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.