85-11e7-b8f9-525400e5a74a (letzter Abruf am: 28.02.2020).

Die Bundesregierung der Bundesrepublik Deutschland, Entwurf eines Betriebsverfassungsgesetzes. (Entwurf der Bundesregierung), Bonn 1971 [zitiert als BT-Drs. VI/1786].

dies., Entwurf eines Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz - ElGVG), Berlin 2008 [zitiert als BT-Drs. 16/3078].

dies., Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680. (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU), Berlin 2017 [zitiert als BT-Drs. 18/11325].

dies., Unterrichtung durch die Bundesregierung: Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU - DSAnpUG-EU) - Drucksache 18/11325. Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung, Berlin 2017 [zitiert als BT-Drs. 18/11655].

Diercks, Nina, Big Data-Analysen & Scoring in der (HR-)Praxis. Dürfen aus allgemein zugänglichen personenbezogenen (Arbeitnehmer-)Daten Score-Werte erstellt und genutzt werden?, PinG 2016, S. 30–36.

Dorschel, Joachim, Praxishandbuch Big Data, Wiesbaden 2015.

Dreyer, Stephan/Schulz, Wolfgang, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme? Potentiale und Grenzen der Absicherung individueller, gruppenbezogener und gesellschaftlicher Interessen, Gütersloh 2018, abrufbar unter: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/BSt_DSGVOundADM_dt.pdf (letzter Abruf am: 02.04.2021).

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

dies., Beschäftigtendatenschutz nach der Umsetzung der Datenschutz-Grundverordnung: Viele Änderungen und wenig Neues, NZA 2017, S. 1081–1085.

Dzida, Boris, Big Data und Arbeitsrecht, NZA 2017, S. 541–546.

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

Dzida, Boris/Groh, Naemi, Diskriminierung nach dem AGG beim Einsatz von Algorithmen im Bewerbungsverfahren, NZA 2018, S. 1917–1922.

dies., People Analytics im Personalbereich - Rechtiche Risiken beim Einsatz von Algorithmen im Betrieb, ArbRB 2018, S. 179–182.

Eckhardt, Jens, § 16. Automatisierte Entscheidungsfindung einschließlich Profiling, in: Rüpke/von Lewinski/Eckhardt (Hrsg.), Datenschutzrecht. Grundlagen und europarechtliche Neugestaltung, München 2018, S. 231–243.

Eckhardt, Jens/Kramer, Rudi, Auftragsdatenverarbeitung beim Einsatz von Persönlichkeitsanalysetools, DuD 2016, S. 144–149.

Ehmann, Eugen, Der weitere Weg zur Datenschutzgrundverordnung - Näher am Erfolg, als viele glauben?, ZD 2015, S. 6–12.

Ehmann, Eugen/Helfrich, Marcus (Hrsg.), EG-Datenschutzrichtlinie. Kurzkommentar, Köln 1999.

Ehmann, Eugen/Selmayr, Martin (Hrsg.), DS-GVO. Datenschutz-Grundverordnung : Kommentar, München, Wien 2017 [zitiert als: Ehmann/Selmayr (2017)/*Bearbeiter*].

dies., DS-GVO. Datenschutz-Grundverordnung : Kommentar. 2. Aufl., München, Wien 2018 [zitiert als: Ehmann/Selmayr/*Bearbeiter*].

Ehmann, Horst, Anmerkung "Mitbestimmung bei Bildschirmarbeitsplätzen", EzA § 87 BetrVG 1972 Bildschirmarbeitsplatz Nr. 1.

Eichenhofer, Johannes, Vom Zweckbindungsgrundsatz zur Interessenabwägung?, PinG 2017, S. 135–140.

Eichler, Carolyn, Zulässigkeit der Tätigkeit von Auskunfteien nach der DS-GVO, RDV 2017, S. 10–13.

Eisemann, Hans/Seidel, Ralf/Voelzke, Thomas, Stichwort "Kündigung, betriebsbedingte", in: Küttner (Hrsg.), Personalbuch 2020. Arbeitsrecht, Lohnsteuerrecht, Sozialversicherungsrecht, München 2020.

Ernst, Stefan, Der Arbeitgeber, die E-Mail und das Internet, NZA 2002, S. 585–591.

ders., Die Einwilligung nach der Datenschutzgrundverordnung. Anmerkungen zur Definition nach Art. 4 Nr. 11 DS-GVO, ZD 2017, S. 110–114.

Eschholz, Stefanie, Big Data-Scoring unter dem Einfluss der Datenschutz-Grundverordnung, DuD 2017, S. 180–185.

Eßer, Martin/Kramer, Philipp/von Lewinski, Kai (Hrsg.), Auernhammer, DSGVO / BDSG - Kommentar. Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze : Kommentar. 5. Aufl., Köln 2017 [zitiert als: Auernhammer (5. Aufl. 2017)/*Bearbeiter*].

dies., Auernhammer, DSGVO / BDSG - Kommentar. Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze : Kommentar. 7. Aufl., Köln 2020 [zitiert als: Auernhammer/*Bearbeiter*].

European Data Protection Board (EDPB), DRAFT Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. Adopted on 9 April 2019 2019 [zitiert als: *EDPB*, DRAFT Guidelines 2/19].

dass., Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. Version 2.0 2019, abrufbar unter: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf (letzter Abruf am: 31.03.2021 [zitiert als: *EDPB*, Guidelines 2/19].

European Data Protection Supervisor (EDPS), Opinion 7/2015 - Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability 2015, abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf (letzter Abruf am: 24.01.2020 [zitiert als: *EDPS*, Opinion 7/15].

Faas, Thomas, 70.2 Einführung und Nutzung von Informationstechnologie im Arbeitsverhältnis, in: Taeger/Pohle (Hrsg.), Computerrechts-Handbuch. Informationstechnologie in der Rechts- und Wirtschaftspraxis, München 2020.

Fischer, Peter/Hofer, Peter, Lexikon der Informatik. 15. Aufl., Berlin, Heidelberg 2011.

Fitting, Karl (Hrsg.), Betriebsverfassungsgesetz. 30. Aufl., München 2020.

Forgó, Nikolaus/Helfrich, Marcus/Schneider, Jochen (Hrsg.), Betrieblicher Datenschutz. Rechtshandbuch. 3. Aufl., München 2019.

Forst, Gerrit, Bewerberauswahl über soziale Netzwerke im Internet, NZA 2010, S. 427–433.

Franzen, Martin, Datenschutz im Unternehmen - Zwischen Persönlichkeitsschutz der Arbeitnehmer und Compliance-Anforderungen, ZfA 2012, S. 172–195.

ders., Der Vorschlag für eine EU-Datenschutz-Grundverordnung und der Arbeitnehmerdatenschutz, DuD 2012, S. 322–326.

ders., Rechtliche Rahmenbedingungen psychologischer Eignungstests, NZA 2013, S. 1–5.

ders., Datenschutz-Grundverordnung und Arbeitsrecht, EuZA 2017, S. 313–351.

Franzen, Martin/Gallner, Inken/Oetker, Hartmut (Hrsg.), Kommentar zum europäischen Arbeitsrecht. 3. Aufl., München 2020 [zitiert als: EuArbRK/*Bearbeiter*].

Freeman, Laura, People Analytics for Dummies, Toronto 2019.

Friedewald, Michael/Schiering, Ina/Martin, Nicholas, Datenschutz-Folgenabschätzung in der Praxis. Herausforderungen bei der Implementierung eines innovativen Instruments der DSGVO, DuD 2019, S. 473–477.

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

Gausling, Tina, Künstliche Intelligenz im Anwendungsbereich der Datenschutz-Grundverordnung, PinG 2019, S. 61–70.

Geiger, Jan, Teil A. VI. Bedrohung des Persönlichkeitsrechts des Arbeitnehmers, in: Weth/Herberger/Wächter/Sorge (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis. Praxishandbuch zum Arbeitnehmerdatenschutz, München 2019, Rn. 1–53 [zitiert als: WHWS/*Geiger*, Teil A. VI. Bedrohung des Persönlichkeitsrechts des Arbeitnehmers].

Geppert, Martin/Schütz, Raimund (Hrsg.), Beck'scher TKG-Kommentar. Telekommunikationsgesetz. 4. Aufl., München 2013.

Gerberding, Johannes/Wagner, Gert, Qualitätssicherung für "Predictive Analytics" durch digitale Algorithmen, ZRP 2019, S. 116–119.

Gersdorf, Hubertus/Paal, Boris P. (Hrsg.), BeckOK Informations- und Medienrecht. 31. Aufl., München 2021 [zitiert als: BeckOK InfoMedienR/*Bearbeiter*].

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

Gierschmann, Sibylle/Schlender, Katharina/Stentzel, Rainer/Veil, Winfried (Hrsg.), Kommentar Datenschutz-Grundverordnung, Köln 2018.

Gola, Peter, Die Erhebung von Bewerberdaten - ein Vergleich der geltenden Rechtslage mit (eventuellem) künftigem Recht, RDV, 2011 (2011), S. 109–117.

ders., Die Ortung externer Beschäftigter - Abwägung zwischen Überwachungsinteresse und schutzwürdigen Arbeitnehmerinteressen, ZD 2012, S. 308–311.

ders., Datenschutz am Arbeitsplatz. Handlungshilfen beim Einsatz von Intranet und Internet, E-Mail und Telefon, Video und GPS, Big Data und Social Media. 5. Aufl., Heidelberg, Hamburg 2014.

ders., Der "neue" Beschäftigtendatenschutz nach § 26 BDSG n. F., BB 2017, S. 1462–1472.

ders., Aus den aktuellen Berichten der Aufsichtsbehörden (33): Die Digitalisierung des Bewerbermanagements - Videointerviews bei der Bewerbung, RDV 2018, S. 24–28.

ders., Datenschutz-Grundverordnung. VO (EU) 2016/679 : Kommentar. 2. Aufl., München 2018.

ders., Das Internet als Quelle von Bewerberdaten. Vorgaben von DS-GVO, BDSG und UWG, NZA 2019, S. 654–658.

Gola, Peter/Heckmann, Dirk (Hrsg.), BDSG. Bundesdatenschutzgesetz. 13. Aufl., München 2019.

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

Gola, Peter/Thüsing, Gregor/Schmidt, Maximilian, Was wird aus dem Beschäftigtendatenschutz? Die DS-GVO, das DS-AnpUG und § 26 BDSG-neu, DuD 2017, S. 244–250.

Göpfert, Burkard/Dußmann, Andreas, Recruiting und Headhunting in der digitalen Arbeitswelt - Herausforderungen für die arbeitsrechtliche Praxis, NZA-Beilage 2016, S. 41–46.

Götz, Thomas, Big Data im Personalmanagement. Datenschutzrecht und betriebliche Mitbestimmung. 1. Aufl., Baden-Baden 2020.

Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin (Hrsg.), Das Recht der Europäischen Union. 40. Aufl., München 2009 [zitiert als: GHN (40. Aufl. 2009)/*Bearbeiter*].

Grafenstein, Maximilian von, Das Zweckbindungsprinzip zwischen Innovationsoffenheit und Rechtssicherheit. Zur mangelnden Differenzierung der Rechtsgüterbetroffenheit in der Datenschutzgrund-VO, DuD 2015, S. 789–795.

Gragert, Nicola, Vorlage- und Auskunftspflichten im Verfahren nach § 99 BetrVG (Anm. zu BAG, Beschl. v. 21.10.2014 - 1 ABR 10/13), ArbRAktuell 2015, S. 135.

Greenbone Networks GmbH, Sicherheitsbericht. Ungeschützte Patientendaten im IInternet, Osnabrück 2019, abrufbar unter: https://www.greenbone.net/wp-content/uploads/CyberResilienceReport_DE.pdf (letzter Abruf am: 19.09.2019).

Grimm, Detlef, Die "Rahmenbetriebsvereinbarung-DSGVO" als Mittel zur Umsetzung der neuen Datenschutzvorgaben - Teil 1. Gestaltungsgrundsätze und rechtlicher Rahmen, ArbRB 2018, S. 78–82.

ders., Die "Rahmenbetriebsvereinbarung-DSGVO" als Mittel zur Umsetzung der neuen Datenschutzvorgaben - Teil 2. Formulierungsvorschlag, ArbRB 2018, S. 122–127.

Groß, Nadja/Gressel, Jacqueline, Entpersonalisierte Arbeitsverhältnisse als rechtliche Herausforderung - Wenn Roboter zu Kollegen und Vorgesetzten werden, NZA 2016, S. 990–996.

Grothe, Martin/Gentsch, Peter, Business intelligence. Aus Informationen Wettbewerbsvorteile gewinnen, München 2000.

Hackenberg, Wolfgang, Teil 15.2 Big Data und Datenschutz, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht. Rechtsfragen des elektronischen Geschäftsverkehrs, München 2020.

Hamann, Christian, Europäische Datenschutz-Grundverordnung - neue Organisationspflichten für Unternehmen, BB 2017, S. 1090–1097.

ders., Kapitel 6: Datenschutzrecht, in: Arnold/Günther (Hrsg.), Arbeitsrecht 4.0. Praxishandbuch zum Arbeits-, IP- und Datenschutzrecht in einer digitalisierten Arbeitswelt, München 2018, Rn. 1–102.

Hanke, Moritz, Datenschutzprobleme und Gestaltungsmöglichkeiten in der Praxis, 2018, abrufbar unter: https://www.arbeitnehmerkammer.de/fileadmin/user_upload/Veranstaltungen/Veranstaltungsdokumentation/Downloads/Datenschutzrecht_20180221_Hanke.pdf (letzter Abruf am: 31.03.2020).

Hanser, Hartwig (Hrsg.), Lexikon der Neurowissenschaft. Gesamtausgabe, Heidelberg 2005.

Härting, Niko, Profiling: Vorschläge für eine intelligente Regelung. Was aus der Zweistufigkeit des Profiling für die Regelung des nicht-öffentlichen Datenschutzbereichs folgt, CR 2014, S. 528–536.

ders., Big Data und Profiling nach der DSGVO, ITRB 2016, S. 209–211.

ders., Datenschutz-Grundverordnung, Köln 2016 [zitiert als: *Härting*, DSGVO].

ders., Internetrecht. 6. Aufl., Köln 2017.

Haufe Online Redaktion, Künstliche Intelligenz im Recruiting: Das halten Bewerber davon, 07.01.2019, abrufbar unter: https://www.haufe.de/personal/hrmanagement/Kuenstliche-Intelligenz-im-Recruiting-Das-halten-Bewerber-davon_80_475156.html (letzter Abruf am: 21.01.2019).

dies., People Analytics: Wie lässt sich Big Data für HR nutzen?, 10.10.2019, abrufbar unter: https://www.haufe.de/personal/hrmanagement/People-Analytics-Wie-laesst-sich-Big-Data-fuer-HR-nutzen_80_501534.html (letzter Abruf am: 11.10.2019).

Haußmann, Katrin/Brauneisen, Kai, Bestehende IT-Betriebsvereinbarungen - welchen Renovierungsbedarf bringt das neue Datenschutzrecht?, BB 2017, S. 3065–3067.

Heckmann, Dirk (Hrsg.), juris PraxisKommentar Internetrecht. Telemediengesetz, E-Commerce, E-Government. 6. Aufl., Saarbrücken 2019.

Heckmann, Dirk/Scheurer, Martin, Kap. 9 Datenschutz, in: Heckmann (Hrsg.), juris PraxisKommentar Internetrecht. Telemediengesetz, E-Commerce, E-Government, Saarbrücken 2019 [zitiert als: jurisPK-Internetrecht/*Heckmann/Scheurer*, Kap. 9 Datenschutz].

Heidrich, Joerg/Wegener, Christoph, Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten - Problemfall Logging, MMR 2015, S. 487–493.

Heinson, Dennis/Schmidt, Bernd, IT-gestützte Compliance-Systeme und Datenschutzrecht Ein Überblick am Beispiel von OLAP und Data Mining, CR 2010, S. 540–547.

Helbing, Thomas, Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung, K&R 2015, S. 145–150.

Helfrich, Marcus, Teil IX. Kapitel 3, in: Forgó/Helfrich/Schneider (Hrsg.), Betrieblicher Datenschutz. Rechtshandbuch, München 2019.

Helfrich, Marcus/Forgó, Nikolaus/Schneider, Jochen, Teil I. Kapitel 5. Grundsätze der datenschutzrechtlichen Prüfung, in: Forgó/Helfrich/Schneider (Hrsg.), Betrieblicher Datenschutz. Rechtshandbuch, München 2019.

Herfurth, Constantin, Interessensabwägung nach Art. 6 Abs. 1 lit. f DS-GVO. Nachvollziehbare Ergebnisse anhand von 15 Kriterien mit dem sog. "3x5-Modell", ZD 2018, S. 514–520.

Hinz, Katja, 11. Arbeitsrecht, in: Kaulartz/Ammann/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, München 2020.

Hochhold, Stefanie/Rudolph, Bernd, Principal-Agent-Theorie, in: Schwaiger/Meyer (Hrsg.), Theorien und Methoden der Betriebswirtschaft. Handbuch für Wissenschaftler und Studierende, München 2011, S. 131–145.

Hoening, Claus/Esch, Martin/Wald, Andreas, Big Data, Business Intelligence und Business Analytics: Bedeutung, Nutzen und Mehrwert für die Unternehmenssteuerung, Haufe Steuer Office Gold, HI10713394.

Hoeren, Thomas, Big Data und Datenqualität - ein Blick auf die DS-GVO, ZD 2016, S. 459–463.

ders., Thesen zum Verhältnis von Big Data und Datenqualität - Erstes Raster zum Erstellen juristischer Standards, MMR 2016, S. 8–11.

Hoeren, Thomas/Niehoff, Maurice, KI und Datenschutz – Begründungserfordernisse automatisierter Entscheidungen, RW 2018, S. 47–66.

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.), Handbuch Multimedia-Recht. Rechtsfragen des elektronischen Geschäftsverkehrs. 54. Aufl., München 2020.

Hof, Hans-Joachim, 5 Datenschutz mittels IT-Sicherheit, in: Tinnefeld/Buchner/Petri/Hof (Hrsg.), Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht, Berlin, Boston 2020.

Höller, Heinz-Peter/Wedde, Peter, Die Vermessung der Belegschaft. Mining the Enterprise Social Graph, Düsseldorf 2018.

Holtel, Stefan/Hufenstuhl, Andreas/Klug, Andreas, Künstliche Intelligenz verstehen als Automation des Entscheidens. Leitfaden 2017, abrufbar unter: https://www.bitkom.org/sites/default/files/file/import/Bitkom-Leitfaden-KI-verstehen-als-Automation-des-Entscheidens-2-Mai-2017.pdf (letzter Abruf am: 31.03.2021).

Holthaus, Christian/Park, Young-kul/Stock-Homburg, Ruth, People Analytics und Datenschutz–Ein Widerspruch?, DuD 2015, S. 676–681.

Horn, Norbert (Hrsg.), Europäisches Rechtsdenken in Geschichte und Gegenwart. Festschrift für Helmut Coing zum 70. Geburtstag, München 1982 [zitiert als FS Coing 70].

Imping, Andreas, Neue Zeitrechnung im (Beschäftigten-)Datenschutz. Die Herausforderungen des neuen Datenschutzrechts an die betriebliche Praxis, CR 2017, S. 378–388.

Jäger, Wolfgang/Petry, Thorsten, Digital HR - Ein Überblick, in: Petry/Jäger (Hrsg.), Digital HR. Smarte und agile Systeme, Prozesse und Strukturen im Personalmanagement, Freiburg, München, Stuttgart 2018, S. 27–102.

Jandt, Silke, Datenschutz durch Technik in der DS-GVO, DuD, 2017 (2017), S. 562–566.

dies., Spezifischer Datenschutz für Telemedien und die DS-GVO. Zwischen Rechtsetzung und Rechtsanwendung, ZD 2018, S. 405–408.

Jentzsch, Christoph, BigData@Work. Wie "Big Data" das Personalumfeld revolutionieren wird, HR Performance 2013, S. 60–61.

ders., Nutzung von Big Data für die strategische Personalplanung. Mit Strategic Workforce Planning im Personalumfeld für die Zukunft gerüstet, HR Performance 2013, S. 48–49.

Jerchel, Kerstin/Schubert, Jens, Neustart im Datenschutz für Beschäftigte. Möglichkeit von Kollektivvereinbarungen zur Regelung des Datenschutzes nach der DS-GVO, DuD 2016, S. 782–786.

Jochmann, Walter/Belch, Theresa, Eine ernüchternde Zwischenbilanz. Selbstverständnis, Herausforderungen und Beiträge von HR im Kontext digitaler Transformation, Personalführung 2016, S. 58–63.

Kainer, Friedemann/Weber, Christian, Datenschutzrechtliche Aspekte des "Talentmanagements", BB 2017, S. 2740–2747.

Kaiser, Stephan/Kraus, Hans, Big Data im Personalmanagement. Erste Anwendungen und ein Blick in die Zukunft, zfo 2014, S. 379–385.

Kania, Thomas, Stichwort "Leitende Angestellte", in: Küttner (Hrsg.), Personalbuch 2020. Arbeitsrecht, Lohnsteuerrecht, Sozialversicherungsrecht, München 2020.

Karg, Moritz, Anonymität, Pseudonyme und Personenbezug revisited?, DuD 2015, S. 520–526.

Katko, Peter/Babaei-Beigi, Ayda, Accountability statt Einwilligung? Führt Big Data zum Paradigmenwechsel im Datenschutzrecht?, MMR 2014, S. 360–364.

Kaulartz, Markus/Ammann, Thorsten/Braegelmann, Tom (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, München 2020.

Kersting, Miriam, Moderner Beschäftigtendatenschutz nach der DS-GVO und dem BDSG-neu?, in: Buhl/Frieling/Krois/Malorny/Münder/Richter/Schmidt (Hrsg.), Der erwachte Gesetzgeber. Regulierung und Deregulierung im Arbeitsrecht : Dokumentation der 7. Assistentinnen- und Assistententagung im Arbeitsrecht vom 27.- 29.07.2017, Baden-Baden 2017, S. 55–76.

Kiel, Heinrich/Lunk, Stefan/Oetker, Hartmut/Richardi, Reinhard/Wlotzke, Otfried/Wißmann, Hellmut (Hrsg.), Münchener Handbuch zum Arbeitsrecht. 4. Aufl., München 2019.

Kienbaum Institut @ ISM, Digitalisierung@HR - Strukturen, Prozesse & Kompetenzen der Zukunft 2016, abrufbar unter: https://www.yumpu.com/de/document/read/56587003/digitalisierunghr-strukturen-prozesse-kompetenzen-der-zukunft (letzter Abruf am: 31.03.2021).

Kirkland, Frazar, Cyclopaedia of Commercial and Business Anecdotes. comprising interesting reminiscences and facts, remarkable traits and humors, and notable sayings, dealings, experiences and witticisms of merchants, traders, bankers, mercantile celebrities, millionnaires, bargain makers, etc., etc. in all ages and countries., London, New York 1868.

Kittner, Thomas, Big Datenschutz bei Big Data, 07.02.2018, abrufbar unter: https://www.haufe.de/personal/arbeitsrecht/datenschutz-zulaessigkeit-von-big-data-analysen_76_441566.html.

Klar, Manuel, Künstliche Intelligenz und Big Data - algorithmenbasierte Systeme und Datenschutz im Geschäft mit Kunden, BB 2019, S. 2243–2252.

Kleb, Ralf Hendrik, Big Data & Workforce Analytics, Haufe Steuer Office Gold 2017, HI7351934.

Klein, David, Konzerninternes Outsourcing von E-Mail und anderen Unternehmenskommunikationsdiensten. Plädoyer für einen einheitlichen europarechtskonformen Schutz des Fernmeldegeheimnisses und personenbezogener Daten, CR 2016, S. 606–613.

Klinkhammer, Patrick/Peters, Verena, Fortbildungsvereinbarungen - eine nützliche Investition mit Risiken, ArbRAktuell 2015, S. 369–372.

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

Knapp, Enrico, Delve Analytics - Ich weiß wer du bist, weißt du's?, 12.11.2015, abrufbar unter: https://www.brandmysharepoint.de/delve-analytics-ich-weiss-wer-du-bist-weisst-dus/ (letzter Abruf am: 31.03.2020).

Knopp, Michael, Pseudonym - Grauzone zwischen Anonymisierung und Personenbezug, DuD 2015, S. 527–530.

ders., Stand der Technik. Ein alter Hut oder eine neue Größe?, DuD 2017, S. 663–666.

Knorr, Michael, Datenschutzkonforme Protokollierung, DuD 2006, S. 268–269.

Koch, Ulrich, Sprecherausschüsse, in: Schaub/Koch (Hrsg.), Arbeitsrecht von A-Z. Verständlich, übersichtlich, klar, München 2021.

Köhntopp, Marit/Köhntopp, Kristian, Datenspuren im Internet, CR 2000, S. 248–257.

Kömpf, Nicola/Kunz, Holger, Kontrolle der Nutzung von Internet und E-Mail am Arbeitsplatz in Frankreich und in Deutschland, NZA 2007, S. 1341–1346.

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Diensten am Arbeitsplatz 2016.

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Kurzpapier Nr. 18 - Risiko für die Rechte und Freiheiten natürlicher Personen 2018, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf (letzter Abruf am: 31.03.2021 [zitiert als: *DSK*, Kurzpapier Nr. 18].

dies., Positionsbestimmung zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018 2018, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/ah/201804_ah_positionsbestimmung_tmg.pdf (letzter Abruf am: 31.03.2021 [zitiert als: *DSK*, Positionsbestimmung TMG 2018].

dies., Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO 2019, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/12/20191209_Erfahrungsbericht-zur-Anwendung-der-DS-GVO.pdf (letzter Abruf am: 31.03.2021 [zitiert als: *DSK*, Erfahrungsbericht 2019].

Kontio, Carina, Wie Bewerber die Robo-Recruiter überlisten können, 04.09.2018, abrufbar unter: https://www.handelsblatt.com/unternehmen/beruf-und-buero/the_shift/jobsuche-wie-bewerber-die-robo-recruiter-ueberlisten-koennen/22991974.html?ticket=ST-3589804-FXMKTFgbNgF1zeM14jmT-ap2 (letzter Abruf am: 06.03.2020).

Kopp, Reinhold/Sokoll, Karen, Wearables am Arbeitsplatz - Einfallstore für Alltagsüberwachung?, NZA 2015, S. 1352–1359.

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

Körner, Marita, Die Reform des EU-Datenschutzes: Der Entwurf einer EU-Datenschutz-Grundverordnung (DS-GVO) - Teil II, ZESAR 2013, S. 153–159.

dies., Die Datenschutz-Grundverordnung und nationale Regelungsmöglichkeiten für Beschäftigtendatenschutz, NZA 2016, S. 1383–1386.

dies., Wirksamer Beschäftigtendatenschutz im Lichte der Europäischen Datenschutz-Grundverordnung (DS-GVO), Frankfurt am Main 2017.

dies., Beschäftigtendatenschutz in Betriebsvereinbarungen unter der Geltung der DS-GVO, NZA 2019, S. 1389–1395.

dies., 2.4 Nachvollziehbarkeit von KI-basierten Entscheidungen, in: Kaulartz/Ammann/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, München 2020.

Kort, Michael, Datenschutzrechtliche und betriebsverfassungsrechtliche Fragen bei IT-Sicherheitsmaßnahmen, NZA 2011, S. 1319–1324.

ders., Soziale Netzwerke und Beschäftigtendatenschutz, DuD 2012, S. 722–728.

ders., Arbeitnehmerdatenschutz gemäß der EU-Datenschutz-Grundverordnung, DB 2016, S. 711–716.

ders., Eignungsdiagnose von Bewerbern unter der Datenschutz-Grundverordnung, NZA-Beilage 2016, S. 62–71.

ders., Der Beschäftigtendatenschutz gem. § 26 BDSG-neu. Ist die Ausfüllung der Öffnungsklausel des Art. 88 DS-GVO geglückt?, ZD 2017, S. 319–323.

ders., Die Bedeutung der neueren arbeitsrechtlichen Rechtsprechung für das Verständnis des neuen Beschäftigtendatenschutzes, NZA 2018, S. 1097–1105.

ders., Neuer Beschäftigtendatenschutz und Industrie 4.0, RdA 2018, S. 24–33.

Kramer, Bernd, "Der Algorithmus diskriminiert nicht", 09.02.2018, abrufbar unter: https://www.zeit.de/arbeit/2018-01/roboter-recruiting-bewerbungsgespraech-computer-tim-weitzel-wirtschaftsinformatiker/komplettansicht?print (letzter Abruf am: 21.01.2019).

Kramer, Stefan, Folgen der EGMR-Rechtsprechung für eine IT-Kontrolle bei Privatnutzungsverbot, NZA 2018, S. 637–640.

Kraus, Christopher, Digitalisierung der Arbeitswelt - das Ende der Low Performer?, DB 2018, S. 701–705.

Krause, Rüdiger, Forschungsbericht 482 - Digitalisierung und Beschäftigtendatenschutz. Expertise 2017, abrufbar unter: https://www.bmas.de/SharedDocs/Downloads/DE/PDF-Publikationen/Forschungsberichte/fb482-digitalisierung-und-beschaeftigtendatenschutz.pdf?__blob=publicationFile&v=1 (letzter Abruf am: 24.01.2020 [zitiert als: *Krause*, Forschungsbericht 482].

Kreitner, Jochen/Seidel, Ralf/Voelzke, Thomas, Stichwort "Massenentlassung", in: Küttner (Hrsg.), Personalbuch 2020. Arbeitsrecht, Lohnsteuerrecht, Sozialversicherungsrecht, München 2020.

Kreitner, Jochen/Weil, Barbara/Schlegel, Rainer, Stichwort "Personalinformationssystem", in: Küttner (Hrsg.), Personalbuch 2020. Arbeitsrecht, Lohnsteuerrecht, Sozialversicherungsrecht, München 2020.

Kremer, Michaela/Meyer-van Raay, Oliver, Der Zugriff auf Mitarbeiter-Mails durch den Arbeitgeber und dessen Outsourcing-Provider, ITRB 2010, S. 133–138.

Kremer, Sascha, § 2 Zulässigkeit der Verarbeitung, in: Laue/Kremer (Hrsg.), Das neue Datenschutzrecht in der betrieblichen Praxis, Baden-Baden 2019.

Krügel, Tina, Das personenbezogene Datum nach der DS-GVO, ZD 2017, S. 455–460.

Kühling, Jürgen, Neues Bundesdatenschutzgesetz - Anpassungsbedarf bei Unternehmen, NJW 2017, S. 1985–1990.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung/BDSG. Kommentar. 3. Aufl., München 2020.

Kühling, Jürgen/Klar, Manuel/Sackmann, Florian, Datenschutzrecht. 4. Aufl., Heidelberg 2018.

Kühling, Jürgen/Martini, Mario, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW, S. 448–454.

Kühling, Jürgen/Martini, Mario/Heberlein, Johanna/Kühl, Benjamin/Nink, David/Weinzierl, Quirin/Wenzel, Michael, Die Datenschutz-Grundverordnung und das nationale Recht. Erste Überlegungen zum innerstaatlichen Regelungsbedarf, Münster 2016.

Küttner, Wolfdieter (Hrsg.), Personalbuch 2020. Arbeitsrecht, Lohnsteuerrecht, Sozialversicherungsrecht. 27. Aufl., München 2020.

Lambrich, Thomas/Cahlik, Nina, Austausch von Arbeitnehmerdaten in multinationalen Konzernen - Datenschutz- und betriebsverfassungsrechtliche Rahmenbedingungen -, RDV 2002, S. 287–299.

Laue, Philip/Kremer, Sascha (Hrsg.), Das neue Datenschutzrecht in der betrieblichen Praxis. 2. Aufl., Baden-Baden 2019.

Lensdorf, Lars/Born, Walter, Die Nutzung und Kontrolle des dientlichen E-Mail-Accounts und Internetzugangs, CR 2013, S. 30–37.

Löwisch, Manfred, Fernmeldegeheimnis und Datenschutz bei der Mitarbeiterkontrolle, DB 2009, S. 2782–2787.

Luber, Stefan/Litzel, Nico, Was ist Hadoop?, 01.09.2016, abrufbar unter: https://www.bigdata-insider.de/was-ist-hadoop-a-587448/ (letzter Abruf am: 10.10.2019).

dies., Was ist R?, 27.04.2018, abrufbar unter: https://www.bigdata-insider.de/was-ist-r-a-707966/ (letzter Abruf am: 10.10.2019).

Lücke, Oliver, Die Betriebsverfassung in Zeiten der DS-GVO. "Bermuda-Dreieck" zwischen Arbeitgeber, Betriebsräten und Datenschutzbeauftragten!?, NZA 2019, S. 658–670.

Luhn, Hans Peter, A Business Intelligence System, IBM Journal 1958, S. 314–319.

Lunk, Stefan, Prozessuale Verwertungsverbote im Arbeitsrecht, NZA 2009, S. 457–464.

ders., § 340 Die Mitbestimmung bei der Einstellung, in: Kiel/Lunk/Oetker/Richardi/Wlotzke/Wißmann (Hrsg.), Münchener Handbuch zum Arbeitsrecht, München 2019 [zitiert als: MHdB-ArbR/*Lunk*, § 340 Die Mitbestimmung bei der Einstellung].

Lützeler, Martin/Kopp, Désirée, HR mit System: Bewerbermanagement-Tools, ArbRAktuell 2015, S. 491–494.

Lyman, Peter/Varian, Hal R., Reprint: How Much Information?, The Journal of Electronic Publishing 2000, DOI: 10.3998/3336451.0006.204.

Maamar, Niklas, Social Scoring. Eine europäische Perspektive auf Verbraucher-Scores zwischen Big Data und Big Brother, CR 2018, S. 820–828.

Maier, Natalie, Der Beschäftigtendatenschutz nach der Datenschutz-Grundverordnung, DuD 2017, S. 169–174.

Maier, Natalie/Ossoinig, Verena, Rechtsfragen und praktische Tipps bei der Ortung durch Smartphone-Apps, VuR 2015, S. 330–337.

Mankiw, Nicholas Gregory/Taylor, Mark P., Grundzüge der Volkswirtschaftslehre. 6. Aufl., Stuttgart 2016.

Marnau, Richard, Protokollierung im Windows Betriebssystem, DuD 2006, S. 288–291.

Martini, Mario, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, S. 1017–1025.

Martini, Mario/Botta, Jonas, Iron Man am Arbeitsplatz? - Exoskelette zwischen Effizienzstreben, Daten- und Gesundheitsschutz, NZA 2018, S. 625–637.

Martini, Mario/Nink, David, Wenn Maschinen entscheiden… Persönlichkeitsschutz in vollautomatisierten Verwaltungsverfahren, NVwZ 2017, S. 681–682.

dies., Wenn Maschinen entscheiden… - vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz, NVwZ-Extra 2017, S. 1–14.

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

ders., Führung und Mitarbeiterkontrolle nach neuem Datenschutzrecht, NZA-Beilage 2018, S. 115–124.

McCarthy, John/Minsky, Marvin L./Rochester, Nathaniel/Shannon, Claude, A Proposal for the Dartmouthg Summer Research Project on Artificial Intelligence 1955, abrufbar unter: https://aaai.org/ojs/index.php/aimagazine/article/view/1904/1802 (letzter Abruf am: 02.05.2018).

Mengel, Anja, Kontrolle der E-mail und Internetkommunikation am Arbeitsplatz. Wege durch einen juristischen Irrgarten, BB 2004, S. 2014–2021.

Menzel, Hans-Joachim, Datenschutzrechtliche Einwilligungen. Plädoyer für eine Rückkehr zur Selbstbestimmung, DuD 2008, S. 400–408.

Michl, Walther, Das Verhältnis zwischen Art. 7 und Art. 8 GRCh - zur Bestimmung der Grundlage des Datenschutzgrundrechts im EU-Recht, DuD 2017, S. 349–353.

Micklitz, Hans-W./Rott, Peter, H. V. Verbraucherschutz, in: Dauses/Ludwigs (Hrsg.), Handbuch des EU-Wirtschaftsrechts, München 2020.

Möckel, Theresa, Bluetooth: Wie hoch ist die Reichweite?, 2019, abrufbar unter: https://www.heise.de/tipps-tricks/Bluetooth-Wie-hoch-ist-die-Reichweite-4523661.html (letzter Abruf am: 28.05.2020).

Moll, Wilhelm/Roebers, Dorothea, Beteiligungsrechte des Betriebsrats bei Personalumfragen im Unternehmen, DB 2011, S. 1862–1865.

Monreal, Manfred, Weiterverarbeitung nach einer Zweckänderung in der DS-GVO. Chancen nicht nur für das europäische Verständnis des Zweckbindungsgrundsatzes, ZD 2016, S. 507–512.

Moos, Flemming/Schefzig, Jens/Arning, Marian (Hrsg.), Die neue Datenschutz-Grundverordnung. Mit Bundesdatenschutzgesetz 2018, Berlin 2018.

Mühlbauer, Daniel/Huff, Julian/Süß, Julian, People Analytics und Arbeit 4.0, in: Werther/Bruckner (Hrsg.), Arbeit 4.0 aktiv gestalten. Die Zukunft der Arbeit zwischen Agilität, People Analytics und Digitalisierung, Berlin, Heidelberg 2018.

Mülder, Wilhelm, Überblick zu Potentialen neuer Technologien für HR, in: Petry/Jäger (Hrsg.), Digital HR. Smarte und agile Systeme, Prozesse und Strukturen im Personalmanagement, Freiburg, München, Stuttgart 2018, S. 103–124.

Müller, Falk, Beschäftigtendatenschutz im Arbeitsrecht: dienstliche und private E-Mail-Nutzung, öAT 2019, S. 1–4.

Müller, Johannes Karl Martin, § 8 V. Auskunfteien, Bonitätsauskünfte, Scoring, in: Roßnagel (Hrsg.), Das neue Datenschutzrecht. Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze, Baden-Baden 2018.

Müller-Broich, Jan D. (Hrsg.), Telemediengesetz, Baden-Baden 2012.

Müller-Glöge, Rudi/Preis, Ulrich/Schmidt, Ingrid (Hrsg.), Erfurter Kommentar zum Arbeitsrecht. 2021. Aufl., München 2021 [zitiert als: ErfK/*Bearbeiter*].

Nebel, Maxi, § 3 III. Erlaubnis zur Datenverarbeitung, in: Roßnagel (Hrsg.), Das neue Datenschutzrecht. Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze, Baden-Baden 2018, Rn. 94–137.

dies., Big Data und Datenschutz in der Arbeitswelt, ZD 2018, S. 520–524.

Neufeld, Tobias/Glugla, Catharina, Big Data & künstliche Intelligenz in der Personalrekrutierung, MuT 2019, S. 40–41.

Niklas, Thomas/Thurn, Lukas, Arbeitswelt 4.0 - Big Data im Betrieb, BB 2017, S. 1589–1596.

Oberthür, Nathalie, A. II. Arten von Betriebsvereinbarungen, in: Oberthür/Seitz (Hrsg.), Betriebsvereinbarungen, München 2016.

dies., § 335 Zustimmung zu Personalfragebögen, in: Kiel/Lunk/Oetker/Richardi/Wlotzke/Wißmann (Hrsg.), Münchener Handbuch zum Arbeitsrecht, München 2019 [zitiert als: MHdB-ArbR/*Oberthür*, § 335 Zustimmung zu Personalfragebögen].

dies., § 336 Zustimmung zu allgemeinen Beurteilungsgrundsätzen, in: Kiel/Lunk/Oetker/Richardi/Wlotzke/Wißmann (Hrsg.), Münchener Handbuch zum Arbeitsrecht, München 2019 [zitiert als: MHdB-ArbR/*Oberthür*, § 336 Zustimmung zu allgemeinen Beurteilungsgrundsätzen].

dies., § 337 Mitbestimmung bei Auswahlrichtlinien, in: Kiel/Lunk/Oetker/Richardi/Wlotzke/Wißmann (Hrsg.), Münchener Handbuch zum Arbeitsrecht, München 2019 [zitiert als: MHdB-ArbR/*Oberthür*, § 337 Mitbestimmung bei Auswahlrichtlinien].

Oberthür, Nathalie/Seitz, Stefan (Hrsg.), Betriebsvereinbarungen. 2. Aufl., München 2016.

O'Neil, Cathy, Weapons of math destruction. How big data increases inequality and threatens democracy, London 2018.

Paal, Boris P./Pauly, Daniel A./Ernst, Stefan/Frenzel, Eike Michael/Gräber, Tobias/Hennemann, Moritz/Körffer, Barbara/Martini, Mario/Nolden, Christine (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz. 3. Aufl., München 2021 [zitiert als: Paal/Pauly/*Bearbeiter*].

Panzer-Heemeier, Andrea, B. V. Betriebsvereinbarungen zur Nutzung technischer Einrichtungen, in: Oberthür/Seitz (Hrsg.), Betriebsvereinbarungen, München 2016.

Peck, Don, They're Watching You at Work. What happens when Big Data meets human resources? The emerging practive of "people analytics" is already transforming how employers hire, fire and promote., The Atlantic (Dezember 2013).

Peters, Falk, Personalinformationssysteme - Informationelle Selbstbestimmung oder kollektiver Arbeitnehmerdatenschutz?, DSWR 1985, S. 186–191.

Petry, Thorsten/Jäger, Wolfgang (Hrsg.), Digital HR. Smarte und agile Systeme, Prozesse und Strukturen im Personalmanagement, Freiburg, München, Stuttgart 2018.

Pielow, Johann-Christian (Hrsg.), Beck'scher Online-Kommentar Gewerbeordnung, München 2020.

Piltz, Carlo, Die Datenschutz-Grundverordnung. Teil 2: Rechte der Betroffenen und korrespondierende Pflichten des Verantwortlichen, K&R 2016, S. 629–636.

Plath, Kai-Uwe (Hrsg.), DSGVO/BDSG. Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen von TMG und TKG. 3. Aufl., Köln 2018 [zitiert als: Plath/*Bearbeiter*].

Poeche, Sabine, Stichwort "Fortbildung", in: Küttner (Hrsg.), Personalbuch 2020. Arbeitsrecht, Lohnsteuerrecht, Sozialversicherungsrecht, München 2020.

dies., Stichwort "Rückzahlungsklausel", in: Küttner (Hrsg.), Personalbuch 2020. Arbeitsrecht, Lohnsteuerrecht, Sozialversicherungsrecht, München 2020.

dies., Stichwort "Versetzung", in: Küttner (Hrsg.), Personalbuch 2020. Arbeitsrecht, Lohnsteuerrecht, Sozialversicherungsrecht, München 2020.

Pötters, Stephan, Primärrechtliche Vorgaben für eine Reform des Datenschutzrechts, RDV 2015, S. 10–16.

Putschli, Clemens, Wearables und Datenschutz. Datenschutz bei der Entwicklung der PARADISE Wearables, DuD 2017, S. 721–723.

Raif, Alexander/Swidersky, Manuel, Arbeit 4.0 - Typische Fehler in der digitalen Arbeitswelt vermeiden, GWR 2017, S. 351–354.

Redmond, Tony, Delve Analytics lets Office 365 users track (and maybe change) bad email habits, 02.03.2016, abrufbar unter: https://www.itprotoday.com/print/79221 (letzter Abruf am: 29.01.2019).

Reibach, Boris, Die Regulierung von Algorithmen unter der DS-GVO, RDV 2018, S. 198–201.

Reichold, Hermann, § 96 Datenschutz im Arbeitsverhältnis, in: Kiel/Lunk/Oetker/Richardi/Wlotzke/Wißmann (Hrsg.), Münchener Handbuch zum Arbeitsrecht, München 2019 [zitiert als: MHdB-ArbR/*Reichold*, § 96 Datenschutz im Arbeitsverhältnis].

Reindl, Cornelia Ulrike/Krügl, Stefanie, People Analytics: Big Data im Personalwesen, 2016, abrufbar unter: https://t3n.de/magazin/people-analytics-big-data-personalwesen-239328/ (letzter Abruf am: 26.09.2019).

dies., People Analytics in der Praxis. Mit Datenanalyse zu besseren Entscheidungen im Personalmanagement, Freiburg, München, Stuttgart 2017.

Reinsel, David/Gantz, John/Rydning, John, Data Age 2025: The Evolution of Data to Life-Critical. Don't Focus on Big Data; Focus on the Data That's Big 2017, abrufbar unter: https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf (letzter Abruf am: 24.04.2018).

Richardi, Reinhard (Hrsg.), Betriebsverfassungsgesetz. Mit Wahlordnung : Kommentar. 16. Aufl. [zitiert als: Richardi/*Bearbeiter*].

Richter, Alexander, Anmerkung zu EuGH, Urt. v. 19.10.2016 - C-582/14 - Speicherung von IP-Adressen, EuZW 2016, S. 909–914.

Richter, Philipp, Datenschutz zwecklos? - Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO, DuD 2015, S. 735–740.

ders., Big Data, Statistik und die Datenschutz-Grundverordnung, DuD 2016, S. 581–586.

Rolfs, Christian/Giesen, Richard/Kreikebohm, Ralf/Meßling, Miriam/Udsching, Peter (Hrsg.), BeckOK Arbeitsrecht. 59. Aufl. 2021 [zitiert als: BeckOK ArbR/*Bearbeiter*].

Roßnagel, Alexander, Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR 2005, S. 71–75.

ders., Datenschutzgesetzgebung für öffentliche Interessen und den Beschäftigungskontext, DuD 2017, S. 290–294.

ders., § 1 II. Inhalte der Datenschutz-Grundverordnung, in: Roßnagel (Hrsg.), Das neue Datenschutzrecht. Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze, Baden-Baden 2018.

ders., Das neue Datenschutzrecht. Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze. 1. Aufl., Baden-Baden 2018.

ders., Pseudonymisierung personenbezogener Daten. Ein zentrales Instrument im Datenschutz nach der DS-GVO, ZD 2018, S. 243–247.

Roßnagel, Alexander/Abel, Ralf-Bernd (Hrsg.), Handbuch Datenschutzrecht. Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003.

Roßnagel, Alexander/Geminn, Christian L./Jandt, Silke/Richter, Philipp, Datenschutzrecht 2016 - "smart" genug für die Zukunft? Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts, Kassel 2016.

Roßnagel, Alexander/Jandt, Silke/Skistims, Hendrik/Zirfas, Julia (Hrsg.), Datenschutz bei Wearable Computing. Eine juristische Analyse am Beispiel von Schutzanzügen, Wiesbaden 2012.

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

Roßnagel, Alexander/Pfitzmann, Andreas/Garstka, Hansjürgen, Modernisierung des Datenschutzrechts, Berlin 2001.

Roßnagel, Alexander/Richter, Philipp/Nebel, Maxi, Besserer Internetdatenschutz für Europa. Vorschläge zur Spezifizierung der DSGVO, ZD 2013, S. 103–108.

Ruchhöft, Matthias, Die Vermessung sozialer Beziehungen. Office Graph, CuA 2017, S. 8–15.

Rudel, Steffi, People Analytics aus drei Blickwinkeln, Personalmagazin 2019, S. 76–78.

Rudkowski, Lena, "Predictive policing" am Arbeitsplatz, NZA 2019, S. 72–77.

Rüpke, Giselher, § 10. Betroffene. Personenbezogene Informationen, in: Rüpke/von Lewinski/Eckhardt (Hrsg.), Datenschutzrecht. Grundlagen und europarechtliche Neugestaltung, München 2018.

ders., § 12. Rechtsgrundlagen der Verarbeitung, in: Rüpke/von Lewinski/Eckhardt (Hrsg.), Datenschutzrecht. Grundlagen und europarechtliche Neugestaltung, München 2018.

Rüpke, Giselher/von Lewinski, Kai/Eckhardt, Jens (Hrsg.), Datenschutzrecht. Grundlagen und europarechtliche Neugestaltung, München 2018.

Salamon, Erwin, § 325 Mitbestimmung bei der technischen Überwachung, in: Kiel/Lunk/Oetker/Richardi/Wlotzke/Wißmann (Hrsg.), Münchener Handbuch zum Arbeitsrecht, München 2019 [zitiert als: MHdB-ArbR/*Salamon*, § 325 Mitbestimmung bei der technischen Überwachung].

Sander, Charlotte/Schumacher, Pascal/Kühne, Roland, Weitergabe von Arbeitnehmerdaten in Unternehmenstransaktionen. Datenschutzrechtliche Grenzen nach dem BDSG und der DS-GVO, ZD 2017, S. 105–110.

Sarre, Frank, § 1 Erstellung und Pflege von Software, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, München 2019 [zitiert als: HdbIT-DSR/*Sarre*, § 1 Erstellung und Pflege von Software].

Sarunski, Maik, Big Data - Ende der Anonymität? Fragen aus Sicht der Datenschutzaufsichtsbehörde Mecklenburg-Vorpommern, DuD 2016, S. 424–428.

Schael, Christopher, Künstliche Intelligenz in der modernen Gesellschaft. Bedeutung der "künstlichen Intelligenz" für die Gesellschaft, DuD 2018, S. 547–551.

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

ders., C.II. Anwendungsbereich der DS-GVO, in: Schantz/Wolff (Hrsg.), Das neue Datenschutzrecht. Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, München 2017.

ders., D. V. Verbot automatisierter Einzelfallentscheidungen und Profiling, in: Schantz/Wolff (Hrsg.), Das neue Datenschutzrecht. Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, München 2017, Rn. 727–753.

Schantz, Peter/Wolff, Heinrich Amadeus (Hrsg.), Das neue Datenschutzrecht. Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, München 2017.

Schaub, Günter/Koch, Ulrich (Hrsg.), Arbeitsrecht von A-Z. Verständlich, übersichtlich, klar. 25. Aufl., München 2021.

Schmidt, Kristina, Stichwort "Interessensausgleich", in: Küttner (Hrsg.), Personalbuch 2020. Arbeitsrecht, Lohnsteuerrecht, Sozialversicherungsrecht, München 2020.

Schmitz, Alja, Interessenausgleich im Beschäftigtendatenschutz. Mit besonderem Blick auf die Zulässigkeit von Internetrecherchen und Kontrollen der Internet- und E-Mail-Nutzung durch den Arbeitgeber, Baden-Baden 2016.

Schulz, Sebastian, Datenverarbeitungen im Auskunfteienwesen nach neuem Datenschutzrecht. Bringt § 31 BDSG-neu mehr Klarheit?, zfm 2017, S. 91–96.

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

Schürmann, Kathrin, Auswertung von Mitarbeiterdaten - (Any)/(No)thing possible?, in: Taeger (Hrsg.), Smart world - smart law? Weltweite Netze mit regionaler Regulierung, Edewecht 2016, S. 501–517.

Schwaiger, Manfred/Meyer, Anton (Hrsg.), Theorien und Methoden der Betriebswirtschaft. Handbuch für Wissenschaftler und Studierende, München 2011.

Schwartmann, Rolf/Jaspers, Andreas/Thüsing, Gregor/Kugelmann, Dieter (Hrsg.), DSGVO/BDSG. Datenschutzgrundverordnung, Bundesdatenschutzgesetz, Heidelberg 2018 [zitiert als: HK DSGVO/BDSG (2018)/*Bearbeiter*].

dies., DSGVO/BDSG. Datenschutzgrundverordnung, Bundesdatenschutzgesetz. 2. Aufl., Heidelberg 2020 [zitiert als: HK DSGVO/BDSG/*Bearbeiter*].

Schwartmann, Rolf/Weiß, Steffen, Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für die Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017. Leitlinien für die rechtssichere Nutzung von Pseudonymisierungslösungen unter Berücksichtigung der Datenschutz-Grundverordnung, Bonn 2017 [zitiert als: *Schwartmann/Weiß*, Whitepaper zur Pseudonymisierung].

Schwarz, Lea-Christina, Datenschutzrechtliche Zulässigkeit des Pre-Employment Screening - Rechtliche Grundlagen und Einschränkungen der Bewerberprüfung durch Arbeitgeber, ZD 2018, S. 353–356.

Seeger, Martin, Praxis der UNIX-Systemprotokollierung. Stärken und Schwächen der aktuellen Implementierung, DuD 2006, S. 285–287.

Seifert, Achim, Veränderungen der Regelungstechniken im Arbeitsrecht der EU - Einige Überlegungen zum aktuellen Zustand des europäischen Arbeitsrechts, EuZA 2018, S. 51–64.

Simitis, Spiros, Datenschutz: Voraussetzung oder Ende der Kommunikation?, in: Horn (Hrsg.), Europäisches Rechtsdenken in Geschichte und Gegenwart. Festschrift für Helmut Coing zum 70. Geburtstag, München 1982, S. 495–520 [zitiert als: *Simitis*, in: FS Coing 70/].

ders., Bundesdatenschutzgesetz. 8. Aufl., Baden-Baden 2014.

Simitis, Spiros/Hornung, Gerrit/Spiecker, Indra (Hrsg.), Datenschutzrecht. DSGVO mit BDSG, Baden-Baden 2019.

Skistims, Hendrik, 8.2 Rechtsgrundlagen für datenverarbeitende KI, in: Kaulartz/Ammann/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, München 2020.

Sliwka, Disk/Biemann, Torsten, Evidenzbasiertes Personalmanagement statt Best Practice, Human Resources Manager 2011, S. 76–79.

Sommer, Katrin, Personalinformationssysteme im radikalen Wandel. Success factors von SAP - das schwarze Mitarbeiterdatenloch, CuA 2014, S. 4.

dies., Herausforderung Workday, CuA 2017, S. 8–13.

Sörup, Thorsten/Marquardt, Sabrina, Auswirkungen der EU-DSGVO auf die Datenverarbeitung im Beschäftigtenkontext, ArbRAktuell 2016, S. 103–106.

Spelge, Karin, Der Beschäftigtendatenschutz nach Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO), DuD 2016, S. 775–781.

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

Spindler, Gerald/Schuster, Fabian (Hrsg.), Recht der elektronischen Medien. 4. Aufl., München 2019.

Staab, Philipp/Nachtwey, Oliver, Die Digitalisierung der Dienstleistungsarbeit, APuZ 2016, S. 24–31.

Stadler, Hubert, Die Mitbestimmung des Betriebsrats nach dem neuen Betriebsverfassungsgesetz in Fragen der Leistungsentlohnung, BB 1972, S. 800–804.

Steidle, Roland, Datenschutz bei der Nutzung von Location Based Services im Unternehmen, MMR 2009, S. 167–171.

Stiemerling, Oliver, 2.1 Technische Grundlagen, in: Kaulartz/Ammann/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, München 2020.

Ströbel, Lukas/Böhm, Wolf-Tassilo/Breunig, Christina/Wybitul, Tim, Beschäftigtendatenschutz und Compliance: Compliance-Kontrollen und interne Ermittlungen nach der EU-Datenschutz-Grundverordnung und dem neuen Bundesdatenschutzgesetz, CCZ 2018, S. 14–21.

Strohmeyer, Stefan, Informationssysteme im Personalmanagement, Wiesbaden 2008.

Stück, Volker, EGMR: Arbeitgeber können E-Mails der Arbeitnehmer bei Verbot der Privatnutzung überwachen. Anmerkung zum EGMR-Urteil vom 12.01.2016 - 61496/08 - Barbulescu/Rumänien, CCZ 2016, 285-287.

Sydow, Gernot (Hrsg.), Europäische Datenschutzgrundverordnung. Handkommentar. 2. Aufl., Baden-Baden, Wien, Zürich 2018 [zitiert als: Sydow/*Bearbeiter*].

Taeger, Jürgen, Scoring in Deutschland nach der EU-Datenschutzgrundverordnung, ZRP 2016, S. 72–75.

ders., Smart world - smart law? Weltweite Netze mit regionaler Regulierung, Edewecht 2016.

ders., Verbot des Profiling nach Art. 22 DS-GVO und die Regulierung des Scoring ab Mai 2018, RDV 2017, S. 3–9.

Taeger, Jürgen/Gabel, Detlev (Hrsg.), DSGVO - BDSG. Kommentar. 3. Aufl., Frankfurt am Main 2019.

Taeger, Jürgen/Pohle, Jan (Hrsg.), Computerrechts-Handbuch. Informationstechnologie in der Rechts- und Wirtschaftspraxis. 35. Aufl., München 2020.

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

TeleTrusT - Bundesverband IT-Sicherheit e.V., IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum "Stand der Technik" technischer und organisatorischer Maßnahmen, Berlin 2020, abrufbar unter: https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/2020-01_TeleTrusT_Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DEU.pdf (letzter Abruf am: 26.03.2020).

Thiel, Michael, Werkzeugkiste - 24. Soziale Netzwerkanalyse, Organisationsentwicklung 2010, S. 78–85.

Thüsing, Gregor, Arbeitnehmerdatenschutz als Aufgabe von Gesetzgebung und Rechtsprechung, RDV 2009, S. 1–6.

ders., § 3. Zum System des Beschäftigtendatenschutzes, in: Thüsing (Hrsg.), Beschäftigtendatenschutz und Compliance. Effektive Compliance im Spannungsfeld von BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung, München 2021.

ders., Beschäftigtendatenschutz und Compliance. Effektive Compliance im Spannungsfeld von BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung. 3. Aufl., München 2021.

Thüsing, Gregor/Traut, Johannes, § 10. Überwachung von Telefonverbindungsdaten, in: Thüsing (Hrsg.), Beschäftigtendatenschutz und Compliance. Effektive Compliance im Spannungsfeld von BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung, München 2021.

dies., § 9. Speicherung und Sichtung von E-Mails und E-Mail-Logfiles, in: Thüsing (Hrsg.), Beschäftigtendatenschutz und Compliance. Effektive Compliance im Spannungsfeld von BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung, München 2021.

Thüsing, Gregor/Wurth, Gilbert (Hrsg.), Social Media im Betrieb. Arbeitsrecht und Compliance. 2. Aufl., München 2020.

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

Tinnefeld, Marie-Theres/Buchner, Benedikt/Petri, Thomas/Hof, Hans-Joachim (Hrsg.), Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht. 7. Aufl., Berlin, Boston 2020.

Tinnefeld, Marie-Theres/Viethen, Hans Peter, Arbeitnehmerdatenschutz und Internet-Ökonomie - Zu einem Gesetz über Information und Kommunikation im Arbeitsverhältnis, NZA 2000, S. 977–983.

Traut, Johannes, Maßgenscheiderte Lösungen durch Kollektivvereinbarungen? Möglichkeiten und Risiken des Art. 88 Abs. 1 DS-GVO, RDV 2016, S. 312–319.

ders., § 7. Überwachung der Nutzung von Internet und Social Media - Datenschutzrechtliche Grenzen, in: Thüsing/Wurth (Hrsg.), Social Media im Betrieb. Arbeitsrecht und Compliance, München 2020.

Turing, Alan M., Computing Machinery and Intelligence, Mind 1950, S. 433–460.

Universität Mannheim, Presseinformation 46/2016: Ausbildung zum Datenspezialisten: Neuer Masterstudiengang in Data Science startet im Frühjahr 2017, Mannheim 2016 [zitiert als: *Universität Mannheim*, Presseinformation 46/2016].

Veil, Winfried, DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip - Eine erste Bestandsaufnahme, ZD 2015, S. 347–353.

ders., Accountability - Wie weit reicht die Rechenschaftspflicht der DS-GVO? Praktische Relevanz und Auslegung eines unbestimmten Begriffs, ZD 2018, S. 9–16.

Vietmeyer, Katja/Byers, Philipp, Der Arbeitgeber als TK-Anbieter im Arbeitsverhältnis. Geplante BDSG-Novelle lässt Anwendbarkeit des TKG im Arbeitsverhältnis unangetastet, MMR 2010, S. 807–811.

Voitel, Björn, Sind Hash-Werte personenbezogene Daten? Auf Kollissionskurs mit der EU-DSGVO, DuD 2017, S. 686–687.

von Lewinski, Kai/Barros Fritz, Raphael de/*Biermeier, Katrin*, Bevorstehende und künftige Regelungen des Einssatzes von Alogrithmen im HR-Bereich 2019, abrufbar unter: https://algorithmwatch.org/de/rechtsgutachten-von-lewinski / (letzter Abruf am: 29.04.2021).

von Lewinski, Kai/Pohl, Dirk, Auskunfteien nah der europäischen Datenschutzreform - Brüche und Kontinuitäten der Rechtslage, ZD 2018, S. 17–23.

Voßoff, Andrea/Hermerschmidt, Sven, Rote Linien eingehalten? Zur Verabschiedung der Datenschutz-Grundverordnung, DANA 2016, S. 68–69.

Waidner, Michael, SIT-TR-2015-06: Big Data und Privatheit, Stuttgart 2015 [zitiert als: *Waidner*, SIT-TR-2015-06].

Walter, Axel von, 8.4 Automatisierte Entscheidungsfindung (Art. 22 DSGVO), in: Kaulartz/Ammann/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, München 2020.

Walz, Stefan, Personalinformationen und Datenschutz, Mitbestimmung 1986, S. 292–295.

Wedde, Peter, Mobiltelefone und Arbeitsrecht, CR 1995, S. 41–47.

ders., Automatisierung im Personalmanagement - arbeitsrechtliche Aspekte und Beschäftigtendatenschutz 2020, abrufbar unter: https://algorithmwatch.org/de/gutachten-arbeitsrecht-datenschutz-wedde/ (letzter Abruf am: 29.04.2021).

Weichert, Thilo, Big Data und Datenschutz - Chancen und Risiken einer neuen Form der Datenanalyse, ZD 2013, 251-259.

ders., „Sensitive Daten" revisited, DuD 2017, S. 538–543.

Weitzel, Tim/Maier, Christian/Oehlhorn, Caroline/Weinert, Christoph/Wirth, Jakob/Laumer, Sven, Digitalisierung der Personalgewinnung. Ausgewählte Ergebnisse der Recruiting Trends 2018, einer empirischen Unternehmens-Studie mit den Top-1.000-Unternehmen aus Deutschland sowie den Top-300-Unternehmen aus der Branche IT und der Bewerbungspraxis 2018, einer empirischen Kandidaten-Studie mit Antworten von über 2.800 Kandidaten 2018, abrufbar unter: https://www.uni-bamberg.de/fileadmin/uni/fakultaeten/wiai_lehrstuehle/isdl/Studien_2018_2_Digitalisierung_der_Personalgewinnung_Digital-Version_20180207_ff_a.pdf (letzter Abruf am: 26.09.2019).

Werther, Simon/Bruckner, Laura (Hrsg.), Arbeit 4.0 aktiv gestalten. Die Zukunft der Arbeit zwischen Agilität, People Analytics und Digitalisierung, Berlin, Heidelberg 2018.

Weth, Stephan/Herberger, Maximilian/Wächter, Michael/Sorge, Christoph (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis. Praxishandbuch zum Arbeitnehmerdatenschutz. 2. Aufl., München 2019.

Wichert, Andreas, Künstliche Intelligenz, in: Hanser (Hrsg.), Lexikon der Neurowissenschaft. Gesamtausgabe, Heidelberg 2005.

Wiese, Günther/Kreutz, Peter/Oetker, Hartmut/Raab, Thomas/Weber, Christoph/Franzen, Martin/Gutzeit, Martin/Jacobs, Matthias (Hrsg.), Betriebsverfassungsgesetz. Gemeinschaftskommentar. 11. Aufl., Köln 2018 [zitiert als: GK-BetrVG/*Bearbeiter*].

Wildhaber, Isabelle, Die Roboter kommen - Konsequenzen für Arbeit und Arbeitsrecht, ZSR 2016, S. 315–351.

Wojak, Stefanie, Intelligente Kollektiv-Algorithmen in der Personalverwaltung. Betrachtung ausgewählter Problemfelder zweier fiktiver Szenarien nach Art. 22 DS-GVO, DuD 2018, S. 553–557.

Wójtowicz, Monika, Wirksame Anonymisierung im Kontext von Big Data, PinG 2013, S. 65–69.

Wolff, Heinrich Amadeus, A. I. Unionsrechtliche Grundlagen, in: Schantz/Wolff (Hrsg.), Das neue Datenschutzrecht. Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, München 2017.

ders., C. I. Die Regelungswerke im Überblick, in: Schantz/Wolff (Hrsg.), Das neue Datenschutzrecht. Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, München 2017.

ders., D. I. Grundsätze der Datenverarbeitung, in: Schantz/Wolff (Hrsg.), Das neue Datenschutzrecht. Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, München 2017.

ders., E. Technisch-Organisatorische Pflichten, in: Schantz/Wolff (Hrsg.), Das neue Datenschutzrecht. Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, München 2017.

Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht. 35. Aufl., München 2020 [zitiert als: BeckOK DatenSR/*Bearbeiter*].

Wroblewski, Andrej, Arbeitsrecht in einer Datenschutzverordnung?, NZA 2015, Editorial zu Heft 21.

Wunderer, Rolf/Dick, Petra/Jäger, Urs, Personalmanagement - quo vadis? Analysen und Prognosen zu Entwicklungstrends bis 2010. 4. Aufl., München 2006.

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

Wybitul, Tim, Neue Spielregeln bei E-Mail-Kontrollen durch den Arbeitgeber - Überblick über den aktuellen Meinungsstand und die Folgen für die Praxis, ZD 2011, S. 69–71.

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

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

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

Wybitul, Tim/Pötters, Stephan, Der neue Datenschutz am Arbeitsplatz, RDV, S. 10–16.

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

Zahariev, Martin, The evolution of EU data protection law on automated data profiling, PinG 2017, S. 73–79.

Zarsky, Tal Z., Incompatible: The GDPR in the Age of Big Data, Seton Hall Law Review 2017, S. 995–1020.

Rechtsprechungsverzeichnis

BAG, Urt. v. 05.12.1957 – 1 AZR 594/56, NJW 1957, 516.

BAG, Urt. v. 06.12.1973 – 2 AZR 10/73, NJW 1973, 1263.

BAG, Beschl. v. 09.09.1975 – 1 ABR 20/74, AP BetrVG 1972 § 87 Überwachung Nr. 2 1975.

BAG, Beschl. v. 29.03.1977 – 1 ABR 123/74, AP BetrVG 1972 § 87 Provision Nr. 1.

BAG, Beschl. v. 18.07.1978 – 1 ABR 8/75, AP BetrVG 1972 § 99 Nr. 7.

LAG Düsseldorf, Beschl. v. 21.11.1978 – 19 TaBV 39/78, DB 1978, 459.

BAG, Urt. v. 31.01.1979 – 5 AZR 454/77, BAGE 1979, 266.

BAG, Urt. v. 28.03.1979 – 5 AZR 80/77, AP BPersVG § 75 Nr. 3.

BAG, Beschl. v. 10.07.1979 – 1 ABR 50/78, AP BetrVG 1972 § 87 Überwachung Nr. 3 1979.

BAG, Beschl. v. 24.03.1981 – 1 ABR 32/78, NJW 1981, 404.

BAG, Beschl. v. 19.05.1981 – 1 ABR 109/78, AP BetrVG 1972 § 118 Nr. 18.

BAG, Beschl. v. 26.10.1982 – 1 ABR 11/81, BAGE 1982, 92.

BAG, Beschl. v. 06.12.1983 – 1 ABR 43/81, BAGE 1983, 285.

BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 1983, 1.

BAG, Beschl. v. 14.09.1984 – 1 ABR 23/82, NZA 1984, 28.

BAG, Beschl. v. 23.10.1984 – 1 ABR 2/83, NZA 1984, 224.

BAG, Beschl. v. 23.04.1985 – 1 ABR 2/82, AP BetrVG 1972 § 87 Überwachung Nr. 12.

BAG, Beschl. v. 03.12.1985 – 1 ABR 72/83, AP BetrVG 1972 § 99 Nr. 29.

BAG, Beschl. v. 18.02.1986 – 1 ABR 21/84, BAGE 1986, 143.

BAG, Beschl. v. 18.02.1986 – 1 ABR 27/84, AP BetrVG 1972 § 99 Nr. 33.

BAG, Beschl. v. 11.03.1986 – 1 ABR 12/84, AP BetrVG 1972 § 87 Überwachung Nr. 14 1986.

BAG, Beschl. v. 27.05.1986 – 1 ABR 48/84, AP BetrVG 1972 § 87 Überwachung Nr. 15.

BAG, Beschl. v. 18.08.1987 – 1 ABR 30/86, AP BetrVG 1972 § 77 Nr. 23.

BAG, Beschl. v. 08.12.1987 – 1 ABR 32/86, AP BetrVG 1972 § 98 Nr. 4 1987 = NZA 1987, 401.

BVerwG, Beschl. v. 31.08.1988 – 6 P 35.85, AP BPersVG § 75 Nr. 25.

BAG, Beschl. v. 18.10.1988 – 1 ABR 26/87, AP BetrVG 1972 § 99 Nr. 56.

BAG, Beschl. v. 08.08.1989 – 1 ABR 65/88, AP BetrVG 1972 § 87 Ordnung des Betriebes Nr. 15 1989.

BVerfG, Beschl. v. 14.09.1989 – 2 BvR 1062/87, BVerfGE 1989, 367.

BAG, Beschl. v. 17.10.1989 – 1 ABR 100/88, BAGE 1989, 169.

BAG GS, Beschl. v. 07.11.1989 – GS 3/85, AP BetrVG 1972 § 77 Nr. 46.

BAG, Beschl. v. 28.11.1989 – 1 ABR 97/88, NZA 1989, 406.

BVerwG, Beschl. v. 02.02.1990 – 6 PB 11.89, BeckRS 1990, 30937999.

BAG, Beschl. v. 01.08.1990 – 7 ABR 99/88, AP ZA-Nato-Trupppenstatus Art. 56 Nr. 20.

BAG, Beschl. v. 06.11.1990 – 1 ABR 60/89, NZA 1990, 358.

BAG, Beschl. v. 04.12.1990 – 1 ABR 10/90, AP BetrVG 1972 § 97 Nr. 1.

BAG, Beschl. v. 19.02.1991 – 1 ABR 21/90, AP BetrVG 1972 § 95 Nr. 25.

BVerwG, Beschl. v. 27.11.1991 – 6 P 7.90, BeckRS 1991, 30937826.

BAG GS, Beschl. v. 03.12.1991 – GS 2/90, AP BetrVG 1972 § 87 Lohngestaltung Nr. 51.

BAG, Beschl. v. 27.10.1992 – 1 ABR 4/92, NZA 1992, 607.

BAG, Beschl. v. 21.09.1993 – 1 ABR 28/93, AP BetrVG 1972 § 94 Nr. 4.

BAG, Beschl. v. 23.11.1993 – 1 ABR 38/93, AP BetrVG 1972 § 95 Nr. 33.

BAG, Beschl. v. 30.08.1995 – 1 ABR 4/95, NZA 1995, 218.

BAG, Beschl. v. 21.01.1997 – 1 ABR 53/96, AP BetrVG 1972 § 87 Ordnung des Betriebes Nr. 27.

LAG Niedersachsen, Urt. v. 13.01.1998 – 13 Sa 1235/97, NZA-RR 1998, 259.

BVerfG, Urt. v. 14.07.1999 – 1 BvR 2226/94, 2420/95, 2437/95, BVerfGE 1999, 313.

BAG, Beschl. v. 29.02.2000 – 1 ABR 4/99, AP BetrVG 1972 § 87 Lohngestaltung Nr. 105.

BAG, Beschl. v. 18.04.2000 – 1 ABR 28/99, AP BetrVG 1972 § 98 Nr. 9.

BAG, Urt. v. 13.06.2002 – 2 AZR 234/01, NZA 2002, 265.

BAG, Beschl. v. 10.12.2002 – 1 ABR 27/01, BeckRS 2002, 41197.

BAG, Beschl. v. 21.01.2003 – 3 ABR 26/02, NJOZ 2003, 2274.

EuGH, Urt. v. 06.11.2003 – C-101/01, EuZW, 2004, 245 – Lindqvist.

BAG, Beschl. v. 27.01.2004 – 1 ABR 7/03, NZA 2004, 556.

BVerfG, Urt. v. 03.03.2004 – 1 BvR 2378/98, 1084/99, BVerfGE 2004, 279.

BAG, Beschl. v. 29.06.2004 – 1 ABR 21/03, NZA 2004, 1278.

ArbG Frankfurt/M, Urt. v. 14.07.2004 – 9 Ca 10256/03, MMR 2004, 829.

OLG Karlsruhe, Beschl. v. 10.01.2005 – 1 Ws 152/04, MMR 2005, 178.

BAG, Beschl. v. 28.06.2005 – 1 ABR 26/04, NZA 2005, 111.

BAG, Beschl. v. 26.07.2005 – 1 ABR 29/04, NZA 2005, 1372.

BAG, Urt. v. 17.11.2005 – 6 AZR 118/05, NZA 2005, 370.

BAG, Beschl. v. 28.03.2006 – 1 ABR 5/05, NZA 2006, 932.

BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, BVerfGE 2006, 320.

BVerfG, Urt. v. 13.06.2007 – 1 BvR 1550/03, 2357/04, 603/05, BVerfGE 2007, 168.

BAG, Urt. v. 13.12.2007 – 2 AZR 537/06, NZA 2007, 1008-1012.

BVerfG, Urt. v. 27.02.2008 – 1 BvR 370, 595/07, BVerfGE 2008, 274.

BVerfG, Urt. v. 11.03.2008 – 1 BvR 2074/05, 1 BvR 1254/07, BVerfGE 2008, 378.

BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187.

VG Frankfurt/M., Urt. v. 06.11.2008 – 1 K 628/08.F (3), CR 2008, 125.

VGH Kassel, Beschl. v. 19.05.2009 – 6 A 2672/08.Z, NJW 2009, 2470.

BAG, Beschl. v. 23.03.2010 – 1 ABR 81/08, NZA 2010, 811.

BAG, Beschl. v. 20.04.2010 – 1 ABR 78/08, NZA 2010, 902.

LAG Niedersachsen, Urt. v. 31.05.2010 – 12 Sa 875/09, MMR 2010, 639.

BAG, Urt. v. 09.11.2010 – 1 AZR 708/09, NZA 2010, 466.

EuGH, Urt. v. 09.11.2010 – C-92/09, C-93/09 – Schecke und Eifert.

OLG Köln, Urt. v. 19.11.2010, BeckRS 2010, 14259.

LAG Berlin-Brandenburg, Urt. v. 16.02.2011 – 4 Sa 2132/10, ZD 2011, 43.

BGH, Urt. v. 22.02.2011 – VI ZR 120/10, NJW 2011, 2204.

EuGH, Urt. v. 05.05.2011 – C-543/09, EuZW, 2011, 485 – Deutsche Telekom AG/ Deutschland.

EuGH, Urt. v. 24.11.2011 – C-468/10, C-469/10, CR, 2012, 29 – ASNEF.

BAG, Beschl. v. 17.01.2012 – 1 ABR 45/10, NZA 2012, 687.

LG Berlin, Urt. v. 31.01.2013 – 57 S 87/08, ZD 2013, 618.

VG Karlsruhe, Urt. v. 27.05.2013 – 2 K 3249/12, CR 2013, 428.

BAG, Beschl. v. 09.07.2013 – 1 ABR 2/13 (A), NZA 2013, 1433.

EuGH, Urt. v. 18.07.2013 – C-426/11, NZA, 2013, 835 – Alemo-Herron.

BAG, Beschl. v. 14.01.2014 – 1 ABR 49/12, NZA-RR 2014, 356.

BGH, Urt. v. 28.01.2014 – VI ZR 156/13, ZD 2014, 306.

EuGH, Urt. v. 27.02.2014 – C-656/11, BeckRS 2014, 80469 – Kommission / Vereinigtes Königreich.

BAG, Beschl. v. 15.04.2014 – 1 ABR 2/13 (B), NZA 2014, 551.

VGH Baden-Württemberg, Urt. v. 30.07.2014 – 1 S 1352/13, ECLI:DE:VGHBW:2014:0730.1S1352.13.0A.

BAG, Urt. v. 18.09.2014 – 8 AZR 759/13, AP AGG § 15 Nr. 20 2014.

BAG, Beschl. v. 21.10.2014 – 1 ABR 10/13, NZA 2014, 311.

BAG, Urt. v. 11.12.2014 – 8 AZR 1010/13, NZA 2014, 604.
BAG, Urt. v. 12.02.2015 – 6 AZR 845/13, NZA 2015, 741.
BAG, Beschl. v. 17.03.2015 – 1 ABR 48/13, NZA 2015, 885.
LAG Berlin-Brandenburg, Urt. v. 14.01.2016 – 5 Sa 657/15 2016.
VG Saarlouis, Urt. v. 29.01.2016 – 1 K 1122/14, PharmR 2016, 207.
BAG, Beschl. v. 22.03.2016 – 1 ABR 12/14, NZA 2016, 894.
BAG, Beschl. v. 23.08.2016 – 1 ABR 22/14, NZA 2016, 194.
EuGH, Urt. v. 19.10.2016 – C-582/14, NJW, 2016, 3579 – Breyer.
BAG, Urt. v. 20.10.2016 – 2 AZR 395/15, NZA 2016, 443.
LAG Rheinland-Pfalz, Urt. v. 23.11.2016 – 2 Ca 1147/16, BeckRS 2016, 123929.
BAG, Beschl. v. 13.12.2016 – 1 ABR 7/15, NZA 2016, 657.
LAG München, Urt. v. 19.01.2017 – 3 Sa 668/16, BeckRS 2017, 152341.
BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205.
BAG, Urt. v. 27.07.2017 – 2 AZR 681/16, NZA 2017, 1327.
BAG, Beschl. v. 22.08.2017 – 1 ABR 52/14, NZA 2017, 50.
LAG Hamm, Beschl. v. 19.09.2017 – 7 TaBV 43/17, ZD 2017, 129.
LG Krefeld, Urt. v. 07.02.2018 – 7 O 198/17 2018.
BAG, Beschl. v. 07.05.2019 – 1 ABR 53/17, NZA 2019, 1218.
BVerfG, Beschl. v. 06.11.2019 – 1 BvR 16/13, NJW 2020, 300.
BVerfG, Beschl. v. 06.11.2019 – 1 BvR 276/17, NJW 2020, 314.
EuGH, Urt. v. 16.07.2020 – C 311/18, ECLI:EU:C:2020:559 – Schrems II

Anhang I: Genese des Art. 22 DSGVO

Ursprüngliche **Kommissionsfassung**[1534]

Artikel 20

Auf Profiling basierende Maßnahmen

(1) Eine natürliche Person hat das Recht, nicht einer auf einer rein automatisierten Verarbeitung von Daten basierenden Maßnahme unterworfen zu werden, die ihr gegenüber rechtliche Wirkungen entfaltet oder sie in maßgeblicher Weise beeinträchtigt und deren Zweck in der Auswertung bestimmter Merkmale ihrer Person oder in der Analyse beziehungsweise Voraussage etwa ihrer beruflichen Leistungsfähigkeit, ihrer wirtschaftlichen Situation, ihres Aufenthaltsorts, ihres Gesundheitszustands, ihrer persönlichen Vorlieben, ihrer Zuverlässigkeit oder ihres Verhaltens besteht.

Erste Fassung des **Europäischen Parlaments**[1535]

Artikel 20

~~Auf~~ Profiling ~~basierende Maßnahmen~~

(1) ~~Eine~~ **Unbeschadet der Bestimmungen des Artikels 6 hat jede** natürliche Person ~~hat~~ das Recht~~, nicht einer auf einer rein automatisierten Verarbeitung von Daten basierenden Maßnahme unterworfen zu werden, die ihr gegenüber rechtliche Wirkungen entfaltet oder sie in maßgeblicher~~ **dem Profiling gemäß Artikel 19 zu widersprechen. Die betroffene Person ist über ihr Recht, dem Profiling zu widersprechen, in deutlich sichtbarer** Weise ~~beeinträchtigt und deren Zweck in der Auswertung bestimmter Merkmale ihrer Person oder in der Analyse beziehungsweise Voraussage etwa ihrer beruflichen Leistungsfähigkeit, ihrer wirtschaftlichen Situation, ihres Aufenthaltsorts, ihres Gesundheitszustands, ihrer persönlichen Vorlieben, ihrer Zuverlässigkeit oder ihres Verhaltens besteht~~ **zu unterrichten**.

(2) Unbeschadet der sonstigen Bestimmungen dieser Verordnung darf eine Person ~~einer Maßnahme nach Absatz 1~~ **dem Profiling, das Maßnahmen**

1534 Vorschlag der Europäischen Kommission vom 25.01.2012, 2012/011 (COD), KOM/2012/11 endgültig, CELEX Nr. 52012PC0011.

1535 ABl. EU 2017, Nr. C 378/399.

zur Folge hat, durch die sich rechtliche Konsequenzen für die betroffene Person ergeben, oder die ähnlich erhebliche Auswirkungen auf die Interessen, Rechte oder Freiheiten der betroffenen Personen hat, nur unterworfen werden, wenn die Verarbeitung […]

[…]

(5) **Profiling, das Maßnahmen zur Folge hat, durch** die ~~Kommission wird ermächtigt, delegierte Rechtstakte~~ **sich rechtliche Konsequenzen für die betroffene Person ergeben, oder die ähnlich erhebliche Auswirkungen auf die Interessen, Rechte oder Freiheiten der betroffenen Person hat, darf sich nicht ausschließlich oder vorrangig auf automatisierte Verarbeitung stützen und muss eine persönliche Prüfung, einschließlich einer Erläuterung der** nach ~~Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Bedingungen, die für geeignete~~ **einer solchen Prüfung getroffenen Entscheidung enthalten. Zu den geeigneten** Maßnahmen zur Wahrung der berechtigten Interessen gemäß Absatz 2 ~~gelten sollen, näher zu regeln.~~ **gehören das Recht auf persönliche Prüfung und die Erläuterung der nach einer solchen Prüfung getroffenen Entscheidung.**

Aktuelle Fassung des Art. 22 DSGVO

Artikel 22

Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

(1) Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung - einschließlich Profiling - beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

(2) Absatz 1 gilt nicht, wenn die Entscheidung

a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,

b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder

c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

(3) In den in Absatz 2 Buchstaben a und c genannten Fällen trifft der Verantwortliche angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu

mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.

(4) Entscheidungen nach Absatz 2 dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 beruhen, sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

Anhang II: Muster-Betriebsvereinbarung konsolidiert

Präambel

Bereits aus der Bezeichnung „Human Ressources“ geht hervor, dass das Humankapital eines Unternehmens – im Gegensatz zu den Anfängen der Personalarbeit – ein wesentlicher Faktor für den Erfolg eines Unternehmens ist. Entscheidend prägen also die fachlichen und sozialen Fähigkeiten der Mitarbeiter den wirtschaftlichen Erfolg unseres Unternehmens XY. Gerade in der aktuellen Zeit, in welcher Arbeit in hohem Maße digitalisiert wird und der persönliche Kontakt auch unter den Kollegen abnimmt sowie die Unternehmensstrukturen immer komplexer werden, ist es von entscheidender Bedeutung für die Zufriedenheit der Arbeitnehmerschaft, dass innerbetriebliche Prozesse möglichst effizient ablaufen und Probleme frühzeitig erkannt und behoben werden. Hierfür setzt XY die Methode **People Analytics** ein, die den Entscheidungsträgern ermöglichen soll, etwaige Ungereimtheiten im Betriebsablauf bereits frühzeitig zu erkennen und gegensteuern zu können. Eine niedrige Reaktionszeit ist erforderlich, um mit den Maßnahmen nicht immer einen Schritt hinterherzuhinken, sondern eine Steuerung in Echtzeit zum Vorteil der Arbeitnehmerschaft zu ermöglichen.

XY setzt im Rahmen von People Analytics auf die **Auswertung von IT-Nutzungsdaten** und nutzt die Techniken des **Profilings und Scorings**, um den Arbeitnehmern und Entscheidungsträgern im Unternehmen in verständlicher Form alle für sie wesentlichen Informationen in **Dashboards** darzustellen und rasche Entscheidungen zu ermöglichen. Um Kommunikationsabläufe zu verbessern, wird die **Netzwerk-Analyse** eingesetzt.

Alltägliche Prozesse sollen durch automatisierte Entscheidungen beschleunigt und vereinfacht, somit das Human Resources Management entlastet und schnelle Entscheidungen ermöglicht werden.

Damit diese Form des modernen und evidenzbasierten Personalmanagements ermöglicht werden kann, wird folgende Vereinbarung geschlossen, die gleichzeitig auch als **datenschutzrechtliche Legitimationsgrundlage** für die hierfür erforderlichen Verarbeitungsvorgänge nach Art. 88 Abs. 1 DSGVO, § 26 Abs. 4 BDSG gilt. Um die gesetzlichen Vorgaben der DSGVO und des BDSG einzuhalten, regelt diese Vereinbarung die

betriebsverfassungsrechtlichen und datenschutzrechtlichen Rahmenbedingungen für den Einsatz von People Analytics **abschließend**.

§ 1 Anwendungsbereich, Gegenstand und allgemeine Grundsätze der Datenverarbeitung

(1) Diese Betriebsvereinbarung gilt für alle Arbeitnehmer im Sinne des § 5 Abs. 1 BetrVG, mit Ausnahme der leitenden Angestellten, und für jegliche Datenverarbeitungen, die im Zusammenhang mit der Analyse von personenbezogenen Daten von Arbeitnehmern zum Zwecke des Personalmanagements (People Analytics) stattfinden. Die Begriffsdefinitionen, soweit nicht ausdrücklich anders definiert, entsprechen denjenigen aus Art. 4 DSGVO.

(2) Gegenstand dieser Vereinbarung ist die Regelung angemessener und besonderer Maßnahmen zur Wahrung der berechtigten Interessen, der menschlichen Würde und der Grundrechte sowie des Schutzes der Persönlichkeit der Arbeitnehmer gem. Art. 88 Abs. 2 DSGVO beim Einsatz von People Analytics.

§ 2 Begriffsbestimmungen

1. „Scoring" ist die Verwendung eines Wahrscheinlichkeitswertes, welcher über ein wissenschaftlich-anerkanntes, mathematisches Verfahren berechnet wird, über ein bestimmtes zukünftiges Verhalten einer natürlichen Person im Hinblick auf die Untersuchungsfrage.

2. „Score" ist das Ergebnis eines Scoring-Vorgangs und stellt einen bestimmten Wahrscheinlichkeitswert über ein bestimmtes zukünftiges Verhalten einer natürlichen Person im Hinblick auf die Untersuchungsfrage dar. Dieser kann entweder in Prozent oder in Form einer Punktezahl im Rahmen eines vorgegebenen Schemas in Erscheinung treten.

3. „Ranking" ist ein Verfahren, bei welchem in einer abschließenden Liste die Inhalte der Liste nach einem vorgegebenen, wissenschaftlich-anerkannten, mathematischen Verfahren mit Blick auf die Passgenauigkeit zur Untersuchungsfrage gereiht werden. Das zugrundeliegende Verfahren stellt in der Regel ein „Scoring" bzw. eine Kombination verschiedener Score-Werte dar.

4. „Dashboard" ist eine Visualisierungsform für Daten. Dashboards werden im Rahmen dieser Betriebsvereinbarung dazu eingesetzt, um die aus People Analytics gewonnenen Daten für die jeweilige Zielperson der Analyse übersichtlich darzustellen.

5. „Netzwerk-Graph" ist ein grafisches Tool zur Darstellung der informellen Hierarchie im Unternehmen. Er basiert auf der Auswertung von Kommunikationsdaten der Arbeitnehmer im Unternehmen.

§ 3 Datenschutzrechtliche Grundsätze für die Anwendung von People Analytics

(1) Die in Art. 5 Abs. 1 lit. a bis f DSGVO festgelegten Datenschutzgrundsätze sind Inhalt dieser Vereinbarung und gelten für jegliche Verarbeitungen personenbezogener Daten der Arbeitnehmer und Beschäftigten nach § 26 Abs. 8 BDSG für die Zwecke von People Analytics (vgl. § 1 Abs. 1 dieser Vereinbarung).

(2) Personenbezogene Daten aus informationstechnischen Systemen, die nicht für die Zwecke von People Analytics erhoben wurden, dürfen – außer für die Zwecke der anonymisierten Nutzung – nicht für diesen Zweck verarbeitet werden. Ein Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO findet nicht statt. Ausnahmen sind gesondert unter Bezugnahme zu dieser Regelung spezifizieren.

(3) Zur Gewährleistung der Transparenz der Datenverarbeitung werden die Arbeitnehmer bei der Nutzung von IT-Daten in einfach verständlicher Sprache über die Kategorien der über sie erhobenen IT-Daten in regelmäßigen Abständen (monatlich) per E-Mail informiert. Die Spezifizierung der Kategorie hat so ausführlich wie möglich zu erfolgen.

(4) Soweit es die Auswertungsziele zulassen, werden keine personenbezogenen Daten durch die Systeme der XY erhoben. Ist eine anonyme Datenerhebung nicht möglich, so werden die Daten unverzüglich nach der Erhebung in größtmöglichem Maße aggregiert bzw. anonymisiert. In jedem Falle findet eine Pseudonymisierung der Daten statt.

(5) Sofern für die Analysen keine Zuordnung zu einer bestimmbaren Person notwendig ist, sondern eine Auswertung unter einem Pseudonym ausreichend ist, wird der Zuordnungsschlüssel durch eine dop-

pelte Verschlüsselung gesichert. In diesem Rahmen ist es erforderlich, dass die Geschäftsführung von XY und der (Gesamt-)Betriebsrat nur gemeinsam die Entschlüsselung vornehmen können. Die Verschlüsselung muss dem Stand der Technik entsprechen. Eine Entschlüsselung darf nur im Falle eines Straftatverdachts oder einer groben Pflichtverletzung durch den Arbeitnehmer erfolgen.

§ 4 Datenschutzrechtliche Information

(1) In Form einer „Datenschutzrechtlichen Information zur Erhebung von Beschäftigtendaten" wird den Arbeitnehmern eine leicht zugängliche Information über die Pflichten des Arbeitgebers nach dieser Betriebsvereinbarung, dem BDSG und der DSGVO sowie über die Rechte der Arbeitnehmer in Form einer PDF zur Verfügung gestellt. Diese Information wird laufend aktualisiert und die Arbeitnehmer bei Änderungen per E-Mail informiert. Die Information ist in einer verständlichen, klaren und einfachen Sprache zu verfassen. In der in § 3 Absatz 3 genannten zyklischen Information ist diese Information mit einem Hyperlink zu verknüpfen.

(2) In der Information nach Absatz 1 ist zu erläutern, in welchem Regelungszusammenhang diese Betriebsvereinbarung zu anderen Betriebsvereinbarungen sowie sonstigen betrieblichen Vorgaben und Regelungen steht. Die Normenhierarchie ist grafisch darzustellen.

§ 5 Einrichtung einer FAQ-Seite

Zusätzlich zur Veröffentlichung des Normtextes dieser Betriebsvereinbarung wird im Intranet eine „Frequently Asked Questions (FAQ)"-Seite eingerichtet, auf welcher der Normtext dieser Vereinbarung in leichter und verständlicher Sprache erläutert wird. Ergeben sich (allgemeine) Fragen von Arbeitnehmern zu dieser Vereinbarung, sind diese inklusive Beantwortung in den Katalog aufzunehmen. Die FAQ gelten nicht normativ, dienen jedoch aus Auslegungshilfe für die Regelungen in dieser Vereinbarung.

§ 6 Verzeichnis der Verarbeitungstätigkeiten

Der Arbeitgeber erstellt – zusätzlich zu einem Verzeichnis nach Art. 30 DSGVO – ein Verzeichnis der Verarbeitungstätigkeiten für die einzelnen

Verarbeitungsvorgänge nach dieser Betriebsvereinbarung. Es sind die Vorgaben des Art. 30 DSGVO einzuhalten und das Verzeichnis dieser Betriebsvereinbarung anzuhängen.

§ 7 Informations- und Auskunftsrechte der Arbeitnehmer

(1) Es gelten die gesetzlichen Informations- und Auskunftsrechte gem. Art. 13 ff. DSGVO und §§ 32 ff. BDSG.

(2) In Ergänzung zu den gesetzlichen Informations- und Auskunftsrechten erfolgen in dieser Vereinbarung Konkretisierungen zur Information durch den Arbeitgeber im Rahmen der einzelnen Verarbeitungssituationen.

(3) Die Informationserteilung erfolgt per E-Mail an die dienstliche E-Mail-Adresse des Arbeitnehmers. In begründeten Fällen kann der Arbeitnehmer vom Arbeitgeber eine schriftliche Information verlangen. In jedem Fall ist die Information unentgeltlich zur Verfügung zu stellen. Eine mündliche Information scheidet aus.

§ 8 Vorgangsanalyse von Versicherungsfällen pro Niederlassung

(1) XY ist es gestattet, die personenbezogenen Daten der Arbeitnehmer für die Zwecke der Vorgangsanalyse von Versicherungsfällen auf Niederlassungsebene auszuwerten.

(2) Als Vorgangsanalyse von Versicherungsfällen wird die Berechnung einer durchschnittlichen Anzahl von bearbeiteten Fällen pro Sachbearbeiter und Niederlassung verstanden. Es erfolgt eine Untergliederung der Daten in die Kategorien „Gesamt“, „Versicherungsanträge“, „Policenanpassungen“ und „Beschwerden“.

(3) Vor einer Weiterverarbeitung sind die aus dem System ABC verwendeten Daten auf Niederlassungsebene zu aggregieren. Die Bearbeiterkennung des Sachbearbeiters ist aus dem Datensatz zu entfernen. Darüber hinaus hat XY sicherzustellen, dass keine Identifizierbarkeit eines Sachbearbeiters möglich ist. Die Verknüpfung mit weiteren Daten zu weiteren Verarbeitungszwecken ist vorbehaltlich einer gesonderten Regelung verboten.

§ 9 Erfassung der Bildschirmarbeitszeit zur Gesundheitsvorsorge

(1) Die Betriebsärztin Maxi Musterfrau erfasst im Rahmen des Arbeitsschutzes und der Gesundheitsvorsorge die Bildschirmarbeitszeiten der Arbeitnehmer. Die Verarbeitung und Erfassung dieser personenbezogenen Daten wird für die Auswertung zur Vermeidung von Überbelastungen durch diese Betriebsvereinbarung legitimiert.

(2) Der Datenbestand ist gesondert vom sonstigen Datenbestand der XY zu erfassen und insbesondere vor Zugriffen durch den Arbeitgeber durch geeignete Maßnahmen nach dem Stand der Technik zu schützen. Verantwortliche Verarbeiterin ist allein Maxi Musterfrau; eine Weitergabe der Daten an Dritte, auch an den Betriebsrat, ist nicht gestattet.

(3) Jeder Arbeitnehmer hat jederzeit die Möglichkeit der Datenverarbeitung für den in Absatz 1 genannten Zweck zu widersprechen. Im Falle eines Widerspruchs ist der gesamte Datensatz zu diesem Arbeitnehmer, der im Rahmen von Absatz 1 erhoben wurde, unverzüglich zu löschen und der Arbeitnehmer über die erfolgte Löschung zu informieren.

(4) Die Betriebsärztin verarbeitet diese Daten ausschließlich zur Gesundheitsvorsorge und Prävention sowie im Rahmen von Behandlungen der betroffenen Arbeitnehmer.

§ 10 Einsatz von Wearables im Hochrisikobereich

(1) XY stellt seinen Arbeitnehmern, die in der Versicherungsfall-Werkstatt arbeiten, Wearables zur Verfügung, die den CO-Wert der Luft sowie die Herzfrequenz und die Sauerstoffsättigung des Bluts erfassen.

(2) Arbeitnehmer, die sich im Hochrisikobereich aufhalten, sind während der Zeit des Aufenthalts verpflichtet, ein Wearable zu tragen. XY hat für die Einhaltung dieser Pflicht durch geeignete Maßnahmen zu sorgen.

(3) XY verarbeitet die Daten zum CO-Gehalt der Luft und des Standorts des Wearables zum Zwecke des Arbeitsschutzes. Das Wearable generiert hierbei alle zehn Minuten eine neue, zufällige ID zur Anmeldung

am Access Point. Die generierte ID darf nicht einem bestimmten Arbeitnehmer zuordenbar sein. Es erfolgt keine dauerhafte Speicherung der registrierten IDs.

(4) Der Access Point muss so positioniert und eingestellt werden, dass er alle Wearables im Hochrisikobereich sowie mindestens zwei, aber maximal vier weitere Wearables außerhalb dieses Bereiches zur Alarmierung erfasst.

(5) Überschreitet der CO-Wert des Raumes 30 ppm, so wird der Träger des Wearables vor einer hohen Konzentration gewarnt. Überschreitet der Wert 500 ppm, wird der Träger zum sofortigen Verlassen des Raumes aufgefordert. Bei einem Überschreiten des Grenzwertes von 6.400 ppm erfolgt eine erneute Warnung des Arbeitnehmers und eine Alarmierung aller nach Absatz 4 erfassten Personen. Im letzten Fall übermittelt das Wearable den Namen des Beschäftigten an die alarmierten Personen, um eine rasche Hilfe zu gewährleiten. Werden nach Absatz 4 keine weiteren Personen erfasst, so erfolgt eine Alarmierung über den Verteiler notfall@xy.com.

(6) Bei Überschreiten eines CO-Wertes von 10.000 ppm wird zusätzlich die Betriebsärztin über den Vorfall informiert und neben dem Namen und des konkreten CO-Werts auch die Herzfrequenz sowie die Sauerstoffsättigung der letzten 15 Minuten in ihren Datenbestand übermittelt; die Verarbeitung der Gesundheitsdaten des betroffenen Arbeitnehmers für diesen Zweck wird durch diese Vorschrift legitimiert. Die Übertragung der Daten muss über einen verschlüsselten Kanal nach dem aktuellen Stand der Technik erfolgen.

§ 11 Nutzung von AnalyzeIt

(1) XY setzt zur Optimierung der Arbeitsabläufe im Unternehmen AnalyzeIt ein. AnalyzeIt ermöglicht es, Auswertungen des täglichen (digitalen) Arbeitstages auf Arbeitnehmerbasis zu erstellen. Zur Sicherung des Datenschutzes werden individualisierte Auswertungen nur aufgrund einer Einwilligung von Arbeitnehmern erstellt.

(2) In diesem Rahmen wird die Technik des Scorings eingesetzt. Unter Ausnahme von § 3 Abs. 2 dieser Vereinbarung ist die zweckändernde

Nutzung der hierfür erforderlichen Daten auf Grundlage einer Einwilligung für das persönliche Dashboard möglich.

(3) AnalyzeIt verarbeitet folgende Kategorien von Daten: Einträge im persönlichen Kalender des Arbeitnehmers, E-Mail-Sender und -Empfänger sowie Versende- und Empfangszeitpunkt, Speicherdatum eines E-Mail-Entwurfs. Es erzeugt einen individuellen, täglichen Produktivitätsscore auf Basis dieser Daten.

(4) Bei der Erstellung des Produktivitätsscores ist sicherzustellen, dass ein wissenschaftliches, mathematisch-anerkanntes Verfahren eingesetzt wird, das zu aussagekräftigen Ergebnissen führt. Auf der AnalyzeIt-Plattform muss die Berechnung des Scores gegenüber dem Arbeitnehmer in Grundzügen erläutert werden. In jedem Falle muss es dem Arbeitnehmer möglich sein, den berechneten Score nachvollziehen zu können.

(5) Es ist durch technisch-organisatorische Maßnahmen sicherzustellen, dass nur der Arbeitnehmer selbst Zugriff auf seine individualisierten Auswertungen hat.

(6) Für die Einwilligung des Arbeitnehmers gilt § 26 Abs. 2 BDSG. Die Einwilligung hat durch eine elektronische Zustimmung des Arbeitnehmers mittels einer Check-Box auf der Analytics-Plattform zu erfolgen. Die Freiwilligkeit der Einwilligung wird vermutet. Es ist ausdrücklich darauf hinzuweisen, dass der Arbeitnehmer jederzeit seine Einwilligung widerrufen kann. Abweichend von Art. 7 Abs. 3 S. 2 DSGVO gilt, dass die aufgrund der Einwilligung verarbeiteten personenbezogenen Daten für das persönliche Dashboard rückwirkend und unverzüglich gelöscht werden. Der Arbeitnehmer kann seine Einwilligung jederzeit widerrufen. Die Widerrufserklärung kann im AnalyzeIt-Dashboard direkt oder per E-Mail an widerruf@xy.com erklärt werden.

(7) XY ist gestattet, aggregierte Auswertungen der in Absatz 2 genannten Daten auf Team-, Abteilungs- und Unternehmensebene für Zwecke der People Analytics zu erstellen. Personelle Maßnahmen mit einer negativen Auswirkung auf Arbeitnehmer aufgrund dieser Daten sind ausgeschlossen.

(8) Bei der Aggregation der Daten ist sicherzustellen, dass die Daten nicht mehr einer bestimmbaren Person zuordenbar sind. Im Allgemeinen wird bei einer Aggregation von Daten von mindestens vier Arbeitnehmern von einer Anonymität ausgegangen. Sollte im Einzelfall eine Zuordnung zu einer bestimmbaren Person möglich sein, so sind der Betriebsrat und der betroffene Arbeitnehmer unverzüglich zu informieren und weitere Maßnahmen vorzunehmen, dass weitere Identifizierungen nicht stattfinden. Die individualisierbaren Daten sind unverzüglich zu löschen.

(9) Die aggregierten Auswertungen des eigenen Teams-, der eigenen Abteilung und des Unternehmens sind den Arbeitnehmern zur Verfügung zu stellen. Dies soll, wenn möglich, im persönlichen Dashboard des Arbeitnehmers erfolgen.

§ 12 Nutzung von ScoreIt

(1) XY setzt in Ergänzung der Personalverwaltungssoftware PersoPlus das Plugin ScoreIt ein. ScoreIt ermöglicht es, die vorhandenen Stammdaten der Arbeitnehmer, Zielvereinbarungen und unterjährigen Mitarbeitergespräche auszuwerten, mit den Stellenbeschreibungen abzugleichen und verschiedene Punktewert von 0 bis 10 für Entwicklungspotential, Passgenauigkeit auf die Stelle, Passgenauigkeit auf Beförderungsstellen sowie den Gesamteindruck über den Arbeitnehmer zu generieren. Dieser Score dient der Unterstützung der Personalverantwortlichen bei Personalmaßnahmen.

(2) Bei der Verwendung von ScoreIt ist darauf zu achten, dass ein wissenschaftlich-anerkanntes, mathematisches Verfahren verwendet wird, das nachvollziehbare Punktewerte generiert. Es muss XY zu jedem Zeitpunkt möglich sein, den konkreten Punktewert zu erläutern.

(3) XY ist, in Ausnahme des Grundsatzes von § 3 Abs. 2 dieser Vereinbarung, legitimiert, die Daten auf PersoPlus für das Scoring durch ScoreIt in zweckverändernder Weise weiterzuverarbeiten. Hierbei wird davon ausgegangen, dass eine Zweckkompatibilität im Sinne des Art. 6 Abs. 4 DSGVO besteht. Der Arbeitgeber darf keine besonderen Kategorien von Daten im Sinne des Art. 9 DSGVO verwenden. Durch technisch-organisatorische Maßnahmen muss sichergestellt werden, dass

die Daten entsprechend dem aktuellen Stand der Technik gegen unbefugte Zugriffe Dritter abgesichert werden.

(4) Die generierten Scorewerte dürfen nicht als alleinige Grundlage für Personalmaßnahmen herangezogen werden. Automatisierte Einzelfallentscheidungen sind verboten. Jede vorgeschlagene Maßnahme muss inhaltlich durch einen entscheidungsbefugten Vorgesetzten überprüft und genehmigt werden. Jede benachteiligende Maßnahme, die auf einem Scorewert beruht, ist unter Zugrundelegung der für den Score erheblichen Datenbasis gegenüber dem Arbeitnehmer und dem Betriebsrat zu begründen.

(5) Der betroffene Arbeitnehmer hat den Anspruch, jederzeit Einblick in seinen Scorewert zu nehmen und eine Begründung zur Zusammensetzung in Textform zu fordern. Ebenfalls hat er die Möglichkeit gegen den generierten Wert Widerspruch einzulegen und seinen Standpunkt darzustellen. XY ist verpflichtet, den Scorewert unter Berücksichtigung der Stellungnahme des Arbeitnehmers zu überprüfen und ihm das Ergebnis der Überprüfung schriftlich mitzuteilen.

§ 13 Automatisierte Fortbildungsvorschläge auf Basis von ScoreIt

(1) ScoreIt soll neben dem in § 12 genannten Anwendungsszenario auch dafür genutzt werden, Arbeitnehmern auf Basis ihres Entwicklungsscores und der Passgenauigkeitsscores maßgeschneiderte Fortbildungen vorzuschlagen, um die fachlichen und persönlichen Kompetenzen weiter zu fördern.

(2) In diesem Zusammenhang ist XY legitimiert, die durch ScoreIt generierten Daten, in Ausnahme von § 3 Abs. 2 dieser Vereinbarung, für Fortbildungszwecke zu verarbeiten.

(3) Der Arbeitnehmer erhält hierzu eine E-Mail mit einem Fortbildungsvorschlag und entsprechenden Terminen für die Fortbildung. In dieser E-Mail ist dem Arbeitnehmer die Entscheidungsgrundlage für den Vorschlag auf Basis ihres Scores darzustellen. Ferner soll, nach Möglichkeit, die durch die Maßnahme zu erzielende Scoreverbesserung aufgezeigt werden. In keinem Fall wird der Arbeitnehmer durch einen automatisierten Vorschlag zur Teilnahme an einer Fortbildung verpflichtet.

(4) Soll ein Arbeitnehmer zu einer Fortbildung auf Basis von ScoreIt verpflichtet werden, so ist sicherzustellen, dass ein Vorgesetzter den generierten Vorschlag unter Zugrundelegung bisheriger Personalgespräche und Erfahrungswerten überprüft und die Teilnahme zur Fortbildung unter Ausübung des Direktionsrechts persönlich anordnet.

(5) Bei begrenzten Ausbildungskapazitäten ist dem Betriebsrat vor Übermittlung der Vorschläge die Vorschlagsliste des Systems vorzulegen. Dieser hat nach Erhalt der Liste eine Woche Zeit, um die Liste zu überprüfen und eigene Vorschläge einzubringen. XY und Betriebsrat einigen sich unter Beachtung des von ScoreIt generierten Scores auf eine gemeinsame Liste.

(6) In jedem Falle ist dem Betriebsrat eine Liste der geplanten Fortbildungen zu übermitteln, sodass dieser eigene Vorschläge einbringen kann. Unter Berücksichtigung des von ScoreIt generierten Werts entscheiden Arbeitgeber und Betriebsrat über die Teilnahme der Vorschläge des Betriebsrats an den angebotenen Fortbildungen. Die betroffenen Arbeitnehmer werden nach dem in Absatz 3 geregelten Verfahren über die Fortbildung informiert.

§ 14 Verbot der Privatnutzung der betrieblichen Kommunikation und Durchführung von Netzwerk-Analysen

(1) Die Nutzung der betrieblichen Kommunikationsplattformen (E-Mail, Telefonie und TeamIt) für private Zwecke ist verboten.

(2) XY nutzt die Verbindungsdaten der betrieblichen Kommunikationsplattformen für Netzwerk-Analysen durch den Einsatz eines Enterprise Social Graph. Ziel der Analysen ist es, das informelle Netzwerk des Netzwerks darzustellen und hierdurch die formale Hierarchie des Unternehmens zu optimieren.

(3) Nach Information der Arbeitnehmer über die Zweckerweiterung der Verarbeitung der Verbindungsdaten ist XY legitimiert, die personenbezogenen Verbindungsdaten für Netzwerkanalysen zu nutzen. Die Arbeitnehmer sind mindestens eine Woche vor Aktivierung des Enterprise Social Graph umfassend in Textform per E-Mail sowie durch deutlich sichtbaren Hinweis im Intranet zu informieren. Diese Information umfasst auch die Warnung, dass hierdurch bei unerlaubter Pri-

vatnutzung private Beziehungen zwischen einzelnen Arbeitnehmern aufgedeckt werden können.

(4) Personelle Maßnahmen auf Basis der durch den Enterprise Social Graph gewonnen Erkenntnisse dürfen nicht zum Nachteil der Arbeitnehmer angewandt werden. Ausnahme sind repressive Maßnahmen, die unter den Voraussetzungen des § 26 Abs. 2 BDSG ergriffen werden.

(5) Der Zugriff auf den Enterprise Social Graph ist auf das erforderliche Minimum zu beschränken; jeder Zugriff auf das System ist zu dokumentieren.

(6) Dem Betriebsratsvorsitzenden und seinem Stellvertreter sind unter den Voraussetzungen des Absatz 5 Einsicht in den Enterprise Social Graph zu gewähren; die hierdurch erlangten Kenntnisse unterliegen der Geheimhaltungspflicht.

(7) Die Daten der Netzwerkanalyse sind spätestens nach einem Jahr nach Erhebung zu löschen; wurde das mit der Verarbeitung erstrebte Ziel vorher erreicht, sind die Daten nach Zielerreichung unverzüglich zu löschen.

§ 15 Spezifische technische und organisatorische Sicherungsmaßnahmen

(1) Es ist sicherzustellen, dass alle aufgrund dieser Vereinbarung verarbeiteten Daten nach dem Stand der Technik verschlüsselt werden. Beim Einsatz eines symmetrischen Verschlüsselungsverfahrens ist (Stand: Mai 2021) mindestens AES-256 einzusetzen.

(2) Die Daten sind darüber hinaus, soweit möglich, zu pseudonymisieren. Eine Rückführung zum Klarnamen darf erst im Rahmen der Anzeige der Daten für den Endanwender erfolgen.

(3) Es ist ein Berechtigungskonzept zu erarbeiten, in welchem alle Arbeitnehmer mit Zugriff auf die personenbezogenen Daten in dieser Betriebsvereinbarung konkret benannt werden und begründet wird, weshalb ein Zugriff auf die Daten erforderlich ist. Über jede Berechtigungsvergabe ist der Betriebsrat zu informieren. Alle Personen mit

einem Zugriff auf die personenbezogenen Daten nach dieser Vereinbarung sind zur Geheimhaltung zu verpflichten.

(4) Ferner ist ein Löschkonzept zu entwickeln, welches dieser Betriebsvereinbarung angehängt wird und verpflichtend ist. In diesem müssen für jede Kategorie der im Rahmen dieser Vereinbarung erhobenen Daten Speicherfristen sowie der konkrete Vorgang der Löschung und dessen Dokumentation festgelegt werden. Des Weiteren sollen Überprüfungsmöglichkeiten des Betriebsrats einer sicheren Löschung festgelegt werden. Dieses Löschkonzept dient der Sicherstellung der Datenminimierung und Speicherbegrenzung und ist mit dem Betriebsrat abzustimmen. Es ist an geeigneter Stelle im Intranet zu veröffentlichen.

§ 16 Verfahren bei Streitigkeiten / Einigungsstelle

(1) Bei Streitigkeiten über die Anwendung, Auslegung oder Reichweite dieser Vereinbarung sind sowohl XY als auch der Betriebsrat berechtigt, die Einigungsstelle anzurufen.

(2) Die Entscheidung der Einigungsstelle ist verbindlich.