E. Bewertung von People Analytics-Einsatzszenarien

Es wurde herausgestellt, dass sich ein Wandel vom „klassischen Personalmanagement 1.0“ hin zu People Analytics in Kombination mit evidenzbasiertem Management als Teil der Arbeit 4.0 vollzogen hat bzw. noch vollzieht (**Kapitel B**). Der Begriff der „People Analytics“ als Oberbegriff für moderne Ansätze im Personalmanagement und dessen Vor- und Nachteile im Vergleich zum Personalmanagement 1.0 wurden in **Kapitel C** ausführlich dargestellt. Im Anschluss wurden in **Kapitel D** die rechtlichen Grundlagen für den Einsatz moderner HR-Maßnahmen und Tools geklärt.

In diesem Kapitel soll nun in verschiedenen Stufen untersucht werden, inwiefern überhaupt Datenanalysen, die Bewertungen in Form von „Scores“ oder Persönlichkeitsprofile erzeugen sollen, als Rechtsgrundlage für Entscheidungen dienen dürfen (§ **1**), bevor im Anschluss untersucht wird, inwieweit diese Datengrundlagen auch für automatisierte Entscheidungen herangezogen werden dürfen (§ **2**). Ein mögliches und prominentes Beispiel von People-Analytics stellen Dashboards dar, die sowohl dem Arbeitnehmer als auch dem Arbeitgeber die nutzerfreundliche Darstellung der Analyseergebnisse auf dem Computer oder Mobilgerät überhaupt erst ermöglichen. Dieser Art der Datenaufbereitung soll daher besondere Aufmerksamkeit gewidmet werden (§ **3**). Ein mit vielen Analysetools einhergehendes und besonders in jüngerer Zeit aufkommendes Werkzeug sind sog. Netzwerk-Graphen, nunmehr in Form des sog. *Enterprise Social Graph*. Letzterer soll das (innerbetriebliche) Kommunikationsnetzwerk analysieren und weitere Einsichten in die informelle Hierarchie geben. Ein weiterer Abschnitt wird daher den Netzwerk-Graphen gewidmet (§ **4**).

Das nachfolgende Kapitel (**Kapitel F**) soll auf Basis der in diesem Kapitel gefundenen Ergebnisse Regelungsmöglichkeiten der Betriebspartner für die dargestellten Werkezuge und Tools erarbeiten und schließlich in einer Muster-Betriebsvereinbarung münden, die den Verhandlungspartnern als Grundstruktur für die Regelung eigener People-Analytics-Sachverhalte dienen und die Reichweite der Regelungsmöglichkeiten aufzeigen soll.

§ 1 People Analytics als Grundlage bzw. Unterstützung für Personalentscheidungen

In einem ersten Schritt muss geklärt werden, inwiefern Analyseergebnisse – die rechtmäßige Erhebung der Daten (für andere Zwecke) vorausgesetzt – als Grundlage bzw. Unterstützung für Personalentscheidungen dienen dürfen.

I. Grundsatz der Zweckbindung von personenbezogenen Daten

Sofern Daten für einen bestimmten Zweck, beispielsweise für die Begründung des Arbeitsverhältnisses, rechtmäßig erhoben wurden, ist zu beachten, dass diese Daten nicht beliebig für andere Verarbeitungszwecke eingesetzt werden. Art. 5 Abs. 1 lit. b DSGVO statuiert den Grundsatz der Zweckbindung. Hiernach müssen Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesem Zweck nicht zu vereinbarenden Weise weiterverarbeitet werden. Hs. 2 statuiert eine Ausnahme für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke. Eine weitere Auflockerung des Zweckbindungsgrundsatzes stellt Art. 6 Abs. 4 DSGVO dar. Dieser bestimmt, dass wenn die Verarbeitung zu einem anderen Zweck als zu demjenigen erfolgt, zu dem die personenbezogenen Daten erhoben wurden, und weder auf der Einwilligung der betroffenen Person oder einer Rechtsvorschrift beruht, der Verantwortliche die Zweckvereinbarkeit anhand vorgegebener Kriterien zu prüfen hat (sog. *Kompatibilitätstest*): Die Kriterien des Kompatibilitätstestes sind in Art. 6 Abs. 4 lit. a - e DSGVO aufgezählt: Verbindung zwischen den Zwecken der Erhebung und der Weiterverarbeitung (lit. a), Zusammenhang, in welchem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen (lit. b), Art der personenbezogenen Daten, insbesondere ob es sich um sensitive Daten im Sinne von Art. 9 DSGVO handelt oder ob Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 DSGVO verarbeitet werden (lit. c), Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen (lit. d) sowie Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören können (lit. e).

In einem ersten Schritt ist zu prüfen, wie weit ein Verarbeiter den Verarbeitungszweck unter der Maßgabe des Art. 5 Abs. 1 lit. b DSGVO festlegen

kann bzw. wie weit ein gesetzlicher Verarbeitungszweck ist, bevor auf eventuelle Ausnahmen von der Zweckbindung eingegangen wird. Wäre es dem Verarbeiter, z.B. im Rahmen einer Betriebsvereinbarung oder einer Einwilligung möglich, einen sehr weiten Verarbeitungszweck zu definieren, kommt es auf mögliche Ausnahmen nicht mehr an.

1. Spezifität der Zweckbestimmung nach Art. 5 Abs. 1 lit. b DSGVO

Der Grundsatz der Zweckbestimmung wird auch in Erwägungsgrund 39 S. 6 der DSGVO nochmals aufgegriffen. Hier wird verdeutlicht, dass insbesondere die bestimmten Zwecke, zu denen personenbezogene Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung feststehen sollen. Auf den ersten Blick scheint es, dass die Zweckbestimmung daher sehr eng gefasst werden muss[805] und insbesondere Big Data-Auswertungen mit ungewissem Ausgang nach den Erwägungsgründen ausgeschlossen werden sollen.

Tatsächlich ist es so, dass der Grundsatz der Zweckbindung eines der zentralen Prinzipien des Datenschutzrechts ist.[806] So wurde dieser bereits 1990 nach dem Volkszählungsurteil des BVerfG[807] für den öffentlichen Bereich in das BDSG aufgenommen.[808] In Verbindung mit dem Erforderlichkeitsgrundsatz kann hieraus die Forderung entnommen werden, dass der Betroffene genau wissen soll, was andere (bzw. Datenverarbeiter) über ihn wissen,[809] da er seine Daten unter der Erwartung eines bestimmten Verwendungszwecks offenlegt.[810] Es ist somit ein Ausfluss des in Art. 5 Abs. 1 lit. a DSGVO statuierten Transparenzgrundsatzes, denn nur wenn die betroffene Person weiß, zu welchen Zwecken ihre Daten verarbeitet werden, ist die Datenverarbeitung für sie nachvollziehbar. Die Zweckbe-

805 So auch *Schantz*, NJW 2016, 1841 (1842).
806 *Herbst*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 5 DSGVO Rn. 21; *Kühling/Klar/Sackmann*, Datenschutzrecht, S. 146 Rn. 338; *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, S. 201; *Article 29 Data Protection Working Party*, WP 203, S. 4; EuArbRK/*Franzen*, Art. 5 DSGVO Rn. 5.
807 BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1 – Volkszählungsurteil.
808 *Rüpke*, § 12. Rechtsgrundlagen der Verarbeitung, in: Rüpke/von Lewinski/Eckhardt, Datenschutzrecht, Rn. 38.
809 *Rüpke*, § 12. Rechtsgrundlagen der Verarbeitung, in: Rüpke/von Lewinski/Eckhardt, Datenschutzrecht, Rn. 38.
810 *Article 29 Data Protection Working Party*, WP 203, S. 4.

stimmung ist der „Fixpunkt", an dem sich die datenschutzrechtliche Prüfung vollzieht.[811]

Gerade aufgrund moderner Verarbeitungstechniken und der damit verbundenen Verknüpfungsmöglichkeiten verschiedener Daten, nicht zuletzt aufgrund Big Data, gewinnt der Zweckbindungsgrundsatz an immenser Bedeutung.[812] Auswertungen unter dem Stichwort „Big Data" basieren darauf, dass die Daten frei genutzt werden können, um neue Erkenntnisse zu gewinnen.[813] Der Grundsatz steht somit, wie Kritiker behaupten, Innovationsprozessen in der Wirtschaft klar entgegen.[814] Ziel von solchen Auswertungen ist es – wie bereits dargestellt – unbekannte Zusammenhänge zu entdecken, die dem menschlichen Betrachter bislang verborgen blieben.

Bei den Regelungen zur Zweckvereinbarkeit in Art. 6 Abs. 4 DSGVO handelt es sich nunmehr um eine Aufweichung des früher in Deutschland geltenden (relativ) strengen Zweckbindungsgrundsatzes.[815]

Die Zweckvereinbarkeit ist jedoch von der Zweckbestimmung nach Art. 5 Abs. 1 lit. b DSGVO zu unterscheiden. In einem ersten Schritt muss zunächst ein Verarbeitungszweck festgelegt werden, bevor dieser auf weitere mit diesem vereinbare Verarbeitungsmaßnahmen geprüft werden kann.

Bei der Festlegung des Verarbeitungszwecks muss der Verarbeiter so spezifisch sein, dass exakt feststellbar ist, welche Verarbeitungsvorgänge davon erfasst sind und welche nicht. Nur dann kann die Rechtmäßigkeit der Verarbeitung sicher festgestellt werden.[816] Zulässig ist es auch, mehrere Verarbeitungszwecke festzulegen, wobei allerdings jeder genau bestimmt sein muss.[817] Diese Festlegungen sind sowohl in der Datenschutzinformation nach Art. 13 f. DSGVO als auch im grundsätzlich schriftlich bzw. elektronisch zu führenden Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO aufzunehmen.[818]

---

811 Vgl. EuArbRK/*Franzen*, Art. 5 DSGVO Rn. 14; *Dammann*, ZD 2016, 307 (311).
812 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 52 Rn. 5.
813 *Buchner*, DuD 2016, 155 (156).
814 Vgl. hierzu *Grafenstein*, DuD 2015, 789 zum Spannungsfeld von Datenschutz und Innovationsprozessen.
815 *Kremer*, § 2 Zulässigkeit der Verarbeitung, in: Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, Rn. 44; aA *Gierschmann* ZD (2016), 51 (54).
816 *Article 29 Data Protection Working Party*, WP 203, S. 15.; so wohl auch EuArbRK/*Franzen*, Art. 5 DSGVO Rn. 5.
817 Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 13.
818 Insofern ist es nicht ganz korrekt, wenn *Götz*, Big Data im Personalmanagement, S. 121 davon spricht, dass Formvorschriften nicht existierten. Es gibt

Die *Artikel-29-Datenschutzgruppe* nannte in ihrem Arbeitspapier zur Zweckbindung Beispiele für zu vage Zweckfestlegungen. Das wären zum Beispiel „*IT-Sicherheitszwecke*", „*Marketingzwecke*" oder „*zukünftige Untersuchungen*". Die Spezifität der Zweckbestimmung hängt vom Kontext der Datensammlung und -verarbeitung sowie der Art der involvierten Daten ab. Teilweise wird vertreten, dass mit steigender Sensibilität der Erkenntnisse auch die Anforderungen an die Zweckdefinition steigen.[819] Kontraproduktiv sind aber auch zu detaillierte Zweckbestimmungen, insbesondere wenn diese zu sehr in Rechtssprache mit vielen Hinweisen gehalten sind und der Zweck hierdurch verschleiert würde.[820]

Folgende Zweckfestlegungen reichen nach Auffassung der Literatur aus: „*Reise nach Mallorca im Mai 2015*" oder „*Bearbeitung des Antrags auf Sondernutzungsgenehmigung v. 15.07.2015*".[821]

a) Zweckbestimmung im Rahmen der Einwilligung / einer Kollektivvereinbarung

Maßgeblich wird die Zweckbestimmung insbesondere bei der Einwilligung oder der Festlegung in einer Kollektivvereinbarung, bei welchen der Verarbeiter die Zwecke frei angeben kann. Bis auf die oben genannte Bestimmung, dass der Zweck eindeutig und rechtmäßig sein muss, verhält sich die DSGVO nicht zur Frage der Zweckbestimmung. Ebenso wenig hat sich der EuGH bislang dazu geäußert.[822]

Sieht man die Zweckbestimmung – zumindest im Rahmen der Einwilligung – als Ausfluss der informationellen Selbstbestimmung, müsste es strenggenommen, wie *Grafenstein* richtig ausführt, ausreichen, wenn diese in der Allgemeinheit angegeben werden, wenn der Betroffene darüber aufgeklärt ist und dieser weiten Zweckbestimmung zustimmt. Allerdings

---

zahlreiche Vorschriften in der DSGVO, die eine zumindest in Textform vorzunehmende Fixierung des Zwecks erfordern.

819 *Götz*, Big Data im Personalmanagement, S. 126.

820 *Article 29 Data Protection Working Party*, WP 203, S. 16.

821 *Buchner*, 2 Grundsätze des Datenschutzrechts, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 244 Rn. 60.

822 Der EuGH beschäftigte noch unter Geltung der DS-RL mit der Zweckfestlegung, wobei er hierzu jedoch keine näheren Spezifikationen traf, vgl. EuGH, Urt. v. 05.05.2011 – C-543/09, EuZW, 2011, 485 (487 f.) – Deutsche Telekom AG/Deutschland Rn. 64 ff.

kritisiert sie zu Recht, dass Betroffene dann mitunter nicht in der Lage sind, die Folgen richtig abzuschätzen.[823]

Grafenstein spricht sich daher dafür aus, nicht nur die Selbstbestimmung bzw. die Erwartungen des Betroffenen in den Raum zu stellen, sondern „alle verfassungsrechtlich geschützten Risikosphären", also nicht nur die Privatsphäre, sondern auch die allgemeine Handlungsfreiheit und weitere Freiheits- und Gleichheitsrechte.[824] Dies kann jedoch nur insofern gelten, als die Zwecke der Verarbeitung außerhalb der bereits gesetzlich genannten und festgelegten Zwecke liegen, da nur dort ein Spielraum für den Verarbeiter zur Zweckfestlegung besteht. So treffen die Ausführungen ausschließlich auf den Fall der Einwilligung oder der Regelung einer Kollektivvereinbarung zu, denn selbst bei der Verarbeitung im Rahmen von Art. 6 Abs. 1 lit. f DSGVO muss der Zweck der Verarbeitung die Erforderlichkeit zur Wahrung von berechtigten Interessen des Verarbeiters sein.

Da die Einwilligung im Arbeitsverhältnis – zumindest für die hier dargestellten Szenarien – jedoch eine untergeordnete Rolle spielt,[825] wird hierauf an dieser Stelle nicht näher eingegangen. Nicht zuletzt werden Arbeitgeber selbst daran interessiert sein, aufgrund § 26 Abs. 2 S. 2 BDSG eine enge Zweckbestimmung zu treffen, da die Einwilligung im Zweifel nur dann wirksam sein wird, wenn Arbeitnehmer und Arbeitgeber gleichgelagerte Interessen verfolgen. Eine weite Zweckbestimmung würde der Überprüfung der gleichgelagerten Interessen zuwiderlaufen, wobei hier die Überprüfung zu Lasten des Arbeitgebers, der die Daten auf Basis der Einwilligung verarbeiten möchte, ausfallen würde.

Im Rahmen von Betriebsvereinbarungen müssen Arbeitgeber und Betriebsrat aufgrund Art. 88 Abs. 2 DSGVO, § 75 Abs. 2 BetrVG auf eine hinreichend spezifische Zweckbestimmung achten. In der Praxis wird jedoch in aller Regel der Betriebsrat zur Wahrung seiner Mitbestimmungsrechte und zur Sicherung der Überprüfbarkeit der Einhaltung der Betriebsvereinbarung auf eine detaillierte und präzise Zweckbestimmung drängen.

b) § 26 BDSG: Verarbeitung zum Zwecke des Beschäftigungsverhältnisses

§ 26 Abs. 1 BDSG bestimmt, dass eine Verarbeitung von personenbezogenen Daten von Beschäftigten (und gem. Abs. 8 S. 2 auch von Bewerbern)

823 *Grafenstein*, DuD 2015, 789 (793).
824 *Grafenstein*, DuD 2015, 789 (794).
825 Hierzu bereits **D. § 1 III. 2. a**).

für Zwecke des Beschäftigungsverhältnisses verarbeitet werden dürfen, *wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses, für dessen Durchführung oder Beendigung […] erforderlich ist*.

In Konkretisierung der obigen Ausführungen unter **D. § 1 IV. 2. b**) muss an dieser Stelle nunmehr genauer auf die Frage eingegangen werden, wann eine Datenverarbeitung nach § 26 Abs. 1 BDSG zum Zwecke des Beschäftigungsverhältnisses erforderlich ist, insbesondere wie weit die vom Gesetzgeber genannten Zwecke zu verstehen sind.[826]

aa) Erforderlichkeit für die Entscheidung über die Begründung des Beschäftigungsverhältnisses

Der erstgenannte Verarbeitungszweck betrifft insbesondere die in § 26 Abs. 8 S. 2 BDSG genannten Bewerber für ein Beschäftigungsverhältnis. Nach § 26 Abs. 1 S. 1 Var. 1 BDSG ist der Arbeitgeber befugt, personenbezogene Daten dieser Personengruppe zu verarbeiten, wenn dies für seine Entscheidung über die Begründung des Beschäftigungsverhältnisses erforderlich ist.

Angesichts der Formulierung der Norm mag die Vermutung aufkommen, dass der Zweck weit zu verstehen ist und der Arbeitgeber frei bestimmen kann, welche Daten er zur Entscheidung über die Begründung des Beschäftigungsverhältnisses benötigt. Das Kriterium der Erforderlichkeit ist jedoch nicht subjektiv, sondern objektiv zu verstehen.[827] Allerdings darf es gleichfalls nicht im Sinne einer unverzichtbaren Notwendigkeit interpretiert werden. Vielmehr muss es so gelesen werden, dass der Nutzer bei vernünftiger Betrachtung auf die Datenerhebung angewiesen ist.[828] Es kommt darauf an, ob die Wahl einer anderen Datenverarbeitungsmethode oder der Verzicht sinnvoll oder zumutbar wäre, wobei die Organisationsform und Arbeitsweise der datenerhebenden Stelle zugrunde zu legen

826 Die gesetzliche Differenzierung zwischen Begründung, Durchführung und Beendigung wird teilweise in der Literatur als überflüssig bezeichnet, vgl. *Pötters*, in: Gola, Datenschutz-Grundverordnung, Art. 88 DSGVO Rn. 45 Andere wiederum verweisen auf die Wichtigkeit der Zweckbestimmung für die Verhältnismäßigkeitsprüfung, vgl. BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 71.

827 Es hat eine Verhältnismäßigkeitsprüfung stattzufinden, vgl. *Pötters*, in: Gola, Datenschutz-Grundverordnung, Art. 88 DSGVO Rn. 46.

828 OLG Köln, Urt. v. 19.11.2010, BeckRS 2011, 14259 unter II. 1. c) cc) der Gründe.

ist.[829] Bei vielen People-Analytics-Maßnahmen werden die Daten in aller Regel nicht mehr zum Zwecke der Begründung des (konkreten) Beschäftigungsverhältnisses, sondern zur Optimierung von Bewerbungsprozessen eingesetzt, sodass es sich hierbei um einen beschäftigungsfremden Zweck handelt und die Zulässigkeit der Weiterverarbeitung nach Art. 6 Abs. 1 lit. f DSGVO[830] zu prüfen ist.

Insbesondere aufgrund des bestehenden Machtgefälles zwischen Arbeitgeber und Arbeitnehmer in der Bewerbungssituation ist zu beachten, dass die Bewerber keine vollständige Entscheidungsfreiheit haben.[831] Im Zweifel werden sie die Daten dem Arbeitgeber überlassen und sich nicht nur aufgrund einer zu weitgehenden Datenerhebung einen anderen Vertragspartner suchen, zumal oft eine finanzielle Abhängigkeit von diesem Vertrag besteht. Es ist daher eine objektive Überprüfung und Interessenabwägung vorzunehmen.[832]

Gerade in Bewerbungssituationen ist die Gefahr groß, dass Arbeitgeber versuchen, so viel Daten wie möglich über die Bewerber zu sammeln („*Ausforschungsgefahr*"), da zu diesem Zeitpunkt die Bereitwilligkeit, Informationen Preis zu geben, am größten und eine Fehlbesetzung teuer ist. Der Arbeitgeber hat ein großes Interesse daran, ein vollständiges Persönlichkeitsprofil von Bewerbern zu erstellen,[833] nicht zuletzt, weil es sich beim Arbeitsverhältnis um ein Dauerschuldverhältnis mit höchstpersönlichem Charakter (§ 613 S. 1 BGB) handelt.[834]

Die Praxisrelevanz dieser Einschränkung der „Datenerhebungsmacht" zeigt sich an den vielen Entscheidungen des Bundesarbeitsgerichts zum Fragerecht des Arbeitgebers sowie zur Zulässigkeit von psychologischen Untersuchungen an Bewerbern noch unter Geltung des Vorgängergeset-

829 *Wolff*, A. I. Unionsrechtliche Grundlagen, in: Schantz/Wolff, Das neue Datenschutzrecht, S. 32.

830 Ein Rückgriff auf die allgemeinen Erlaubnistatbestände wird in der Literatur überwiegend als zulässig erachtet, vgl. ErfK/*Franzen*, § 26 BDSG Rn. 4 f.; *Kainer/Weber*, BB 2017, 2740 (2743); *Kort*, NZA 2018, 1097 (1099 f.); *Kramer*, NZA 2018, 637 (638); *Ströbel et al.*, CCZ 2018, 14 (19); so wohl auch LAG Hamm, Beschl. v. 19.09.2017 – 7 TaBV 43/17, ZD 2018, 129 (131) Rn. 35; *Kainer/Weber*, BB 2017, 2740 (2741).

831 *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 19.

832 Siehe bereits **D. § 1 I V. 2. b**).

833 Zum Interessenskonflikt im Arbeitsverhältnis, siehe **A. § 2**.

834 Siehe die Kommentierung zum im Wortlaut nahezu identischen § 32 BDSG a.F., *Seifert*, in: Simitis, Bundesdatenschutzgesetz, § 32 BDSG Rn. 21.

zes.[835] Im Kern prüft das BAG hierbei einzelfallbezogen, ob der Arbeitgeber Daten erhebt, an deren Kenntnis er ein „berechtigtes, billigenswertes und schutzbedürftiges Interesse“[836] hat.[837]

Zu beachten sind zwei Dinge, die sich zur bisherigen Rechtslage verändert haben: Erstens: Trotz der Gesetzesbegründung, wonach die zu § 32 BDSG a.F. entwickelten Grundsätze unter § 26 BDSG n.F. fortgelten sollen, ist die Diskussion um das Fragerecht und sonstige Datenerhebungsmaßnahmen nicht mehr unter dem Gesichtspunkt des berechtigten Interesses an der Beantwortung der Frage durch den Bewerber zu führen, sondern am Stichwort der „Erforderlichkeit für die Entscheidung über die Begründung des Beschäftigungsverhältnisses, § 26 Abs. 1 S. 1 Var. 1 BDSG.[838] Der Prüfungsmaßstab der Abwägung verändert sich allerdings nicht,[839] insofern ist inhaltlich die Auffassung des Gesetzgebers richtig. Zweitens: Die Privilegierung von Daten aus „allgemein zugänglichen Quellen“ (§ 28 Abs. 1 S. 1 Nr. 3 BDSG a.F.) ist weggefallen, sodass die Verarbeitung von Daten insbesondere aus dem Internet mitunter nunmehr erhöhten Voraussetzungen unterliegen könnte.[840] Dagegen spricht, dass die DSGVO grundsätzlich keinen ausdrücklichen Vorrang der Direkterhebung mehr kennt[841] und für sensitive Daten eine Verarbeitungserleichterung in Art. 9 Abs. 2 lit. e DSGVO ausdrücklich aufgenommen wurde[842]. Eine solche muss in der Abwägung dann *erst recht* für nicht-sensitive Daten berücksich-

835 Eine Darstellung der Einzelfragen der Datenerhebung würde hier den Rahmen sprengen, sodass auf die unzähligen Spezialbeiträge in der rechtswissenschaftlichen Literatur verwiesen wird. Vgl. daher die ausführliche Kommentierung von *Seifert*, in: Simitis, Bundesdatenschutzgesetz, § 32 BDSG Rn. 22 ff. m.w.N.; ebenso den ausführlichen Aufsatz von *Gola*, RDV 27(3) (2011), 109.

836 *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 22; *Gola*, NZA 2019, 654 (655).

837 Vgl. u.a. BAG, Urt. v. 13.06.2002 – 2 AZR 234/01, NZA 2003, 265 (266).

838 Insofern wurde die sog. „Informationserhebungsfreiheit des Arbeitgebers“ grundsätzlich abgeschafft und durch das allgemeine Verbot des Art. 6 DSGVO ersetzt, vgl. BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 72.

839 *Seifert*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 88 DSGVO Rn. 77 f.

840 So wohl *Schwarz*, ZD 2018, 353 (354).

841 So auch *Däubler*, Digitalisierung und Arbeitsrecht, § 4 Rn. 11 f., der hierdurch zum Ergebnis gelangt, dass die Grenzen des Fragerechts aufgrund eines stärkeren Eingriffs in das Persönlichkeitsrecht weiterhin eingehalten werden müssen.

842 *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 61; ErfK/*Franzen*, § 26 BDSG Rn. 19.

tigt werden. Im Ergebnis gilt also derselbe Maßstab wie unter § 32 Abs. 1 BDSG a.F.[843]

Die Prüfung der „Erforderlichkeit" im Sinne des § 26 Abs. 1 BDSG erfolgt vierstufig: In einem ersten Schritt wird überprüft, ob der Arbeitgeber mit der Datenerhebung/-verarbeitung einen *legitimen Zweck* verfolgt. Im Anschluss daran wird geprüft, ob die Datenverarbeitung zur Erreichung dieses Zwecks auch *geeignet*, also zweckförderlich, ist. Im dritten Schritt wird die *Erforderlichkeit* geprüft, m.a.W., ob es kein milderes und gleich geeignetes Mittel zur Erreichung des Zwecks gibt.[844] Im Anschluss daran wird die *Angemessenheit* oder Verhältnismäßigkeit der Datenverarbeitung geprüft.[845] All diese Punkte erfolgen unter dem (im vorliegenden Fall europarechtlich geprägten[846]) Tatbestandsmerkmal der Erforderlichkeit. Im Rahmen der Abwägung[847] der widerstreitenden (Grundrechts-)Positionen soll versucht werden, praktische Konkordanz zu erreichen, also einen möglichst schonenden Ausgleich unter weitestgehender Berücksichtigung der gegenläufigen Interessen.[848]

Letztlich wird die Eingriffsintensität im Einzelfall geprüft, wobei mögliche Kriterien der Umfang der Verarbeitung, die Anlassbezogenheit, Dauer der Datenverarbeitung, Persönlichkeitsrelevanz der Daten, Verknüpfungsmöglichkeiten sowie mögliche Folgen sein können.[849]

Beispiel: Im Rahmen des Fragerechts des Arbeitgebers wird immer geprüft, ob die Fragen einen Bezug zum konkreten Beschäftigungsverhältnis aufweisen (Anlassbezogenheit) oder dem privaten Bereich zuzuordnen sind. Fragen zur sexuellen Orientierung sind aufgrund der hohen Persönlichkeitsrelevanz unzulässig. Ebenso darf der Arbeitgeber nur so viel Daten

---

843 *Däubler*, Digitalisierung und Arbeitsrecht, § 4 Rn. 12; i.E. ebenso *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 61; ErfK/*Franzen*, § 26 BDSG Rn. 19; wohl auch *Kainer/Weber*, BB 2017, 2740 (2743 f.).

844 *Schwarz*, ZD 2018, 353 (354).

845 *Hamann*, Kapitel 6: Datenschutzrecht, in: Arnold/Günther, Arbeitsrecht 4.0, Rn. 46.

846 *Schwarz*, ZD 2018, 353 (354): Der Begriff der Erforderlichkeit ist unionskonform auszulegen.

847 Kritisch betreffend den Begriff der „Abwägung", *Pötters*, in: Gola, Datenschutz-Grundverordnung, Art. 88 DSGVO Rn. 51.

848 Vgl. BT-Drs. 18/11325, S. 97. Dies ist ein Ausfluss des Verhältnismäßigkeitsgrundsatzes, vgl. *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 21.

849 Beispiele aus *Pötters*, in: Gola, Datenschutz-Grundverordnung, Art. 88 DSGVO Rn. 51 und BeckOK DatenSR/*Wolff*, Syst. A. Prinzipien des Datenschutzrechts 61.1 mit weiteren Beispielen.

über den Arbeitnehmer in Erfahrung bringen, wie er für die Entscheidung des Beschäftigungsverhältnisses benötigt (Umfang der Verarbeitung).

Schlussendlich muss der Arbeitgeber bei einem abgelehnten Bewerber die Daten nach einem bestimmten Zeitraum (Dauer der Datenverarbeitung) wieder löschen, da er dann kein berechtigtes Interesse an der Verarbeitung mehr hat und somit die Interessen des Bewerbers überwiegen. Eine dauerhafte Speicherung würde eine hohe Eingriffsintensität für den Betroffenen darstellen.

Mit einer Spezialfrage, nämlich der Erstellung eines Persönlichkeitsprofils auf Basis der erhobenen Daten durch People-Analytics-Maßnahmen, die sowohl im Bewerbungsprozess, aber auch im weiteren Arbeitsverhältnis stattfinden können, erfolgt nachfolgend bei **E. § 1 II. 4** eine vertiefte Auseinandersetzung. Denn hierbei handelt es sich – wie sich zeigen wird – um einen gesonderten Verarbeitungsvorgang, der einer eigenen Legitimationsgrundlage bedarf.

bb) Erforderlichkeit für die Durchführung des Beschäftigungsverhältnisses

Im Rahmen der Datenverarbeitung zur Durchführung des Beschäftigungsverhältnisses ist die soeben angesprochene Ausforschungsgefahr geringer, da der Arbeitgeber den Arbeitnehmer bereits beschäftigt hat. Die Gefahr, dass der Arbeitnehmer dem Arbeitgeber die Daten freiwillig zur Verfügung stellt, ist ebenso kleiner, da Arbeitnehmer, die bereits in einem Beschäftigungsverhältnis stehen, insofern auch nicht mehr mit anderen Bewerbern konkurrieren müssen. Der Anreiz, die eigenen Daten möglicherweise nur (widerwillig) offenbaren, um sich gegen andere Bewerber durchzusetzen, besteht dort nicht mehr. Zudem genießen die Arbeitnehmer in aller Regel Kündigungsschutz durch das KSchG und können ihre Interessen über das „Instrument" des Betriebsrats weitgehend verteidigen.

Eine Datenverarbeitung für diesen Zweck ist jedenfalls erforderlich, wenn der Arbeitgeber diese zur Erfüllung seiner vertraglichen oder gesetzlichen Pflichten oder Wahrnehmung seiner Rechte zwingend benötigt.[850] Jedoch lassen sich auch weitere Verarbeitungsvorgänge unter diesem Tatbestand legitimieren: Der Tatbestand der „Durchführung" des Arbeitsverhältnisses ist weit zu verstehen, sodass alles erfasst ist, was der Zweckbe-

850 BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 114.

stimmung des Arbeitsverhältnisses dient.[851] Aus diesem Grund fällen auch Verarbeitungsvorgänge im Rahmen von *People-Analytics*-Maßnahmen unter diese Zweckbestimmung, wenn diese dazu dienen, das Arbeitsverhältnis in bestmöglicher Form durchzuführen und die notwendige Entscheidungsdaten in wirtschaftlich sinnvoller Weise gewinnen zu können.[852] Für die Feststellung, ob eine Zweckveränderung vorliegt, ist genau zu prüfen, zu welchem Zweck die Daten ursprünglich erhoben wurden und ob von diesem letztlich auch die weitergehende Analyse der Daten abgedeckt ist.

Bei der Datenerhebung im laufenden Beschäftigungsverhältnis entsteht hierdurch eine neue Gefahr, die mit der Ausforschungsgefahr bei der Begründung vergleichbar ist: Die Gefahr der Überwachung und Vorratsdatenspeicherung. Aufgrund des Charakters als Dauerschuldverhältnis und dem weiterhin grundsätzlich fortbestehenden Interessenskonflikt zwischen Arbeitgeber und Arbeitnehmer sind Arbeitgeber dazu geneigt, ihre Arbeitnehmer möglichst engmaschig zu überwachen, um sicherzustellen, dass sie ihrer arbeitsvertraglichen Pflicht zur Leistung nachkommen.[853] Darüber hinaus fallen über die Dauer eines Arbeitsverhältnisses unzählige (personenbezogene) Daten, meist als Nebenprodukte der Arbeitsleistung, an. Diese können – aus rein technischer Sicht – einfach für Auswertungen genutzt werden.

Vor diesem Hintergrund wird es auch verständlich, dass Arbeitgeber dazu neigen, nicht nur Daten zu erheben, die aktuell benötigt werden, sondern auch welche, die in einer prospektiven Betrachtung möglicherweise von Nutzen sein können. Für die Beurteilung der Zulässigkeit muss daher exakt zwischen erforderlicher Datenverarbeitung und unzulässiger Vorratsdatenspeicherung unterschieden werden.[854] Grundsätzlich ist ein berechtigtes Interesse des Arbeitgebers anzuerkennen, für die Personalplanung und -entwicklung Daten von Arbeitnehmern über einen gewissen Zeitraum zu sammeln, um Veränderungen Rechnung tragen

851 *Zöll*, in: Taeger/Gabel, DSGVO - BDSG, § 26 BDSG Rn. 38.

852 Vgl. MHdB-ArbR/*Reichold*, § 96 Datenschutz im Arbeitsverhältnis, Rn. 46 zur Einführung eines Personalinformationssystems unter Verweis auf BAG, Beschl. v. 11.03.1986 – 1 ABR 12/84, AP BetrVG 1972 § 87 Überwachung Nr. 14; a.A. *Götz*, Big Data im Personalmanagement, S. 61 f.: People Analytics im laufenden Beschäftigungsverhältnis fallen nicht unter die Vorschrift, da sie nicht unmittelbar für den Vollzug des Arbeitsverhältnisses benötigt werden.

853 Hierzu bereits **A. § 2 II.**

854 Zu § 32 BDSG a.F.: *Seifert*, in: Simitis, Bundesdatenschutzgesetz, § 32 BDSG Rn. 57.

zu können.[855] Allerdings darf dies nicht als „Blankoermächtigung" zur Datensammlung verstanden werden.[856] Das datenschutzrechtliche Gebot der Datenminimierung (Art. 5 Abs. 1 lit. b und c DSGVO) gilt auch im Arbeitsverhältnis.[857]

Zu beachten ist ferner, dass die Datenverarbeitung einen Beschäftigungsbezug aufweisen muss. Daten, die der Privatsphäre des Beschäftigten zuzuordnen sind, können deshalb nicht unter dem Zweck „Durchführung des Beschäftigungsverhältnisses" verarbeitet werden. Prominente Beispiele sind Angaben zu Freizeitbeschäftigungen, Hobbys, persönliche Interessen, aber auch Konsumverhalten etc.[858]

Ob ein bestimmtes Datum erhoben und verarbeitet werden darf, muss im Einzelfall anhand der unter **aa**) genannten Kriterien überprüft werden; eine Generalisierung ist hierbei nicht möglich.

cc) Erforderlichkeit für die Beendigung des Beschäftigungsverhältnisses

Unter Beendigung des Beschäftigungsverhältnisses ist die Vorbereitung, Durchführung und Abwicklung zu verstehen.[859] Hier sind in den meisten Fällen keine neuen Daten mehr zu erheben, es sei denn, dass ein Straftatverdacht vorliegt (§ 26 Abs. 1 S. 2 BDSG) und der Arbeitgeber noch die notwendigen Beweise benötigt, um eine Kündigung darauf zu stützen.

In aller Regel können aber bereits bestehende Daten nochmals genutzt werden, wenn ein Arbeitsverhältnis betriebs-, verhaltens- oder personenbedingt beendet wird. So werden bestimmte Daten zur Sozialauswahl nach § 1 Abs. 3 S. 1 KSchG benötigt.[860] Die Prüfung der Erforderlichkeit ist analog der Begründung und Durchführung durchzuführen. Für die Zweckänderung ist § 24 BDSG von besonderer Bedeutung (hierzu unten **E. § 1 I. 3**).

855 Hierzu auch BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 117.
856 *Seifert*, in: Simitis, Bundesdatenschutzgesetz, § 32 BDSG Rn. 58.
857 BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 67.
858 *Seifert*, in: Simitis, Bundesdatenschutzgesetz, § 32 BDSG Rn. 59 f.
859 Vgl. hierzu BT-Drs. 16/13657, S. 21.
860 BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 189; ausführlich *Seifert*, in: Simitis, Bundesdatenschutzgesetz, § 32 BDSG Rn. 135 ff.

dd) Zwischenergebnis

Die möglichen Zweckbestimmungen des § 26 BDSG sind weitreichend. Allerdings sind diese – wie sich bereits aus dem Wortlaut der Norm ergibt – auf das konkrete Beschäftigungsverhältnis bezogen. Es muss also immer am konkreten Arbeitsverhältnis geprüft werden, ob eine Erhebung und Verarbeitung der Daten notwendig ist, um über *dieses* Beschäftigungsverhältnis zu entscheiden, es durchzuführen oder abzuwickeln.[861] Weitergehende Analysen beispielsweise zur Berechnung des zukünftigen Personalbedarfs oder der Fluktuationsquote für bestimmte Stellen, Abteilungen oder des Unternehmens sind vom ursprünglichen Erhebungszweck grundsätzlich nicht gedeckt und lassen sich nicht unter die Zweckbestimmungen des § 26 BDSG fassen.[862] Hier gilt Art. 6 Abs. 1 lit. f DSGVO. Lediglich im Rahmen der Personalplanung und -entwicklung könnte die Zweckbestimmung weitergehende Analysen erfassen, sofern es um die Einsatzplanung und Entwicklung des konkreten Mitarbeiters geht.[863]

2. Vereinbarkeit des weitergehenden Verarbeitungszwecks mit dem ursprünglichen Zweck (Art. 6 Abs. 4 DSGVO)

Für *Analytics*-Maßnahmen, die auf personenbezogenen Daten basieren, die für einen anderen Zweck erhoben wurden, ist daher eine Zweckvereinbarkeitsprüfung anhand der oben aufgeführten Kriterien nach Art. 6 Abs. 4 DSGVO vorzunehmen. Zu beachten ist hierbei, dass die dort genannten Prüfungspunkte nicht abschließend und sehr vage sind, was eine praktische Anwendung schwierig macht.[864]

861 So bereits zu § 28 BDSG a.F. *Lambrich/Cahlik*, RDV 2002, 287 (290).
862 So wohl auch *Hamann*, Kapitel 6: Datenschutzrecht, in: Arnold/Günther, Arbeitsrecht 4.0, Rn. 55.
863 Zustimmend für Leistungsdaten unter altem Datenschutzrecht *Lambrich/Cahlik*, RDV 2002, 287 (290 f.).
864 *Hamann*, Kapitel 6: Datenschutzrecht, in: Arnold/Günther, Arbeitsrecht 4.0, Rn. 55 f.

a) Notwendigkeit einer Rechtsgrundlage für die Weiterverarbeitung

Neben der Zweckvereinbarkeitsprüfung benötigt es einen Erlaubnistatbestand,[865] da es sich bei der Weiterverarbeitung der personenbezogenen Daten um einen eigenen, gesondert zu beurteilenden Verarbeitungsvorgang handelt. Hiervon scheint Erwägungsgrund 50 S. 2 eine Ausnahme zu machen: Wenn die Verarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, soll keine andere gesonderte Rechtsgrundlage erforderlich sein als diejenige für die Erhebung der personenbezogenen Daten.

Überwiegend wird aufgrund Erwägungsgrund 50 in der Literatur argumentiert, dass angesichts des klaren Wortlauts keine neue Rechtsgrundlage für die Verarbeitung erforderlich sei; die Zweckvereinbarkeit also die Weiterverarbeitung ohne (erneute) Legitimation erlaube.[866] Als Argument wird die Systematik von Art. 5 Abs. 1 lit. b DSGVO und Art. 6 Abs. 4 DSGVO angegeben, denn Art. 6 Abs. 4 setzte deutlich voraus, dass eine Rechtsgrundlage für die Verarbeitung zu geänderten Zwecken nicht vorliege und formuliere dann die Voraussetzungen, wonach eine Verarbeitung dennoch möglich ist.[867] Zudem handle es sich um eine Weiterverarbeitung und nicht um eine neue Verarbeitung, weshalb diese keiner neuen legitimierenden Grundlage bedürfe.[868] Bei einem anderen Verständnis bliebe für Art. 6 Abs. 4 kein Anwendungsbereich mehr.[869]

---

865 *Franzen*, EuZA 2017, 313 (326 f.).

866 *Franzen*, EuZA 2017, 313 (327); *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 340; *Kühling/Martini*, EuZW, 448 (451); *Spindler*, DB 2016, 937 (943); HK DSGVO/BDSG (2018)/*Schwartmann*, Art. 6 DSGVO Rn. 186; *Eichenhofer*, PinG 2017, 135 (139); *Monreal*, ZD 2016, 507 (510); *Richter*, DuD 2016, 581 (584); *Roßnagel et al.*, Datenschutzrecht 2016 - "smart" genug für die Zukunft?, S. 158; *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, S. 210; einschränkend *Spindler/Dalby*, in: Spindler/Schuster, Recht der elektronischen Medien, Art. 6 DS-GVO Rn. 22: Der Verantwortliche wird nicht davon entbunden, alle Rechtmäßigkeitsanforderungen der ursprünglichen Verarbeitung einzuhalten wie beispielsweise mindestens eine Bedingung der Rechtmäßigkeit nach Art. 6 Abs. 1 lit. a-e.; wohl auch Plath/*Plath*, Art. 6 DSGVO Rn. 133; nunmehr hiergegen HK DSGVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Abs. 4 DSGVO Rn. 235.

867 *Franzen*, EuZA 2017, 313 (327).

868 *Monreal*, ZD 2016, 507 (510).

869 HK DSGVO/BDSG (2018)/*Schwartmann*, Art. 6 DSGVO Rn. 186; HK DSGVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Abs. 4 DSGVO Rn. 235: Art. 6 Abs. 4 DSGVO ist eine Auslegungsregel über die Zulässigkeit der Zweckänderung.

Dagegen wird argumentiert, dass im Rahmen der Zweckvereinbarkeit grundsätzlich eine *zweistufige* Prüfung erfolge, nämlich zunächst (1) eine Prüfung, ob der neue Zweck mit dem ursprünglichen Zweck vereinbar und damit für den Betroffenen weiter vorhersehbar ist und ferner (2) ob für die weitergehende Weiterverarbeitung eine Rechtsgrundlage bestehe.[870] Aus Art. 5 Abs. 1 lit. a DSGVO folge nichts anderes, denn die Norm verankere die Zweckbindung und stelle keinen Erlaubnistatbestand dar; Erwägungsgrund 50 stelle lediglich klar, dass die Verarbeitung ebenfalls auf die ursprüngliche Rechtsgrundlage gestützt werden könne und ein „gesonderter" Legitimationstatbestand nicht zwingend notwendig ist.[871] Bei Erwägungsgrund 50 handle es sich im Übrigen um ein Redaktionsversehen[872], welches aus den Trilog-Verhandlungen herrühre, da die Kommission und der Rat in größerem Umfang als unter der DS-RL Datenverarbeitungen erlauben wollten,[873] sich jedoch gegenüber der strikteren Auffassung des Parlaments nicht haben durchsetzen können.[874] Eine andere Auffassung wäre zudem „kaum" mit Art. 7 und 8 EU-GRC vereinbar.[875]

Die überwiegende Literaturauffassung überzeugt aus mehreren Gründen nicht: Zunächst spricht Erwägungsgrund 50 immer wieder von der „Erhebung" der Daten. Dies ist auch stimmig, denn bei einer zulässigen (zweckvereinbaren) Weiterverarbeitung kann auf die unter anderem Zweck erhobenen Daten zurückgegriffen werden, ohne diese zuerst wieder neu erheben zu müssen. Somit können sich Verarbeiter die erneute Erhebung beim Betroffenen sparen. Keinesfalls kann die Regelung des

---

870 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 76 Rn. 53 f.; *Schantz*, NJW 2016, 1841 (1844); *Albrecht*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 DSGVO Rn. 12; *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 183; Ehmann/Selmayr/*Heberlein*, Art. 6 DSGVO Rn. 53; Sydow/*Reimer*, Art. 6 DSGVO S. 69; *DSK*, Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO, <www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/12/20191209_Erfahrungsbericht-zur-Anwendung-der-DS-GVO.pdf>, S. 13 f.

871 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 76 Rn. 54.

872 A.A. *Monreal*, ZD 2016, 507 (510): Wer Erwägungsgrund 50 als redaktionellen Fehler werte, verkenne das europäische Verständnis des Begriffs der Verarbeitung.

873 Siehe hierzu *Albrecht*, CR 2016, 88 (92); a.A. *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 3: *„Der Vorschlag des Rates zur Rechtfertigung der Zweckänderung in seinem Abs. 4 wurde in die DSGVO dagegen nicht übernommen. Eine Erläuterung der Vorschrift findet sich in EG 50."*

874 *Schantz*, NJW 2016, 1841 (1844).

875 *Schantz*, NJW 2016, 1841 (1844).

Art. 6 Abs. 4 DSGVO jedoch eine Abweichung des Grundsatzes in Abs. 1 darstellen.[876] Auch in systematischer Hinsicht baut Abs. 4 auf Abs. 1 auf.[877] Folgte man der erstgenannten Auffassung, so wäre auch der Grundsatz der Rechtmäßigkeit der Datenverarbeitung ausgehoben. Dies hätte beispielsweise im Arbeitsverhältnis zur Folge, dass Daten, die zunächst für die Zwecke der Begründung des Arbeitsverhältnisses erforderlich waren, ohne jegliche weitere Erforderlichkeitsprüfung weiterverarbeitet werden könnten, sobald Zweckvereinbarkeit bestünde. Dies stünde nicht im Einklang mit dem datenschutzrechtlichen Erlaubnisvorbehalt aus Art. 8 Abs. 1 S. 1 EU-GRC. Letztlich spricht für die Notwendigkeit einer weiteren Legitimationsgrundlage auch der Wortlaut des Art. 6 Abs. 1 DSGVO, wonach eine Datenverarbeitung *nur* zulässig ist, wenn eine der dort genannten Bedingungen einschlägig ist. Weder Abs. 1 noch Abs. 4 machen hiervon eine Ausnahme.[878] Auch das teilweise vorgebrachte Argument, dass Art. 5 Abs. 1 lit. b DSGVO ein genau solches Verständnis voraussetze,[879] überzeugt bei näherer Betrachtung nicht: Art. 5 Abs. 1 lit. b DSGVO spricht von einer Zulässigkeit der *Weiter*verarbeitung bei Zweckvereinbarkeit. Liegt eine Zweckvereinbarkeit im Sinne von Art. 6 Abs. 4 DSGVO nicht vor, so ist es nicht zulässig, die bereits erhobenen Daten weiterzuverarbeiten. Stattdessen muss ein komplett neuer Datenverarbeitungsprozess (inklusive Datenerhebung) gestartet werden.[880] Insofern hat Art. 6 Abs. 4 DSGVO auch bei engerem Verständnis noch einen bedeutenden Anwendungsbereich. Für die Gegenauffassung könnte lediglich die etwas missglückte Formulierung der Art. 13 Abs. 3 und Art. 14 Abs. 4 DSGVO sprechen, wonach bei einer Zweckveränderung vor der Weiterverarbeitung *Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen […] zur Verfügung* zu stellen sind. Dies ließe sich so interpretieren, dass eine veränderte Rechtsgrundlage gerade nicht bestehe, da im Gegensatz Art. 13 Abs. 1 lit. c und Art. 14 Abs. 1 lit. c DSGVO die Rechtsgrundlage explizit aufführen. Die Verpflichtung zur Information fehlt al-

876 *Albrecht*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 DSGVO Rn. 13; im Ergebnis wohl auch *Spindler/Dalby*, in: Spindler/Schuster, Recht der elektronischen Medien, Art. 6 DS-GVO Rn. 22.

877 Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 19.

878 *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 183.

879 *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, S. 210.

880 *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 185.

lerdings auch bei der Auskunft nach Art. 15 Abs. 1 lit. a DSGVO, obwohl kein überzeugender Grund hierfür ersichtlich ist und ein legitimes Interesse des Betroffenen besteht, zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung auch diese Information zu erlangen.[881] Insofern darf dem fehlenden Verweis nicht zu viel Aussagekraft beigemessen werden. Bei einer veränderten Rechtsgrundlage wäre daher auch nach Art. 13 f. DSGVO darüber zu informieren.[882]

Letztlich führt die Gegenauffassung auch zu Folgeproblemen, wenn der ursprüngliche (Erhebungs-)Zweck und der Weiterverarbeitungszweck nicht mehr kohärent sind: Unklar sind die Anforderungen an die Datenerhebung, die Pflichten des Verantwortlichen sowie die Rechte der Betroffenen.[883]

Im Ergebnis ist also festzuhalten, dass bei Zweckvereinbarkeit die Daten weiterverarbeitet werden dürfen, wenn für die weitere Verarbeitung die Rechtmäßigkeitsvoraussetzungen des Art. 6 Abs. 1 DSGVO oder § 26 Abs. 1 BDSG vorliegen.[884] Nicht in jedem Fall ist eine andere Legitimationsgrundlage erforderlich, beispielsweise dann, wenn es sich um eine mit dem ursprünglichen Zweck vereinbare, erforderliche Datenverarbeitung im Rahmen der Vertragsdurchführung handelt.[885] So können beispielsweise Daten im Rahmen des Vertragsschlusses erhoben worden sein, ebenso aber für die Durchführung erforderlich sein. In diesem Fall bedarf es dann keiner anderen Rechtsgrundlage als Art. 6 Abs. 1 lit. b DSGVO oder im Arbeitsverhältnis § 26 Abs. 1 BDSG. In jedem Falle ist der Betroffene nach Maßgabe der Art. 13 Abs. 3 sowie Art. 14 Abs. 4 DSGVO zu informieren. Im „Erfahrungsbericht der unabhängigen Datenschutzbehörden des Bundes und der Länder zur Anwendung der DS-GVO“ (2019) wird sogar eine Streichung des Erwägungsgrund 50 S. 2 DSGVO empfohlen sowie eine

881 *Bäcker*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 15 DSGVO Rn. 13.

882 *Dix*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 15 DSGVO Rn. 21.

883 Wie *Roßnagel* richtigerweise feststellt, sich dennoch aber der Gegenauffassung anschließt und die Lösung dieser Probleme geschickt umgeht, indem er argumentiert, dass es an der Zweckvereinbarkeit fehle, wenn die Probleme nicht gelöst werden könnten, vgl. *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 13, 64.

884 So auch Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 17, 19.

885 Bzw. den mit der Erhebung begonnen Verarbeitungsvorgang fortsetzt, vgl. Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 20.

weitere Klarstellung in Art. 6 Abs. 4.[886] In diesem Rahmen sollten auch die Art. 13 Abs. 3, 14 Abs. 3 DSGVO angepasst werden.

b) Grundlegendes

Die nicht-abschließend aufgezählten Kriterien des Kompatibilitätstests in Art. 6 Abs. 4 DSGVO („*unter anderem*“) werden als „bewegliches System“[887] angewendet, d.h. je mehr Kriterien erfüllt sind, desto eher wird eine zweckverändernde Verarbeitung zulässig sein.

Unabhängig des Kompatibilitätstests ist eine zweckändernde Verarbeitung zulässig, wenn sie auf der Einwilligung („*Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurde, nicht auf der Einwilligung…*“) oder einer entsprechenden mitgliedsstaatlichen oder unionalen Vorschrift[888] (in Deutschland: §§ 23 f. BDSG) beruht.

c) Vermutung der Zweckvereinbarkeit für (anonymisierte) People-Analytics

Eine unwiderlegliche[889] Vermutung zur Zweckvereinbarkeit ist in Art. 5 Abs. 1 lit. b DSGVO festgeschrieben. In der Literatur herrscht Uneinigkeit darüber, ob diese Vermutung unwiderleglich ist. Ein Teil bejaht dies,[890] ohne jedoch hierfür eine nähere Begründung zu liefern. Wiederum ande-

886 *DSK*, Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO, <www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/12/20191209_Erfahrungsbericht-zur-Anwendung-der-DS-GVO.pdf>, S. 14.

887 *Franzen*, EuZA 2017, 313 (327).

888 Art. 6 Abs. 4 DSGVO stellt hierbei keine Öffnungsklausel dar; hierzu und den Anforderungen an solche Vorschriften, vgl. *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 180, 199 f.; a.A. *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 2: „*Abs. 4 enthält im ersten Satzteil eine Öffnungsklausel[…]*“; ausführlich in Rn. 18.

889 *Schantz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 1 DSGVO Rn. 93; Sydow/*Reimer*, Art. 5 DSGVO Rn. 27; a.A. *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 5 DSGVO Rn. 109.

890 *Schantz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 1 DSGVO Rn. 93; Sydow/*Reimer*, Art. 6 DSGVO Rn. 27; unklar *Eichenhofer*,

re lehnen dies ab[891] und führen als Argument den Verweis auf Art. 89 Abs. 1 DSGVO, wonach geeignete Garantien vorzusehen sind. Zudem werde durch die umständliche doppelte Verneinung klargestellt, dass im Einzelfall ein Kompatibilitätstest nach den Kriterien des Art. 6 Abs. 4 DSGVO notwendig sei; im Regelfall dürfte jedoch von einer Vereinbarkeit ausgegangen werden.[892] Gegen letztgenannte Literaturauffassung spricht allerdings ein Vergleich mit der Vorgängernorm Art. 6 Abs. 1 lit. b DS-RL: Hiernach war die Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken *im Allgemeinen* nicht als unvereinbar mit den Zwecken der vorausgehenden Datenerhebung anzusehen, sofern die Mitgliedsstaaten geeignete Garantien vorsehen. Diese Einschränkung hat Art. 5 Abs. 1 lit. b DSGVO nicht mehr: Dort heißt es, dass eine Weiterverarbeitung für die genannten Zwecke als nicht unvereinbar *gilt*. Insofern ist der Wortlaut – entgegen den kritischen Literaturstimmen[893] – klar: Es handelt sich hier – sofern die Voraussetzungen des Art. 89 Abs. 1 DSGVO eingehalten wurden – um eine unwiderlegliche Vermutung („Fiktion") der Zweckvereinbarkeit.

Zurückgeführt werden kann die Ausnahme vom Zweckbindungsgrundsatz wohl auf das *Volkszählungsurteil* des (deutschen) BVerfG, das bereits 1983 festgestellt hat, dass bei der Datenerhebung für statistische Zwecke eine enge und konkrete Zweckbindung der Daten nicht verlangt werden könne: „*Es gehört zum Wesen der Statistik, dass die Daten nach ihrer statistischen Aufbereitung für die verschiedensten, nicht von vornherein bestimmbaren Aufgaben verwendet werden dürfen; demgemäß besteht auch ein Bedürfnis nach Vorratsdatenspeicherung*"[894].

PinG 2017, 135 (140): Bereichsausnahme; noch zur Datenschutzrichtlinie *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, Art. 6 Rn. 16 ff.

891 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 5 DSGVO Rn. 109; Paal/Pauly/*Frenzel*, Art. 5 DSGVO Rn. 32 f.; Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 17.

892 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 5 DSGVO Rn. 109.

893 Vgl. *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 5 DSGVO Rn. 109: „*Der Rechtsgehalt der Fiktion der Nichtunvereinbarkeit ergibt sich nicht aus dem Wortlaut der Vorschrift.*".

894 BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1 (47) – Volkszählungsurteil Rn. 166.

Als Ausnahme vom Zweckbindungsgrundsatz ist diese Norm allerdings eng auszulegen.[895] Wie sich aus den Erwägungsgründen 156 ff. ergibt, gelten hierbei strenge Voraussetzungen. So sollen bereits nach Erwägungsgrund 156 S. 4 die Mitgliedsstaaten geeignete Garantien für die Verarbeitung zu den genannten Zwecken vorsehen. Die Verarbeitung zu wissenschaftlichen Forschungszwecken soll gem. Erwägungsgrund 159 „weit" ausgelegt werden, wobei als Beispiele die technologische Entwicklung und Demonstration, die Grundlagenforschung, die angewandte Forschung sowie die privat finanzierte Forschung genannt werden. Wie sich in Erwägungsgrund 157 zeigt, muss die Forschung allerdings dem Gemeinwohl dienen und soll u.a. die Wissensbasis für politische Entscheidung sichern, sodass unternehmerische bzw. private (Optimierungs-)Zwecke im Rahmen von *People Analytics* nicht von dieser Ausnahme erfasst sind.[896]

Bei der Verarbeitung zu statistischen Zwecken beschreibt Erwägungsgrund 162, dass unter dem Begriff „statistische Zwecke" jeder für die Durchführung statistischer Untersuchungen und die Erstellung statistischer Ergebnisse erforderliche Vorgang der Erhebung und Verarbeitung zu verstehen ist, wobei die Ergebnisse für verschiedene Zwecke verwendet werden können.[897] Allerdings sollte das Unionsrecht oder das Recht der Mitgliedsstaaten den statistischen Inhalt, die Zugangskontrolle, die Spezifikationen für die Verarbeitung personenbezogener Daten zu statistischen Zwecken und geeignete Maßnahmen zur Sicherung der Rechte und Freiheiten der betroffenen Personen und zur Sicherstellung der statistischen Geheimhaltung bestimmen. Hierbei dürfen die Ergebnisse keine personenbezogenen Daten, sondern allenfalls aggregierte Daten sein und die Daten bzw. Ergebnisse nicht für Maßnahmen oder Entscheidungen gegenüber einzelnen natürlichen Personen verwendet werden.

Nach Art. 89 Abs. 1 DSGVO kann die *Pseudonymisierung* eine geeignete Verarbeitungsgarantie darstellen, wenn es möglich ist, die Zwecke hierdurch (noch) zu erfüllen. Die Daten müssen *anonymisiert* werden, wenn dies die Zweckerfüllung nicht beeinträchtigt.[898] Dies entspricht in etwa

---

895 *Buchner*, DuD 2016, 155 (157); *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 341; *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 5 DSGVO Rn. 109.

896 *Richter*, DuD 2016, 581 (584).

897 So wurde bereits zur identischen Formulierung in Art. 6 Abs. 1 lit. b DS-RL von der Artikel-29-Datenschutzgruppe vertreten, dass auch kommerzielle Zwecke davon erfasst werden, vgl. *Article 29 Data Protection Working Party*, WP 203, S. 29.

898 Vgl. hierzu auch *Richter*, DuD 2016, 581 (584).

den Garantien aus dem Kompatibilitätstest aus Art. 6 Abs. 4 lit. e DSGVO, wobei die Regelung des Art. 89 Abs. 1 DSGVO wohl strenger zu verstehen sein dürfte, da hier eine Anonymisierung grundsätzlich verpflichtend ist.

Es wird vereinzelt vertreten, dass Big-Data-Analysen nicht als „Statistik" privilegiert würden.[899] Diese Auffassung ist allerdings zu pauschal ablehnend. Zwar ist es korrekt, dass es keinesfalls für die Inanspruchnahme dieser Ausnahme ausreicht, dass die eingesetzten Verfahren lediglich statistischer oder wissenschaftlicher Natur sind.[900] Kommerzielle Anwendungen sind durch die Ausnahme dennoch nicht ausgeschlossen, wie ein Vergleich mit der im Wortlaut identischen Vorgängerregelung sowie die Formulierung von Erwägungsgrund 162 zeigt. Die Ausnahme vom Zweckbindungsgrundsatz war bereits in Art. 6 Abs. 1 lit. b sowie in Erwägungsgrund 29 der DS-RL geregelt. Hierzu nahm die Artikel-29-Datenschutzgruppe Stellung und verdeutlichte, dass auch kommerzielle Zwecke (wie beispielsweise Big-Data-Auswertungen im Rahmen von Marketing-Zwecken) hierunter fallen können.[901]

Für Profiling- und Scoring-Verfahren im Rahmen von *People Analytics* ist die Ausnahme dennoch irrelevant[902], da die Ergebnisse der Verarbeitung weder personenbezogene Daten sein dürfen noch für Maßnahmen oder Entscheidungen gegenüber einzelnen natürlichen Personen verwendet werden dürfen, wie Erwägungsgrund 162 S. 5 bestimmt.

Dies spricht im Übrigen auch dafür, die Ausnahme der „Statistik" nicht zu eng auszulegen, da die von der Gegenauffassung angesprochenen Gefahren lediglich dann greifen, wenn einerseits die Ergebnisse auf Einzel-

899 So *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 342; *Buchner*, 2 Grundsätze des Datenschutzrechts, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 244 Rn. 61; *Götz*, Big Data im Personalmanagement, S. 130; *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, S. 211 unter zweifelhaftem Verweis auf die Kommissionsbegründung zur DS-RL; wohl auch Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 17: Kein Einfallstor für "Big Data"-Analysen.

900 *Buchner*, DuD 2016, 155; *Buchner*, 2 Grundsätze des Datenschutzrechts, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 244 Rn. 61.

901 *Article 29 Data Protection Working Party*, WP 203, S. 29; kritisch *Richter*, DuD 2015, 735 (738); ebenso *Skistims*, 8.2 Rechtsgrundlagen für datenverarbeitende KI, in: Kaulartz/Ammann/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, Rn. 62.

902 Insofern ist Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 17. zuzustimmen.

personen angewandt werden[903] und andererseits der – wie aufgezeigt – nicht überzeugenden Auffassung gefolgt wird, dass es bei einer Zweckvereinbarkeit die Weiterverarbeitung der personenbezogenen Daten keiner Rechtsgrundlage mehr bedarf. Da die Weiterverarbeitung der Daten jedoch weiterhin einer Legitimation bedarf, ist in diesem Rahmen ohnehin immer das Vorliegen einer Einwilligung oder eine andere Notwendigkeit der Nutzung personenbezogener Daten für die Erstellung derartiger Statistiken erforderlich, sodass auch durch die Ausnahme vom Zweckbindungsgrundsatz keine unbegrenzten Analysen stattfinden dürfen. Für öffentliche Statistiken wird die Legitimation in aller Regel in Art. 6 Abs. 1 lit. e DSGVO liegen. Bei Statistiken im Privatsektor bzw. für kommerzielle Zwecke wird Art. 6 Abs. 1 lit. f DSGVO die einschlägige Norm zur Überprüfung der Rechtmäßigkeit sein, da solch anonyme Analysen in aller Regel nicht zur Vertragsdurchführung erforderlich sind (Art. 6 Abs. 1 lit. e DSGVO bzw. § 26 Abs. 1 BDSG).

People Analytics-Verfahren, die allerdings darauf zielen, bestimmte Kennzahlen im Unternehmen zu ermitteln und deren Ergebnisse somit anonyme Daten darstellen, unterliegen der Ausnahme vom Zweckbindungsgrundsatz. Im Ergebnis dürfen daher die personenbezogenen Daten, soweit ein Legitimationsgrund für die Anonymisierung für statistische *People Analytics*-Verfahren besteht, weiterverarbeitet werden.

d) Kriterien des Kompatibilitätstests

Für die genannten Beispiele des *Profiling* und *Scoring* gilt die Vermutung der Zweckvereinbarkeit im Rahmen der „Statistik-Regelung" nicht, sodass für solche Verarbeitungsvorgänge der Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO vorgenommen werden muss, wenn die Daten zu einem anderen Zweck erhoben wurden. Die oben genannten Kriterien der Zweckvereinbarkeit müssen daher einer genauen Analyse unterzogen werden.

903 Vgl. zum Risiko „tiefgehender Einblicke in einzelne Persönlichkeiten" bei einer Ausnahme für kommerzielle Big-Data-Anwendungen *Götz*, Big Data im Personalmanagement, S. 130

aa) Verbindung zwischen den Zwecken der Erhebung und der Weiterverarbeitung (lit. a)

Als erstes Kriterium der Komptabilitätsprüfung nennt Art. 6 Abs. 4 lit. a DSGVO die Verbindung zwischen den Zwecken der Erhebung und der Weiterverarbeitung. In diesem Rahmen muss vor allem der Inhalt der Beziehung zwischen dem Ursprungszweck und dem Weiterverarbeitungszweck betrachtet werden.[904] Insbesondere, wenn die ursprüngliche Verarbeitung bereits die Weiterverarbeitung impliziert oder als nächster logischer Schritt angesehen werden kann, ist dieses Kriterium als erfüllt anzusehen. Hieraus darf jedoch nicht der Gegenschluss gezogen werden, dass bei einem „Missing-Link" eine Weiterverarbeitung nie zulässig wäre.[905]

Zur Beurteilung kann folgende Faustregel angewandt werden: Je kleiner die inhaltliche Distanz zwischen dem ursprünglichen Erhebungs- und dem weitergehenden Verarbeitungszweck ist, desto eher ist von einer Zweckvereinbarkeit auszugehen.[906] Hintergrund ist, dass der Betroffene dann mit der Verarbeitung rechnen und dies gegebenenfalls bei der Entscheidung, die Verarbeitung im ersten Schritt zu erlauben, berücksichtigen kann.[907]

Roßnagel nennt hier einige Beispiele[908]: So soll es zweckvereinbar sein, wenn die Daten der Kunden beispielsweise bei einem entsprechenden Vertrag für selbstlernende Systeme wie Smart Home oder Smart Car weiterverwendet werden, um sich besser an seine Gewohnheiten und Präferenzen anzupassen. Das gleiche gelte bei Social Networks. Etwas anderes gelte allerdings, wenn der Verarbeiter den kommerziellen Wert der Daten ausnutze. Als Beispiel hierfür kann der Verkauf dieser Datensätze z.B. zu Werbezwecken genannt werden.

Für People Analytics kann eine Zweckvereinbarkeit auch im Rahmen von Profiling oder Scoring-Maßnahmen vorliegen, wenn die Daten zum Zwecke der Durchführung des Beschäftigungsverhältnisses erhoben wur-

---

904 *Article 29 Data Protection Working Party,* WP 203, S. 23.

905 So aber *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 36; wie hier *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 205 unter Bezugnahme auf das WP 203.

906 *Article 29 Data Protection Working Party,* WP 203, S. 24.

907 *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 187; ebenso *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 36.

908 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 37 ff.

den. Hier hängt der durch People Analytics verfolgte Zweck der Weiterverarbeitung (Optimierung der Betriebsabläufe, Verbesserung des Betriebsklimas etc.) eng mit dem ursprünglichen Erhebungszweck zusammen, sodass dieses Kriterium grundsätzlich als erfüllt angesehen werden kann.

bb) Zusammenhang, in welchem die Daten erhoben wurden (lit. b)

Als weiteres Kriterium wird der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen genannt. Erwägungsgrund 50 ergänzt das erste und das zweite Kriterium dahingehend, dass es auf die *„vernünftigen Erwartungen der betroffenen Person […] in Bezug auf die weitere Verwendung der Daten*“ ankomme, also die Sichtweise des Betroffenen eine maßgebliche Rolle spiele.[909] Erforderlich ist letztlich eine Gesamtbetrachtung der Beziehung, wobei es insbesondere auf die ursprüngliche Verarbeitungssituation ankommt: Je enger und restriktiver die Verarbeitung im Rahmen der Erhebung war, desto enger sind die Grenzen der Weiterverarbeitung.[910]

Eine fehlende Vertragsbeziehung zum Verantwortlichen spricht grundsätzlich gegen eine Zweckvereinbarkeit der Weiterverarbeitung, da es gerade auf diese (Vertrauens-)Beziehung zwischen Verantwortlichem und Betroffenen ankommt.[911] Ebenso wird bei einem langjährigen Vertrauensverhältnis in aller Regel eine Verarbeitung in Form einer Übermittlung an Dritte ausgeschlossen sein.[912]

Des Weiteren ist eine gegenseitige Abhängigkeit entscheidend, insbesondere, ob ein Gleichgewicht der Entscheidungsfreiheit herrscht.[913] Wenn die Betroffenen (faktisch) gezwungen sind, die Daten zu offenbaren, spricht dies eher gegen eine Zweckvereinbarkeit unter diesem Gesichts-

909 *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 188.
910 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 306; *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 188.
911 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 45; Paal/Pauly/*Frenzel*, Art. 6 DSGVO Rn. 49.
912 Paal/Pauly/*Frenzel*, Art. 6 DSGVO Rn. 49.
913 *Monreal*, ZD 2016, 507 (510).

punkt.[914] Dies ist besonders relevant bei Datenverarbeitungen im Beschäftigungsverhältnis.[915]

Der Schluss einer pauschalen Verneinung der Zweckvereinbarkeit bei Ungleichgewicht der Entscheidungsfreiheit darf hieraus allerdings nicht gezogen werden. Gerade für die genannten Profiling und Scoring-Verfahren im Rahmen von *People Analytics* ist besonders auf die Sichtweise des Betroffenen und die vernünftigen Erwartungen im Rahmen einer Arbeitsbeziehung abzustellen. Werden die Verfahren eingesetzt, um „Profile" der Arbeitnehmer zu erstellen, beispielsweise für die Einsatzplanung, mögliche Weiterbildungen, aber auch Leistungsbeurteilungen, so ist dies vernünftigerweise im Rahmen des Beschäftigungsverhältnisses zu erwarten. Solche Verarbeitungsvorgänge erfolgen schließlich nicht zum Nachteil des Beschäftigten, sondern in aller Regel zu einer Optimierung der Arbeitsabläufe, aber auch zur Förderung von Arbeitnehmern. Somit besteht in aller Regel ein gleichgerichtetes Interesse. Jedenfalls aber sind diese Datenverarbeitungen in einer arbeitsvertraglichen Beziehung nicht überraschend für Arbeitnehmer.

cc) Art der personenbezogenen Daten (lit. c)

Als weiterer Aspekt im Rahmen des Kompatibilitätstests ist die Art der personenbezogenen Daten zu berücksichtigen, insbesondere ob sensitive Daten gem. Art. 9 DSGVO oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 DSGVO verarbeitet werden.

Hintergrund ist, dass diese Daten eine besondere Schutzbedürftigkeit haben und ein besonders hohes Risiko bei der Datenverarbeitung besteht. Wie sich bereits aus dem Einschub „*insbesondere*" ergibt, ist die Überprüfung der Sensibilität der Daten nicht auf die beiden Kategorien beschränkt, sondern es können auch andere Daten als besonders schutzbedürftig eingestuft werden, wenn der Aussagegehalt der Daten sehr hoch ist.[916] Als Beispiele werden Kommunikations- und ortsbezogene Daten genannt.[917]

---

914 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 46; *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 206.

915 *Monreal*, ZD 2016, 507 (510).

916 I.E. auch *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 54.

917 *Article 29 Data Protection Working Party*, WP 203, S. 25.

Als Faustregel gilt: Je sensibler die Daten, desto enger ist der Spielraum für eine mögliche Weiterverarbeitung.[918]

Im Rahmen von *People Analytics* dürfte offensichtlich sein, dass sensitive Daten, die dem Arbeitgeber offenbart werden, in aller Regel für weitergehende Analysen ausscheiden, da aufgrund des hohen Risikos eines Missbrauchs der Zweck sehr eng gefasst werden muss. Ein genereller Ausschluss ist aber nicht zwingend: Werden Gesundheitsdaten der Beschäftigten, die der Arbeitgeber im Rahmen von ärztlichen Untersuchungen oder Krankmeldungen erhalten hat, beispielsweise verwendet, um Arbeitsplätze sicherer oder ergonomischer zu gestalten, indem er die Daten nutzt, um besonders risikobehaftete Positionen und typische Krankheiten zu identifizieren, so spricht auch die Art der Daten nicht gegen eine Weiterverwendung dieser Daten außerhalb des Erhebungszweckes „Krankmeldung". Dies gilt insbesondere dann, wenn die Daten ausreichend durch technische und organisatorische Maßnahmen wie Pseudonymisierung und Anonymisierung geschützt werden, sodass negative Folgen für den Beschäftigten ausgeschlossen sind.

dd) Möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen (lit. d)

Als weiterer Aspekt im Rahmen des Kompatibilitätstests sind die zuletzt genannten (möglichen) Folgen der Zweckänderung für die betroffenen Personen zu berücksichtigen. Dabei dürfen nicht nur negative Folgen berücksichtigen werden, sondern auch positive.[919] Zur Beurteilung können die Erkenntnisse aus der Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO genutzt werden.[920] Könnte die Weiterverarbeitung zu einer Diskriminierung führen, so wird diese regelmäßig ausscheiden.[921]

Ein wichtiges Kriterium ist, ob im Rahmen der Weiterverarbeitung Dritte Kenntnis von den personenbezogenen Daten erlangen. Denn in einem solchen Fall ist es für die betroffene Person deutlich schwieriger, abzuschätzen, welche Folgen eine Weiterverarbeitung hat und für welche

---

918 *Article 29 Data Protection Working Party*, WP 203, S. 25.

919 *Article 29 Data Protection Working Party*, WP 203, S. 25; *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 56; *Monreal*, ZD 2016, 507 (511).

920 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 56.

921 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 208.

Zwecke der Dritte die Daten im Rahmen weiterer zweckkompatibler Verarbeitungsvorgange nutzen könnte.[922] So müssen in diesem Zusammenhang auch mögliche emotionale Folgen berücksichtigt werden, wie beispielsweise die Angst, die Kontrolle über die eigenen Daten zu verlieren oder Datenskandalen zu unterliegen.[923]

Bei Maßnahmen der Profilbildung ist zu beachten, dass solche in aller Regel schon bei der Datenerhebung vorhersehbar sind. Deshalb sollten bei der Erfassung hinreichend transparente Informationen gegeben werden sollten, um eine Zweckvereinbarkeit sicherzustellen.[924] Sofern ein konkreter Profiling-Zweck vorgesehen ist, muss dieser bereits bei Erhebung angegeben werden; auf eine Zweckvereinbarkeit kommt es dann nicht mehr an.

Die Art, wie die Daten weiterverarbeitet werden, hat einen großen Einfluss auf die möglichen Folgen für die betroffenen Personen, insbesondere dann, wenn im Rahmen von Profilingmaßnahmen mittels *Big Data* verschiedenartige Datensätze miteinander verknüpft werden. Mögliche Erkenntnisse sind vielfach nicht vorhersehbar (bzw. ist gerade Zweck der Verknüpfung und Analyse unbekannte Zusammenhänge zu entdecken und somit unvorhergesehene Ergebnisse zu erzeugen).[925] Aus diesem Grund wird in der Literatur vertreten, dass dieses Kriterium „im Kontext von Big Data, künstlicher Intelligenz, *selbstlernenden System*, *Kontexterfassung, Internet der Dinge und anderen Anwendungen des Ubiquitous Computing […] nur restriktiv wirken kann.*"[926]

Die Personalakte eines Arbeitnehmers ist ein typisches Beispiel für eine Profilbildung, die vorhergesehen werden kann, ohne dass diese explizit

---

922 Ähnlich *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 190; gegen eine Zweckvereinbarkeit in der Regel daher *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 57 : "*Durch Übermittlungen entsteht das Risiko nicht mehr kontrollierbarer Parallelspeicherungen, für die Schutzmaßnahmen wie Verwertungsverbote, Zugriffsbeschränkungen, Auskunftssperren und ähnliche nicht mehr wirken. Auch entsteht die große Gefahr, dass die Betroffenenrechte auf Berichtigung, Sperrung und Löschung ihre Wirksamkeit verlieren, wenn die Kette der Übermittlungen nicht mehr lückenlos nachvollzogen werden kann oder für die praktische Wahrnehmung der Rechte zu lang wird.*".

923 *Article 29 Data Protection Working Party*, WP 203, S. 25 f.

924 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 208.

925 Vgl. hierzu auch *Article 29 Data Protection Working Party*, WP 203, S. 26.

926 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 56.

als Zweck der Datenerhebung aufgeführt wird. Diese wird in aller Regel elektronisch geführt.

Inwiefern weitergehende Analysen und Profiling- oder Scoring-Maßnahmen vom Zweck abgedeckt sind oder zweckkompatibel sind, hängt vom Einzelfall ab. Grundsätzlich muss aber davon ausgegangen werden, dass betriebsnotwendiges Profiling, z.B. zur optimalen Stellenbesetzung oder gezielten Förderung von Arbeitnehmern zweckkompatibel ist, da die Folgen für den Arbeitnehmer positiver Natur sind. Hier sind die Interessen von Arbeitgeber und Arbeitnehmer in aller Regel gleichläufig: Der Arbeitgeber sucht die optimale Besetzung für eine bestimmte Stelle bzw. möchte seine Arbeitnehmer bestmöglich auf die Stelle ausbilden und Schwächen gezielt ausmerzen. Dadurch profitiert der Arbeitnehmer, der seine Arbeitsaufgaben somit zufriedenstellend ausführen und im Rahmen von Weiterbildungen gezielt auf bestimmte (Beförderungs-)Positionen ausgebildet werden kann. Hierfür spricht auch das Argument, dass in solchen Fällen die Freiwilligkeit einer Einwilligung vermutet wird (§ 26 Abs. 2 S. 2 BDSG).[927]

Bei der weitergehenden Zwecksetzung ist freilich darauf zu achten, dass die Verknüpfung mit anderen Datensätzen so stark wie möglich eingegrenzt wird und eine entsprechende Information stattfindet. Ansonsten sind die Folgen für den Betroffenen unübersehbar und die Zweckkompatibilität ist zu verneinen.

ee) Vorhandensein geeigneter Garantien (lit. e)

Als letzten Prüfungspunkt der beispielshaft aufgezählten Kriterien nennt die DSGVO das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann. Nach Erwägungsgrund 50 S. 6 sollen hierbei sowohl die Garantien beim ursprünglichen Verarbeitungsvorgang als auch bei der Weiterverarbeitung maßgeblich sein. Wie sich bereits an den beiden genannten Verfahren zeigt, sind diese Garantien weniger auf der juristischen Seite als auf der technischen Seite anzusiedeln.[928]

---

927 Dagegen wohl *Rudkowski*, NZA 2019, 72 (73).

928 *Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, Art. 6 DSGVO Rn. 142 Juristische Garantien sind aber nicht ausgeschlossen, wie nachfolgend unter **E. § 1 III. 2. b**) (**2**) begründet wird.

Die „geeigneten Garantien" sind in Zusammenhang mit dem Kriterium der möglichen Folgen aus lit. d zu sehen: Durch technisch-organisatorische Maßnahmen wie Pseudonymisierung oder Verschlüsselung können bei der Weiterverarbeitung der Daten die Risiken für die Betroffenen gesenkt[929] und somit eine zweckändernde Verarbeitung (wieder) legitimiert werden.[930] Dabei kommt es maßgeblich auf die Schutzwirkung der Maßnahmen an.[931] Eine Vereinbarkeit unter diesem Aspekt ist anzunehmen, wenn bei gleichem (Verarbeitungs-)Risiko auch gleichwertige Schutzmechanismen angewandt werden; bei höherem Risiko müssen Daten entsprechend besser geschützt werden.[932] Für Big Data-Anwendungen können nach Auffassung des BfDI die Garantien im Rahmen eine ansonsten inkompatible Weiterverarbeitung sogar ermöglichen.[933]

Für die in dieser Arbeit untersuchten *People Analytics*-Verfahren können – sofern nicht ohnehin von einer Zweckvereinbarkeit aufgrund „Statistik" (wie hier vertreten) ausgegangen wird – solche Garantien, insbesondere die Pseudonymisierung eine Zweckvereinbarkeit herstellen. Wird wirksam anonymisiert (zu den Voraussetzungen siehe bereits **D. § 1 I. 4. b**)), fällt die weitergehende Auswertung nicht mehr in den Anwendungsbereich der DSGVO.[934] Zu beachten ist jedoch, dass der Vorgang der Anonymisierung selbst aber einer Legitimation bedarf.[935] Die zweckändernde Verarbeitung (Verarbeitung der personenbezogenen Daten zu anonymisierten Daten für weitergehende Auswertungen) wird daher aufgrund geeigneter Garantien in aller Regel als zulässig zu erachten sein, wenn das Risiko der Re-Identifikation ausgeschlossen ist.

Im Hinblick auf die eingangs erwähnten Profiling und Scoring-Methoden darf nicht der gleiche Schluss gezogen werden: Es ist gerade erforderlich, dass die Daten personenbezogen, wenn auch in pseudonymisierter Form, bleiben, um die Auswertungsergebnisse einzelnen Arbeitnehmern wieder zuordnen zu können. Denkbar als Verarbeitungsgarantie zur Minderung möglicher Folgen für den Betroffenen ist jedoch eine Aggregati-

929 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 209.
930 *Article 29 Data Protection Working Party*, WP 203, S. 26 spricht hierbei von Kompensation.
931 Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 60.
932 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 60 f.; dagegen wohl Sydow/*Reimer*, Art. 6 DSGVO Rn. 75.
933 *Voßoff/Hermerschmidt*, DANA 2016, 68 (69).
934 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 61.
935 Hierzu nachfolgend **E. § 1 III. 1. a) aa)** und **E. § 1 III. 1. b) aa)**.

on[936] der Daten auf Team- oder Abteilungsebene und somit eine gewisse „Anonymisierung" (auch wenn nicht zwingend vollständige, sofern aufgrund von Ausreißern in den Daten der Team- oder Abteilungsleiter in der Lage wäre, Rückschlüsse auf einzelne Arbeitnehmer zu ziehen). Letztlich ist es dann aber nur noch für bestimmte Personen möglich, Rückschlüsse auf den einzelnen Arbeitnehmer zu ziehen.

3. § 24 BDSG: Nationale Regelung zur Zweckänderung

Eine nationale Sonderregelung zur Zweckänderung stellt § 24 BDSG dar. Sie stellt eine Spezifizierung in Ausfüllung der Öffnungsklausel in Art. 6 Abs. 4 DSGVO dar[937] und schafft somit neben den in Art. 6 Abs. 4 BDSG genannten Zweckänderungsmöglichkeiten zwei weitere Erlaubnistatbestände. Nach § 24 Abs. 1 BDSG ist die Verarbeitung personenbezogener Daten zu einem anderen als dem Erhebungszweck nur zulässig, wenn sie (1.) zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten, alternativ (2.) zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist. In beiden Fällen dürfen die Interessen der betroffenen Person am Ausschluss der Verarbeitung nicht überwiegen.

Unabhängig davon, ob der Weiterverarbeitungszweck nach Art. 6 Abs. 4 DSGVO mit dem ursprünglichen vereinbar ist, darf der Verarbeiter nach § 24 BDSG die Daten für die genannten Zwecke weiterverarbeiten.[938] Die Vorschrift stellt keine Einschränkung des Zweckkompatibilitätstests dar, sondern eine Ausnahme vom strengen Grundsatz der Zweckbindung.[939]

Beide Erlaubnistatbestände sind allerdings für die Arbeit nicht weiter von Bedeutung, da die hier untersuchten Analytics weder dem Zwecke der Gefahrenabwehr für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten dienen noch im Rahmen der Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche eingesetzt werden. Letztere könnten im Rahmen der Datenverarbeitung für die Zwecke der Beendigung des Beschäftigungsverhältnisses erforderlich sein,

936 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 209.
937 *Heckmann/Scheurer*, in: Gola/Heckmann, BDSG, § 24 BDSG Rn. 3; vgl. auch BT-Drs. 18/11325, S. 96.
938 BT-Drs. 18/11325, S. 96; *Herbst*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, § 24 BDSG Rn. 1.
939 ErfK/*Franzen*, § 24 BDSG Rn. 2 f.

wenn beispielsweise ein kündigungsrechtlicher Streit geführt wird oder Schadensersatzansprüche aus Pflichtverletzungen im Arbeitsverhältnis geltend gemacht werden sollen und hierfür IT-Daten zum Nachweis genutzt werden.

4. Zwischenergebnis

Der Grundsatz der Zweckbindung ist der Kern des Datenschutzrechts. Ohne Zweckfestlegung kann die Rechtmäßigkeit der Verarbeitung nicht überprüft werden. Aus diesem Grund ist es von höchster Bedeutung, dass die Zwecke eindeutig und unmissverständlich spezifiziert sowie dem Betroffenen nach Art. 13 und 14 DSGVO mitgeteilt werden. Die Zweckfestlegung erfolgt aber auch zum Selbstzweck des Verarbeiters, der sich hierdurch bereits im Vorfeld Gedanken machen muss, für welche Zwecke er die Daten verwenden möchte und somit mögliche Folgen der Datenverarbeitung (z.B. bei besonders risikobehafteten Verarbeitungssituationen im Rahmen der Datenschutzfolgenabschätzung gem. Art. 35 DSGVO) absehen kann.

Treten mögliche Weiterverarbeitungszwecke auf, die im Rahmen der Datenerhebung noch nicht feststanden, so ist eine Weiterverarbeitung nicht grundsätzlich ausgeschlossen, sondern es muss geprüft werden, ob die weitere Verarbeitung mit dem ursprünglichen Erhebungszweck vereinbar ist. Hierbei wird die Statistik, wobei auch die kommerziell genutzte Statistik, wie beispielsweise anonyme *People Analytics*, durch Big-Data-Auswertungen darunter zu fassen sind, gemäß Art. 5 Abs. 1 lit. b DSGVO privilegiert. Werden die in Art. 89 Abs. 1 DSGVO genannten Verarbeitungsgarantien eingehalten, ist von einer Zweckvereinbarkeit auszugehen.

Für andere Zwecke ist – sofern keine wirksame Einwilligung für die Weiterverarbeitung vorliegt – ein Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO vorzunehmen. Die Verordnung nennt beispielshaft einige Kriterien, die ein Verarbeiter zu prüfen hat: Im Ergebnis ist eine Weiterverarbeitung in der Regel dann zweckkompatibel, wenn diese für den Betroffenen vorhersehbar war und die Folgen sowie Risiken der Weiterverarbeitung möglichst geringgehalten werden. So sind im Bereich der personalisierten *People Analytics*, die nicht unter die Privilegierung der Statistik fallen, durchaus zweckkompatible Weiterverarbeitungen denkbar. Als Beispiele können genannt werden: Arbeitnehmerprofile zur optimalen Stellenbesetzung oder gezielten Förderung. Ebenfalls in begrenztem Maße auch für die gesundheitliche Förderung bzw. Unfallverhütung. Es muss jedoch im-

mer im Einzelfall geprüft werden, ob die Voraussetzungen der Zweckkompatibilität vorliegen.

In jedem Fall muss für die weitergehende Verarbeitung eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO oder § 26 Abs. 1 BDSG vorliegen, sodass keine unbegrenzte Nutzung der Daten für Analytics zulässig ist, sondern – insbesondere im Arbeitsverhältnis – eine erneute Interessensabwägung stattzufinden hat.

II. People Analytics als Profiling im Sinne von Art. 4 Nr. 4 DSGVO

Eine mögliche (Weiter-)Verarbeitungsform stellt das sog. *Profiling* dar, welches in Art. 4 Nr. 4 der Datenschutzgrundverordnung legaldefiniert ist. Es handelt sich um einen gesonderten Verarbeitungsvorgang, der im Kern dazu dient, bestimmte persönliche Aspekte einer Person vorherzusagen.[940] Er unterliegt gegenüber der Verarbeitung der dafür erforderlichen Grunddaten erhöhten Voraussetzungen. Zu beachten ist, dass nicht jede (An-)Sammlung an Daten über eine Person als *Profiling* im Sinne der DSGVO aufzufassen ist, weshalb im Folgenden genau geklärt werden muss, ab wann die hier dargestellten und untersuchten Verarbeitungsvorgänge als *Profiling* gelten und somit gesondert legitimationsbedürftig[941] sind.

1. Grundlagen

Profiling beruht auf der Annahme, dass menschliches Verhalten mathematisch berechenbar ist und sich somit bestimmte Verhaltensweisen und Interessen prognostizieren lassen.[942]

Der Begriff des *Profiling* wurde mit der Datenschutz-Grundverordnung neu eingeführt; weder das BDSG a.F. noch die Datenschutzrichtlinie kannten diesen Begriff. Lediglich für das *Scoring* enthielt § 28b BDSG a.F. eine Regelung, die die Berechnung eines Wahrscheinlichkeitswerts für ein bestimmtes zukünftiges Verhalten des Betroffenen unter gewisse Voraussetzungen stellte. Eine ähnliche Regelung enthält nunmehr § 31

940 Siehe bereits die grundlegenden Ausführungen in **D. § 1 V. 3. b**).
941 Zur Notwendigkeit einer gesonderten Legitimation des Profilings, siehe oben **D. § 1 V. 3. b**).
942 *Härting*, CR 2014, 528 (529).

BDSG.[943] Scoring darf jedoch nicht gleichgesetzt werden mit Profiling. Profiling erfordert im Gegensatz zum Scoring keine Berechnung eines Wahrscheinlichkeitswerts für ein zukünftiges Verhalten; ausreichend ist bereits die Verarbeitung personenbezogener Daten zur Bewertung persönlicher Aspekte. Der DSGVO ist der Begriff des Scorings unbekannt.[944]

Eine eigenständige Rechtsgrundlage hat das Profiling in der DSGVO jedoch nicht.[945] Wie sich aus Erwägungsgrund 72 S. 1 ergibt, unterliegt das Profiling den Vorschriften der Verordnung für die Verarbeitung personenbezogener Daten, wie etwa dem Erfordernis einer Rechtsgrundlage für die Verarbeitung oder der Beachtung der Datenschutzgrundsätze.

Verschiedene Normen in der DSGVO knüpfen an das Profiling an. So haben Betroffene nach Art. 21 Abs. 1 DSGVO ein Widerspruchsrecht, wenn das Profiling auf die Legitimationsgrundlagen Art. 6 Abs. 1 lit. e oder f DSGVO gestützt wird oder es für Direktwerbung genutzt wird (Art. 21 Abs. 2 DSGVO). Nach Art. 35 Abs. 3 lit. a DSGVO ist eine Datenschutz-Folgenabschätzung zwingend vorzunehmen, ohne dass es hierfür einer automatisierten Einzelfallentscheidung bedürfte.[946]

2. Die zwei bzw. drei Stufen des Profilings

Härting beschreibt den Profiling-Vorgang als zweistufigen Vorgang. Danach werden in einem ersten Schritt zunächst die für die Analysen notwendigen Daten erfasst, gespeichert und vorgehalten und in einem zweiten Schritt anhand komplexer Formeln bzw. Algorithmen bestimmte Wahrscheinlichkeiten (Prognosen) berechnet.[947] Je größer die zugrundeliegende Datenbasis, desto aussagekräftiger kann ein Profil werden.

---

943 Spezifisch zum Scoring siehe **E. § 1 III. 2. c) bb)**.

944 *Kort*, RdA 2018, 24 (29).

945 *Veil*, in: Gierschmann et al., Kommentar Datenschutz-Grundverordnung, Art. 4 DSGVO Rn. 1.

946 So auch *Kremer*, § 2 Zulässigkeit der Verarbeitung, in: Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, Rn. 98; a.A. *Veil*, in: Gierschmann et al., Kommentar Datenschutz-Grundverordnung, Art. 4 DSGVO Rn. 3, der verkennt, dass die Formulierung des Art. 35 Abs. 3 lit. a DSGVO gerade nicht erfordert, dass eine automatisierte Einzelfallentscheidung vorliegt Hierfür spricht auch ErwG 60 S. 3 DSGVO, der explizit statuiert, dass der Betroffene über Profilingmaßnahmen zu informieren ist.

947 *Härting*, CR 2014, 528 (529); so auch *Rudkowski*, NZA 2019, 72 (75).

Der Europarat differenziert in seiner Empfehlung zu Profiling sogar noch feingliedriger: In einem ersten Schritt würden die Eigenschaften und das Verhalten von Einzelpersonen digitalisiert überwacht und in großem Umfang gespeichert (sog. *Data Warehousing*). Das Ergebnis der Datenerhebung können pseudonymisierte oder anonyme Daten sein. Im nächsten, zweiten Schritt werden die Daten analysiert und getestet, um Zusammenhänge zwischen verschiedenen Charakteristiken und Verhalten zu erkennen (sog. *Data Mining*). Im letzten, dritten Schritt werden die aus dem Data-Mining-Vorgang gewonnen Erkenntnisse wiederum auf Individualpersonen angewandt, um Prognosen über das Verhalten oder Charakteristiken treffen zu können.[948]

Hinweis: Beiden Definitionen ist gemein, dass sie den Unterschied zum Scoring nach § 31 BDSG nicht trennscharf darstellen. Während das Scoring lediglich Wahrscheinlichkeitswerte über zukünftiges Verhalten betrifft, sind vom weiteren Begriff des Profilings unter anderem auch Wahrscheinlichkeiten für vergangenes Verhalten erfasst.

Zu beachten ist, dass die erste Stufe des Profilings, die Datenerhebung, noch nicht als Profiling im Sinne der DSGVO zu verstehen ist, da unter Profiling lediglich die Bewertung des Verhaltens (meist in Form der Berechnung von Wahrscheinlichkeitswerten) fällt, wie Art. 4 Nr. 4 DSGVO ausdrücklich vorgibt (*„jede Art der automatischen Verarbeitung, die darin besteht […], um bestimmte persönliche Aspekte […] zu bewerten, […]*). Die Datenerhebung unterliegt daher den allgemeinen Rechtmäßigkeitsvoraussetzungen und weitergehende Informationspflichten oder die Pflicht zur Fertigung einer Datenschutzfolgenabschätzung entstehen in diesem Schritt noch nicht. Die Datenbasis, die dem Profiling zugrunde liegt, muss oft nicht gesondert dafür erhoben werden, da diese Daten bereits aus anderen Datenerhebungsvorgängen dem Verarbeiter bekannt sind und ggf. in zweckverändernder Weise weiterverarbeitet werden können.[949]

Der Vorgang des Profilings bzw. die Notwendigkeit, Daten über einen längeren Zeitraum zu speichern, um später weitergehende Analysen an diesen Daten vornehmen zu können, steht dabei grundsätzlich im Widerspruch zum Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c sowie der Speicherbegrenzung aus lit. e DSGVO. Gerade, wenn die Daten nicht im Zeitpunkt der Erhebung für die Zwecke des Profilings bestimmt wurden und daher vorgehalten werden, müssen diese grundsätzlich gelöscht werden, sobald diese nicht mehr erforderlich sind.

---

948 *Council of Europe*, CM/Rec(2010)13, S. 25

949 Hierzu bereits im Detail **E. § 1 I. 2.**

Im Arbeitsverhältnis können als Grundlage beispielsweise die Stammdaten zur Begründung des Arbeitsverhältnisses oder die Verkehrsdaten aus den Serverlogdateien (*Wer hat sich wo wie lange angemeldet? Welche E-Mails gingen von welchem Absender an welchen Empfänger? etc.*) herangezogen werden. Voraussetzung ist – sofern die weitergehenden Auswertungen nicht bereits im Rahmen der Erhebung als Verarbeitungszweck festgelegt wurden –, dass eine Zweckvereinbarkeit besteht.

3. Notwendige Unterscheidung: Profilbildung vs. Profiling

Eine weitere wichtige Unterscheidung, die getroffen werden muss, ist die „Profilbildung" durch eine reine Datensammlung über eine bestimmte natürliche Person und *Profiling* im Sinne der DSGVO. Wie bereits erwähnt, stellt nicht jede Profilbildung zugleich ein Profiling dar. Profiling erfolgt zu dem Zweck, bestimmte Persönlichkeitsaspekte einer Person zu bewerten, in aller Regel, um Aussagen über deren künftiges Verhalten zu treffen.[950] Ein „Profil" kann aber bereits die Personalakte, ein (elektronischer) Lebenslauf oder Social-Media-Profil[951] darstellen, ohne dass in diesem Rahmen Persönlichkeitsaspekte bewertet werden oder künftiges Verhalten vorhergesagt werden soll.

Da nur im Fall des Profilings eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO vorzunehmen ist, ist der Vorgang von der „allgemeinen" Verarbeitung und sortierten Speicherung z.B. in einer Datenbank oder einem Dateisystem nach Art. 4 Nr. 2 DSGVO genau abzugrenzen.

a) Automatisierte Verarbeitung erforderlich

Profiling erfordert, wie sich bereits aus Art. 4 Nr. 4 DSGVO ergibt, eine automatisierte Verarbeitung. Diese ist abzugrenzen von der nichtautomatisierten Verarbeitung, vgl. Art. 2 Abs. 1 DSGVO.

---

950 *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 4 DSGVO Rn. 1.

951 Bei Social-Media-Profilen erfolgt durch den Verarbeiter (z.B. Facebook, Twitter, Instagram etc.) jedoch in aller Regel ein Profiling im Hintergrund, um beispielsweise Freundschaftsvorschläge zu generieren, insbesondere aber um gezielte Werbung anzuzeigen und hierdurch Gewinn erwirtschaften zu können.

Eine bloß manuelle Verknüpfung der Daten zum Zweck der Persönlichkeitsbewertung und -analyse, beispielsweise im Assessment-Center durch Psychologen, ist daher von dieser Vorschrift nicht erfasst.[952]

b) Merkmal: Persönliche Aspekte

Wesentlich für das Profiling ist, dass persönliche Aspekte, die sich auf eine natürliche Person beziehen, verarbeitet werden. Beispielshaft werden in Art. 4 Nr. 4 Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel genannt.[953] Art. 4 Nr. 4 DSGVO knüpft daher die Verarbeitung allein an das verfolgte Ziel, unabhängig vom zugrundeliegenden Datenverarbeitungsvorgang.[954] Scoring ist aufgrund des engeren Anwendungsbereichs (siehe oben) als Unterfall des Profilings einzustufen.[955]

c) Verarbeitungsinhalt: Verarbeitung zum Zwecke der Bewertung

Das Ziel der Verarbeitung muss beim Profiling die Bewertung persönlicher Aspekte einer natürlichen Person sein.[956] Eine Bewertung stellt hierbei noch nicht die Wiedergabe von Information dar, die ein personenbe-

952 Vgl. *Buchner*, 2 Grundsätze des Datenschutzrechts, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 272 Rn. 142. *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 4 Nr. 4 DSGVO Rn. 5; *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 4 DSGVO Rn. 3.

953 Ebenso für eine nicht-abschließende Aufzählung: *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 4 DSGVO Rn. 4; *Zahariev*, PinG 2017, 73 (75 f.); *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 4 Nr. 4 DSGVO Rn. 7.

954 *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 4 Nr. 4 DSGVO Rn. 6.

955 *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 4 Nr. 4 DSGVO Rn. 7.

956 *Artikel-29-Datenschutzgruppe*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679 (WP 251), S. 7; *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 4 DSGVO Rn. 6.

zogenes Datum oder ein Persönlichkeitsmerkmal repräsentiert, sondern erfordert eine Interpretation dieser.[957]

Eine einfache Einteilung von Personen anhand bekannter Merkmale (im Beschäftigungsverhältnis z.B. Statusgruppe, Position, Teilzeit/Vollzeit, Geschlecht u.a.) stellt noch kein Profiling dar, selbst wenn die Einteilung dazu dient, einen zusammenfassenden Blick über die Gruppe der leitenden Angestellten, Vollzeitkräfte oder die Frauenquote im Unternehmen zu erhalten. In diesen Fällen werden keine Vorhersagen oder Schlussfolgerungen über einzelne Personen getroffen, daher liegt keine Bewertung individueller Merkmale und somit kein Profiling vor.[958]

4. Profiling im Arbeitsverhältnis

Die Erstellung einer Personalakte zum Zwecke der Verwaltung des Arbeitsverhältnisses stellt selbst dann kein Profiling dar, wenn es dadurch mit Hilfe der IT möglich ist, die Belegschaft nach Kriterien zu sortieren und filtern, um daraus beispielsweise Statistiken oder Reporte zu generieren. In keinem der genannten Fälle werden persönlichen Aspekte natürlicher Personen im Rahmen automatisierter Verarbeitung *bewertet*. Es liegt auch kein Profiling vor, wenn im Anschluss an diese Sortierung und mit Hilfe der Reporte ein Personalverantwortlicher eigene Schlüsse zieht und daher ein „manuelles Profiling" vorliegt (s.o.).

Beispiel: Es stellt kein Profiling dar, wenn HR-Software einen Bericht über die Fehlzeiten der einzelnen Arbeitnehmer einer Abteilung über die letzten fünf Jahre generiert (und diesen z.B. grafisch darstellt) und der Abteilungsleiter daher den Schluss zieht, dass bestimmte Arbeitnehmer (mit hohen Fehlzeiten) unzuverlässig sind. Es liegt keine Bewertung durch eine automatisierte Verarbeitung vor.

Dieses „klassische Reporting" ist von People Analytics abzugrenzen. Während das genannte Szenario auf Level 2 der eingangs darstellen Automationsstufen der Arbeitnehmeranalyse anzusiedeln ist, beginnen People Analytics erst ab Level 3.[959] Analysen unterhalb Level 3 stellen noch kein Profiling im Sinne der DSGVO dar.

---

957 *Deuster*, PinG 2016, 75 (76); Paal/Pauly/*Martini*, Art. 22 DSGVO Rn. 22.

958 *Artikel-29-Datenschutzgruppe*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679 (WP 251), S. 7.

959 Siehe **C. § 2 III**.

Erst ab Level 3 werden sog. *People Models* erstellt, die auf Basis vorhandener Daten Trendanalysen erstellen, wobei diese mit zunehmendem Reifegrad (Level) immer detaillierter werden. Auf Level 4 erfolgt eine Verknüpfung verschiedener Daten zum Zwecke der Feststellung von Korrelationen und ab Level 5 automatisierte Entscheidungen auf Basis der berechneten Daten.

Zu beachten ist jedoch, dass durch eine alleinige Berechnung von Trends, im oben genannten Fall der Fehlzeiten z.B. durch das Verfahren der linearen Regression, keine Bewertung persönlicher Aspekte vorliegt, sondern lediglich die Fehlzeiten für das kommende Jahr prognostiziert werden. Nach der Definition der DSGVO stellt dies ebenfalls kein Profiling dar, sofern diese Daten nicht mit den Fehlzeiten von anderen Arbeitnehmern zum Zwecke der Bewertung verknüpft werden oder mit der durchschnittlichen Fehlzeit automatisiert verknüpft und hierdurch beispielsweise ein „Zuverlässigkeits-Score" für jeden Arbeitnehmer erstellt wird.

Über neuartige Zusatzmodule (z.B. Workforce Analytics für die Personalverwaltungssoftware SAP Success Factors[960]) können sich Arbeitgeber neue Funktionen dazukaufen und Analysemöglichkeiten erweitern. In vielen neuen Modulen findet nunmehr ein Profiling statt, im Zuge dessen über einzelne Arbeitnehmer oder Bewerber entweder ein „Overall-Rating" im Sinne einer Gesamtnote erstellt wird[961] oder die Arbeitnehmer als „Low Performer" bzw. „High Performer" eingestuft werden, um anhand dieser Klassifizierung weitere Schritte planen zu können.[962]

Für ein Profiling muss aber nicht notwendigerweise eine komplexe (und teure) HR-Software eingesetzt werden. Ausreichend, um als Profiling im Sinne der DSGVO zu gelten, wäre es bereits, wenn Personalverantwortliche bzw. Personalanalysten eine entsprechende Excel-Liste führen und dort anhand von Formeln bestimmte Kennzahlen errechnen lassen und diese Kennzahlen zu einer Einteilung in bestimmte Kategorien („unzuverlässig", „oft krank", „extrem förderungswürdiger Arbeitnehmer", „Kün-

960 Vgl. https://www.sap.com/germany/products/human-resources-hcm/workforce-planning-hr-analytics.html#analytics (letzter Abruf am: 29.07.2020).

961 So beispielweise bei der HR-Lösung „Workday" des Herstellers Gartner, vgl. *Sommer*, CuA 2017, 8 (10).

962 SAP Success Factors Workforce Analytics nimmt eine solche Einteilung vor, siehe hierzu die Website des Herstellers, https://www.successfactors.com/products-services/planning-analytics/hr-analytics.html (letzter Abruf am: 13.12.2019). Zur Klassifizierung im Allgemeinen *Schürmann*, Auswertung von Mitarbeiterdaten - (Any)/(No)thing possible?, in: Taeger, Smart world - smart law?, S. 502 f.

digungskandidat") führen. In diesem Beispielsfall findet keine schlichte Anzeige von Daten mehr statt, sondern eine Interpretation anhand vorgegebener Formeln.

III. Maßstab zur Beurteilung der Rechtmäßigkeit: § 26 BDSG, ggf. Art. 6 Abs. 1 lit. f DSGVO

Für die Beurteilung der Zulässigkeit von People Analytics müssen daher zwei verschiedene Varianten der Analytics beurteilt werden.[963] Auf der einen Seite stehen „einfache" Analytics (im Folgenden: **Simple People Analytics**) ohne Profiling-Verfahren und weitere Datenerhebungen und auf der anderen die „fortgeschrittenen" Analytics (im Folgenden: **Advanced People Analytics**), bei welchen in vielen Fällen (aber nicht notwendigerweise) zusätzliche Echtzeitdaten erhoben werden, jedenfalls aber Arbeitnehmer anhand von Algorithmen in bestimmte Kategorien eingeteilt werden bzw. ein Scoring im Sinne einer Notenvergabe stattfindet.

1. Simple People Analytics

Unter dem Topos „Simple People Analytics" (kurz: **SPA**) werden im nachfolgenden Analyseverfahren betrachtet, die bestimmte Personalkennzahlen ermitteln und beispielsweise anhand linearer Regression Trends vorhersagen, damit Personalverantwortliche hieraus weitere Schlüsse ziehen und Maßnahmen einleiten können.

Beispiel: Im Unternehmen sind die Fluktuationszahlen der vergangenen Jahre bekannt; hieraus wird aus den vergangenen Zahlen mittels linearer Regression eine Vorhersage der Fluktuation für das nächste Jahr berechnet. Ebenso könnten solche Versuche mit Fehlzeiten von Arbeitnehmern auf Monatsbasis gestartet werden, um vorherzusagen, in welchem Monat ein Arbeitnehmer vermutlich wie oft fehlen wird.

Vor allem bei KMUs werden in der Praxis aufgrund der dadurch entstehenden Software-Kosten und dem dafür notwendigen Know-How derzeit wohl keine fortgeschrittenen People Analytics eingesetzt werden. Nichtsdestotrotz besteht auch oftmals dort der Wunsch bzw. das Bedürfnis Perso-

963 Andere Autoren unterscheiden hier zwischen „find", „grow" und „keep", die typische Anwendungsfelder von People-Analytics darstellen würden, vgl. *Götz*, Big Data im Personalmanagement, S. 37.

nalentscheidungen stärker informationsbasiert, anstatt intuitiv zu treffen, da solche Entscheidungen im Durchschnitt eine höhere Vorhersagekraft als Expertenurteile haben.[964]

Vielfach benötigt es als Datenbasis keine personenbezogenen Daten. So beispielsweise, wenn Analytics dazu genutzt werden sollen, die Ursache für eine hohe Fluktuationsquote in bestimmten Bereichen bzw. Zusammenhänge zwischen der Fluktuationsquote und anderen Kennzahlen zu ermitteln. Hierfür reichen vielfach hinreichend aggregierte (und hierdurch anonymisierte) Daten aus. Die durch Analytics erkannten Zusammenhänge können in weiterer Folge wieder dafür genutzt werden, um Maßnahmen zu planen.[965] Sieht der Algorithmus Vorschläge für einzelne (besetzte) Stellen vor, handelt es sich wieder um personenbezogene Daten, jedoch nicht um ein Profiling, da keine Bewertung der einzelnen Stelleninhaber erfolgt, sondern lediglich auf Basis von Kennzahlen bestimmte Empfehlungen für bestimmte Stellen bzw. deren Inhaber vorgeschlagen werden. Letztere wären dann legitimationsbedürftig nach § 26 Abs. 1 BDSG.

Zu beachten ist, dass bereits die Verarbeitung zum Zwecke der Anonymisierung (also das Anonymisieren der personenbezogenen Daten selbst) ein Datenverarbeitungsvorgang im Sinne von Art. 4 Nr. 2 DSGVO und somit legitimationsbedürftig ist.[966] Aus diesem Grund sind bei weitergehender Verarbeitung zum Zwecke der Anonymisierung auch die Kriterien der Zweckvereinbarkeit (Art. 5 Abs. 1 lit. b, Art. 6 Abs. 4 DSGVO) zu prüfen.[967] Erst nach erfolgreicher Anonymisierung[968] unterliegen die Daten nicht mehr den datenschutzrechtlichen Bestimmungen. Möglich ist es aber, bestimmte Daten bereits anonym zu erheben, um somit den Zwischenschritt der (legitimationsbedürftigen) Anonymisierung zu vermeiden.

Sowohl für die Anonymisierung als auch die Nutzung der personenbezogenen Daten kommen verschiedene Legitimationsgrundlagen in Betracht, die im Folgenden näher analysiert werden sollen:

---

964 Vgl. *Jäger/Petry*, Digital HR - Ein Überblick, in: Petry/Jäger, Digital HR, S. 44.

965 *Atabaki/Biemann*, Potenziale der Datenanalyse für HR (People Analytics), in: Petry/Jäger, Digital HR, S. 130.

966 *Article 29 Data Protection Working Party*, Opinion 05/2014 on Anonymization Techniques (WP 216), S. 8; *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 5 Rn. 23; a.A. wohl *Dzida/Groh*, ArbRB 2018, 179 (181).

967 *Article 29 Data Protection Working Party*, Opinion 05/2014 on Anonymization Techniques (WP 216), S. 7.

968 Zu den Voraussetzungen wirksamer Anonymisierung siehe **D. § 1 I. 4. b**).

a) Einwilligung

Die Einwilligung kann grundsätzlich die Datenverarbeitung umfassend legitimieren (Art. 6 Abs. 1 S. 1 DSGVO), wenn die Bedingungen aus Art. 7 DSGVO eingehalten wurden.[969] Im Arbeitsverhältnis ist aufgrund der bestehenden Abhängigkeit die Freiwilligkeit der Einwilligung problematisch, wobei diese nicht von vornherein ausscheidet (hierzu bereits oben **D. § 1 III. 2. a) bb) (2)**).

aa) Einwilligung zum Zwecke der Anonymisierung

Die Einwilligung zum Zwecke der Anonymisierung ist von der Einwilligung für personenbezogene Analytics zu unterscheiden. Durch die Anonymisierung ist es nicht mehr möglich, die Daten des einzelnen Arbeitnehmers diesem zuzuordnen. Aus diesem Grund entsteht für den Arbeitnehmer kein Risiko unmittelbarer nachteilhafter Folgen. § 26 Abs. 2 S. 2 BDSG bestimmt, dass die Freiwilligkeit insbesondere dann vorliegen kann, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird. Es ist nun die Frage aufzuwerfen, ob auch bei „neutralen Einwilligungen", an welche jedenfalls keine unmittelbaren Folgen geknüpft werden können, eine Vermutung für die Freiwilligkeit besteht.

Beispiele für eine Einwilligung für die Nutzung personenbezogener Daten, bei welcher lediglich ein rechtlicher oder wirtschaftlicher Vorteil erlangt wird, sind nach der Gesetzesbegründung die Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung oder die Erlaubnis zur Privatnutzung von betrieblichen IT-Systemen.[970] In der Literatur werden als weitere Beispiele noch die Aufnahme von Beschäftigtendaten in konzernübergreifende Personalentwicklungssysteme oder Firmenrabattsysteme[971] sowie die Weitergabe an Daten zum Zwecke der Sonderzuteilung an Unternehmensaktien[972] genannt.

Ebenso sehen manche Autoren die Einwilligung als wirksam an, wenn der Arbeitnehmer keine Nachteile von der Datenverarbeitung zu befürchten hat.[973] Zu beachten ist in jedem Fall das Koppelungsverbot aus Art. 7

969 Siehe hierzu im Detail **D. § 1 III. 2. a)**.
970 BT-Drs. 18/11325, S. 97.
971 *Ernst*, ZD 2017, 110 (112).
972 *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 132.
973 *Ernst*, ZD 2017, 110 (111 f.).

Abs. 4 DSGVO, wonach die Erfüllung des Vertrags nicht davon abhängig gemacht werden darf, dass die Einwilligung zur Verarbeitung erteilt wird, wenn diese Daten für die Vertragserfüllung nicht erforderlich sind.[974] Da für die Beurteilung der Freiwilligkeit auch die Eingriffstiefe der Verarbeitung entscheidend ist,[975] ist bei der Anonymisierung mangels Eingriff unter diesem Gesichtspunkt von einer Freiwilligkeit auszugehen.

Als weiteres Kriterium für die Beurteilung nennt die Gesetzesbegründung noch die Art des verarbeiteten Datums[976], wobei es hier auch auf die Nähe zum Beschäftigungsverhältnis ankommt (*Verarbeitet der Arbeitgeber die Daten ohnehin und möchte diese nur für einen weiteren Zweck nutzen?*).[977] Bei der Nutzung der Daten zum Zwecke der Anonymisierung ist dies ebenfalls der Fall. Dem Arbeitgeber liegen diese Daten bereits in personenbezogener Form vor, für die weitergehende Nutzung zu Analyticszwecken sollen diese Daten jedoch in anonymisierter Form weiterverarbeitet werden (z.B. um diese unabhängig von bestimmten Datenschutzstandards auch an Konzern- oder Partnerunternehmen im Ausland übermitteln zu können).

Aus diesem Grund ist die Einwilligung durch Beschäftigte für die Zwecke der Anonymisierung grundsätzlich als zulässig zu beurteilen, solange Arbeitgeber keinen Druck auf Beschäftigte ausüben und das Kopplungsverbot des Art. 7 Abs. 4 DSGVO einhalten. Letztlich spricht dafür auch, dass durch *Analytics* vielfach gleichgelagerte Interessen verfolgt werden (§ 26 Abs. 2 S. 2 BDSG), wenn diese genutzt werden sollen, um Arbeitsbedingungen zu optimieren, das Gesundheitsmanagement zu fördern oder Probleme im Betriebsablauf zu entdecken.

Zwar ist die Einwilligung *vor* Abschluss eines Arbeitsvertrages grundsätzlich ausgeschlossen[978]; denkbar ist eine wirksame Einwilligung in solche Analytics allerdings durchaus *mit* Abschluss des Vertrages, z.B. wenn der Arbeitgeber dem Arbeitnehmer (wie in der Praxis häufig) bereits einen einseitig unterzeichneten Arbeitsvertrag zusendet und als Anhang

974 Zu weitgehend daher *Seifert*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 88 DSGVO Rn. 218, der von einer generellen Unwirksamkeit der Einwilligung nach § 134 BGB ausgeht, wenn die Datenverarbeitung für den Beschäftigten keinen Vorteil bringt.

975 BT-Drs. 18/11325, S. 97; vgl. auch *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 131.

976 *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 97.

977 Paal/Pauly/*Gräber/Nolden*, § 26 BDSG Rn. 29.

978 Da hier in aller Regel nicht von einer Freiwilligkeit ausgegangen werden darf, hierzu bereits oben **D. § 1 III. 2. a) bb) (2)**.

zum Arbeitsvertrag sich die Einwilligung der Nutzung der Arbeitnehmerdaten zum Zwecke der Analytics einholt. In einem solchen Fall unterliegt der Bewerber grundsätzlich keiner Drucksituation mehr, da er durch die Unterzeichnung des Arbeitsvertrags bereits einen wirksamen Vertrag geschlossen hätte, unabhängig von der beigefügten Einwilligung zur Datennutzung.[979] In diesem Zusammenhang müssen Arbeitgeber jedoch darauf achten, dass im Rahmen der Einwilligung verdeutlicht wird, dass diese nicht Bestandteil des Arbeitsvertrages ist und die Freigabe der Daten für die vorgesehenen Analytics-Zwecke absolut freiwillig ist. Dem Arbeitnehmer muss eine echte Wahlmöglichkeit geboten werden.[980]

bb) Einwilligung für personenbezogene Analytics (ohne Profiling)

Bei der Einwilligung für personenbezogene Analytics liegt die Situation im Vergleich zur eben untersuchten der Anonymisierung anders: Aufgrund der Zuordenbarkeit der Analytics-Ergebnisse muss grundsätzlich von einer gewissen Eingriffsintensität ausgegangen werden und für den Betroffenen ist die Einwilligung kein „neutrales Geschäft" mehr. Etwaige Analytics-Ergebnisse können zu unmittelbaren Folgen für den Beschäftigten führen. Dennoch ist auch in diesem Fall nicht von einer generellen Unwirksamkeit der Einwilligung auszugehen.[981] Auch hier sind die konkreten Analyticszwecke unter die Beispiele aus § 26 Abs. 2 S. 2 BDSG zu subsumieren, sodass – wie sich bereits aus der Gesetzesbegründung ergibt[982] – durchaus wirksame Einwilligungen möglich sind. Ein Beispiel hierfür sind die unter **E. § 3 I** untersuchten persönlichen Dashboards für den Arbeitnehmer ohne Arbeitgeberzugriff auf die Daten. Da bei „Simple People Analytics" kein Profiling vorgenommen wird, ist die Eingriffsintensität mangels Bewertung persönlicher Aspekte geringer.

Nichtsdestotrotz besteht in diesem Fall für den Arbeitgeber eine rechtliche Unsicherheit, da er im Streitfall für die Freiwilligkeit der Einwilligung

979 Etwas anderes könnte gelten, wenn sich der Bewerber aufgrund einer im Arbeitsvertrag vereinbarten Probezeit dazu genötigt fühlt, die Unterzeichnung ebenfalls zu unterschreiben, weil er die Befürchtung hat, ansonsten unmittelbar wieder gekündigt zu werden.

980 Diese muss er auch subjektiv so wahrnehmen können, vgl. *Rudel*, Personalmagazin 2019, 76 (78).

981 So wohl auch BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 118.3: *Erlaubnis [für People Analytics] könnte daher nur eine Einwilligung geben.*".

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

darlegungs- und beweispflichtig ist.[983] Will sich der Arbeitgeber mit der Einwilligung zusätzlich absichern, so darf es sich nicht um Daten handeln, für die ein Verarbeitungsgebot besteht. Dies wäre beispielsweise bei Daten der Fall, die er für die Erfüllung seiner gesetzlichen Pflichten benötigt (Daten des Arbeitnehmers für die Sozialversicherung etc.).[984] Ferner muss er darauf hinweisen, dass seiner Auffassung nach mehrere Erlaubnistatbestände einschlägig sind, die Einwilligung also als rechtliche Absicherung eingeholt wird.[985] In jedem Falle aber muss der Arbeitgeber bei Einholung der Einwilligung nach § 26 Abs. 3 S. 4 BDSG auf den Zweck der Datenverarbeitung sowie auf das in Art. 7 Abs. 3 DSGVO niedergelegte Widerrufsrecht in Textform aufmerksam machen.

Die Einwilligung eignet sich aufgrund des jederzeitigen Widerrufsrechts daher nur bedingt, da Arbeitgeber im Falle eines Widerrufs sicherstellen müssen, dass die aufgrund der Einwilligung verarbeiteten Daten vollständig für zukünftige Auswertungen aus den Datensätzen entfernt werden. Die darauf basierenden Analysen werden daher unvollständig, weshalb in weiterer Folge zu prüfen ist, ob andere Erlaubnistatbestände einschlägig sein könnten, die nicht dem Widerrufsrecht unterliegen. Nur als letzte Option sollte auf die Einwilligung des Arbeitnehmers zurückgegriffen werden.

b) Erforderlichkeit: Interessensabwägung

Es stellt sich die Frage, ob SPA als erforderlich für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses im Sinne von § 26 Abs. 1 BDSG angesehen werden können. Erforderlich sind Daten grundsätzlich nur dann, wenn der Arbeitgeber ein „berechtigtes, billigenswertes und schutzwürdiges Interesse“[986] an der Verarbeitung der Daten hat.

In diesem Rahmen ist – wie bereits aufgeführt – zu prüfen, ob das zu erreichende Ziel legitim und das eingesetzte Mittel zur Erreichung

---

983 Siehe bereits **D. § 1 III. 2. a**).

984 Hierzu oben **D. § 1 III. 2. c**).

985 Zur Problematik der Einschlägigkeit mehrerer Erlaubnistatbestände, insbesondere der Möglichkeit der Einholung einer Einwilligung neben einem gesetzlichen Erlaubnistatbestand aus Art. 6 Abs. 1 DSGVO, siehe **D. § 1 III. 1**.

986 So im Ansatz bereits BAG, Urt. v. 05.12.1957 – 1 AZR 594/56, NJW 1958, 516; zuletzt zum Fragerecht des Arbeitgebers Urt. v. 18.09.2014 – 8 AZR 759/13, AP AGG § 15 Nr. 20.

des Ziels geeignet (d.h. zweckförderlich) ist. Im Anschluss muss geprüft werden, ob es das relativ mildeste Mittel zur Erreichung des gewünschten Ziels ist, es also keine milderen, *gleich geeigneten* Mittel gibt. Zuletzt muss das Mittel (*in concreto:* Die Verarbeitung der spezifischen Daten.) auch angemessen sein, wobei in diesem Rahmen die widerstreitenden Interessen der Vertragsparteien bzw. von Verarbeiter und Betroffenen miteinander abgewogen und in praktische Konkordanz gebracht werden müssen.

Zu pauschal und deshalb im Ergebnis falsch wäre es, an dieser Stelle festzustellen, dass die Erhebung und Auswertung von Mitarbeiterdaten zur Personalauswahl und -führung mit Hilfe von größeren Datenmengen und Algorithmen nicht der Durchführung des Beschäftigungsverhältnisses *dient* und deshalb nicht von § 26 BDSG gedeckt sei.[987] Unzweifelhaft dient die Personalplanung und somit die prospektive Betrachtung einzelner Arbeitnehmer der Durchführung des Beschäftigungsverhältnisses, ist aber auch erforderlich, um als Arbeitgeber bei stetig steigendem Wettbewerbsdruck noch konkurrenzfähig zu bleiben.[988]

So hat das BAG bereits im Jahr 1979 festgestellt, dass Arbeitgeber die Eignung, Befähigung und fachliche Leistung der bei ihm beschäftigten Arbeitnehmer beurteilen und diese Beurteilungen in den Personalakten festgehalten werden dürfen.[989] Auch hier handelt es sich um eine Sammlung von Daten, die heutzutage – insbesondere bei einer Sammlung über mehrere Jahre bei einer Vielzahl von Arbeitnehmern – unter den Begriff *Big Data* gefasst würde, sofern die Daten (wie in moderner Personalverwaltungssoftware üblich) schnell und übersichtlich darstellbar sind.

aa) Erforderlichkeit der Anonymisierung

In vielen Fällen reichen dem Arbeitgeber anonyme Daten für Analytics aus[990], sodass er die Daten vor einer Nutzung anonymisieren muss, um weitgehende Privilegien bei der Verarbeitung zu erhalten. Durch die Anonymisierung wird der Personenbezug gelöscht und somit das Risiko für die betroffenen Arbeitnehmer gesenkt. Es handelt sich daher um ein mil-

987 So aber BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 118.3.

988 Insofern widerspricht sich *Riesenhuber* hier selbst, wenn er feststellt, dass die Personalplanung zur Durchführung des Beschäftigungsverhältnisses gehört, ebenso wie Regelbeurteilungen, vgl. BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 117 f.

989 BAG, Urt. v. 28.03.1979 – 5 AZR 80/77, AP BPersVG § 75 Nr. 3.

990 Anwendungsbeispiele nennt *Jentzsch*, HR Performance 2013, 48.

deres, gleich effektives Mittel, wenn hierdurch die gewünschten Zahlen erzeugt werden können.

Zu beachten ist, dass der Vorgang der Anonymisierung selbst legitimiert werden muss,[991] also an den Kriterien des § 26 Abs. 1 BDSG bzw. Art. 6 Abs. 1 lit. f DSGVO bei beschäftigungsfremden Zwecken gemessen werden und somit einer Interessensabwägung standhalten. Das durch Arbeitgeber mit SPA verfolgte Ziel, einen Überblick über die Belegschaft zu be- bzw. erhalten und Personalplanung zu betreiben und hierdurch letztlich das Unternehmen wirtschaftlich zu führen, ist (wie bereits das BAG dargestellt hat[992]) ein legitimes Ziel. Hierdurch übt ein Arbeitgeber nur seine Grundrechte aus Art. 15 und 16 EU-GRC bzw. Art. 12 und 14 GG aus. Die hierfür genutzten Personaldaten (insbesondere Leistung, Eignung, fachliche Befähigung, Beurteilungen) und Methoden der SPA sind für die Erreichung des Ziels auch geeignet. Ebenso gibt es kein milderes, gleich geeignetes Mittel, wenn im Rahmen von SPA lediglich grundlegende Daten über das Arbeitsverhalten von Arbeitnehmern ohne Bewertung für Vergleiche oder Prognosen herangezogen werden. Schließlich werden bei SPA lediglich Vergangenheitswerte interpoliert oder mithilfe linearer Regression fortgeschrieben, um Trends erkennen zu können, ohne dass weitere Bewertungen durch automatisierte Verarbeitung stattfinden. Dies stellt bereits das absolute Minimum an Verarbeitung dar, um wenigstens im Ansatz aussagekräftige Zukunftsdaten zu bekommen.

Geprüft wurde in diesem Schritt lediglich, ob der Verarbeitungsvorgang der Anonymisierung, genauer die Nutzung der personenbezogenen Daten zum Zwecke der Anonymisierung für die weitergehende Nutzung für SPA „erforderlich" ist bzw. einer Interessenabwägung standhält.[993] Personenbezogene Daten werden in diesem Fall nicht weiteren Analysen unterzogen, sondern lediglich anonymisierte Daten, sodass die weitergehenden Analysen nicht mehr am Datenschutzrecht zu messen sind.

Zuletzt muss auch eine Zweckvereinbarkeit des Anonymisierungsvorgangs (nicht: der weitergehenden Analysen, da diese nicht mehr dem Datenschutzregime unterliegen) mit dem Erhebungszweck nach Art. 6

991 So wohl auch *Götz*, Big Data im Personalmanagement, S. 88.

992 BAG, Urt. v. 28.03.1979 – 5 AZR 80/77, AP BPersVG § 75 Nr. 3.

993 Der Vorgang der Anonymisierung ist grundsätzlich legitimationsbedürftig, da zunächst personenbezogene Daten verarbeitet werden zum Zwecke der Entfernung des Personenbezugs, wie hier *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 5 Rn. 23; *Article 29 Data Protection Working Party*, Opinion 05/2014 on Anonymization Techniques (WP 216), S. 8 Diese Problematik übersehen wohl *Dzida/Groh*, ArbRB 2018, 179 (181).

Abs. 4 DSGVO vorliegen. Da weitergehende Analysen dann keine Rückschlüsse auf einzelne Personen mehr zulassen, fällt das Recht auf Privatheit aus Art. 7, 8 EU-GRC (dies entspricht in etwa dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) als mögliches entgegenstehendes Interesse des Arbeitnehmers weg, sodass die Interessenabwägung hier klar zugunsten des Arbeitgebers ausfällt. Mangels negativer Folgen für den Betroffenen (keine Zuordenbarkeit der SPA-Ergebnisse[994] mehr erreichbar), fällt auch die Zweckvereinbarkeitsprüfung nach Art. 6 Abs. 4 DSGVO positiv aus.

bb) Erforderlichkeit der Nutzung personenbezogener Daten für Analytics

Ebenso gibt es Fälle, in denen die Nutzung anonymisierter Daten unmöglich ist, beispielsweise dann, wenn Arbeitgeber konkrete Daten über einzelne Arbeitnehmer benötigen. Hier kann die Personaleinsatzplanung, Personalentwicklung oder mitunter auch das Gesundheitsmanagement genannt werden. Bei letzterem ist zu beachten, dass es sich hier in aller Regel um sog. *sensitive Daten* im Sinne von Art. 9 Abs. 1 DSGVO handelt, die weitgehenden Verarbeitungsbeschränkungen unterliegen.[995]

(1) Nutzung nicht-sensitiver Daten für SPA

Sollen personenbezogene Daten von Arbeitnehmern, die nicht für SPA-Zwecke, aber für die Zwecke des Personalmanagements, erhoben wurden, für Analytics weiterverarbeitet werden, so ist zunächst eine Zweckvereinbarkeitsprüfung nach Art. 6 Abs. 4 DSGVO vorzunehmen. Nicht nur in diesem Rahmen, sondern auch bei der Interessenabwägung im Rahmen der Prüfung des Erlaubnistatbestands für die Verarbeitung sind die geeigneten Garantien, insbesondere die Pseudonymisierung von hoher Bedeutung. Pseudonymisierung ist eine Verarbeitungsgarantie, da sie es

994 Aufgrund des weiten Wortlauts des Art. 6 Abs. 4 lit. d DSGVO ist bei der Zweckvereinbarkeit des Anonymisierungsvorgangs mit dem Erhebungsvorgang auch die Analyse, die selbst dem Datenschutzrecht nicht mehr unterliegt, in die Folgenabschätzung miteinzubeziehen (so wohl auch *Article 29 Data Protection Working Party*, WP 203, S. 26, wo ausdrücklich auf die Anonymisierung als Schutzmechanismus verwiesen wird).

995 Siehe hierzu bereits **D. § 1 V. 1.**

Dritten es unmöglich[996] macht, die Daten einer bestimmten Person zuzuordnen;[997] diese Verarbeitung stellt somit ein geeignetes, milderes Mittel der Datenverarbeitung dar. Dies ist vor allem in Fällen von Datenlecks von besonderer Bedeutung. Für Analytics ist eine solche problemlos möglich, sodass die Verarbeitung unter Pseudonym als milderes Mittel zu erfolgen hat und eine Zuordnung der Ergebnisse zu den Namen (oder Personalnummern) der Beschäftigten erst zum Ende des Verarbeitungsvorgangs wieder erfolgen darf (wenn beispielsweise der Sachbearbeiter die Person auf seinem Bildschirm aufruft).

Da die für SPA genutzten Daten ausschließlich das betriebliche Verhalten oder Stammdaten von Arbeitnehmern betreffen, ist in der Angemessenheitsprüfung, also der Abwägung der jeweiligen Interessen bzw. Positionen von einem Überwiegen der Interessen des Arbeitgebers gegenüber den Geheimhaltungsinteressen des Arbeitnehmers auszugehen, zumal die Datengrundlage dem Arbeitgeber bereits in rechtmäßiger Weise vorliegt[998]. Außer der Fortschreibung bereits bestehender Daten mithilfe einfacher statistischer Methoden erfolgt keine Erzeugung neuer personenbezogener Daten, insbesondere keine Persönlichkeitsbewertung einzelner Arbeitnehmer durch automatisierte Verarbeitungsvorgänge.

Nicht-sensitive Daten dürfen daher im Rahmen von SPA in den hier aufgezeigten Grenzen nach § 26 Abs. 1 BDSG verarbeitet werden, sofern zumindest eine Pseudonymisierung (bspw. in Form einer Verschlüsselung) erfolgt und eine Anonymisierung untunlich ist.

(2) Nutzung sensitiver Daten für SPA

Bei sog. *sensitiven Daten* im Sinne von Art. 9 Abs. 1 DSGVO könnte die Interessensabwägung zu einem anderen Ergebnis führen, da diese Daten – wie bereits dargestellt – einem erhöhten Schutz unterliegen und die Verarbeitung daher deutlich höheren Rechtfertigungsanforderungen unterliegt. Zur Verarbeitung solcher Kategorien von Daten durch Arbeitgeber muss

996 Oder jedenfalls sehr schwer, da eine Zuordnungstabelle zur Auflösung der Pseudonyme erforderlich ist, die für die wirksame Pseudonymisierung von den Daten getrennt (und sicher) aufzubewahren ist.

997 Zu den Voraussetzungen und Wirkungen der Pseudonymisierung, siehe **D. § 1 I. 4. c**).

998 Der Fokus der Arbeit liegt auf der Datenverarbeitung für Analytics-Zwecke, weshalb davon ausgegangen wird, dass die vorhandenen Daten in rechtmäßiger erhoben wurden.

die Verarbeitung gem. § 26 Abs. 3 BDSG zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit oder des Sozialschutzes erforderlich sein. Ferner dürfen entgegenstehende Interessen der betroffenen Beschäftigten nicht überwiegen. Gemäß § 26 Abs. 3 S. 4 BDSG sind bei einer Verarbeitung angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen (§ 22 Abs. 2 BDSG). Hierzu kann u.a. gehören, dass die Daten pseudonymisiert und verschlüsselt werden. Weitere mögliche Maßnahmen sind, dass die an den Verarbeitungsvorgängen beteiligten Personen sensibilisiert werden, der Zugang zu den Daten innerhalb der verantwortlichen Stelle beschränkt wird und Maßnahmen eingeführt werden, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind.

Bei genauerer Betrachtung der in § 22 Abs. 2 BDSG aufgezählten technisch-organisatorischen Maßnahmen (insbesondere der Ziff. 1, 2, 5, 6 und 7) fällt auf, dass diese Maßnahmen trotz des Wortlauts („*soll*“) nicht nur optionale Vorschriften im Rahmen von SPA darstellen, sondern vielmehr zwingend sind. Der Datenverarbeiter hat ein hohes, aber (in Bezug auf die hierdurch entstehenden Kosten) risikoadäquates Datenschutzniveau zu gewährleisten. So erfordert es weder großen technischen noch finanziellen Aufwand, die Server, auf denen solche Daten gespeichert werden, entsprechend dem Stand der Technik zu verschlüsseln, die Datenverarbeitung unter Pseudonymen erfolgen zu lassen und den Zugang zu solchen Daten zu beschränken. Dies sind Grundanforderungen an einen technischen Datenschutz, die bei allen Verarbeitungsvorgängen eingehalten werden sollten, insbesondere aber bei sensitiven Daten zwingend einzuhalten sind.

Schwieriger ist die Frage zu beantworten, ob die Verarbeitung solcher Kategorien von Daten im Rahmen von SPA für der in § 26 Abs. 3 BDSG genannten Rechte und Pflichten erforderlich sind.

Pflichten aus dem Arbeitsrecht könnten sich insbesondere aus den Arbeitsschutzgesetzen sowie § 618 BGB ergeben: So bestimmt § 3 ArbSchG, dass der Arbeitgeber verpflichtet ist, die erforderlichen Maßnahmen des Arbeitsschutzes *unter Berücksichtigung der Umstände* zu treffen, die Sicherheit und Gesundheit der Beschäftigten bei der Arbeit beeinflussen. Dabei hat der Arbeitgeber ebenfalls die Maßnahmen auf ihre Wirksamkeit zu überprüfen und erforderlichenfalls sich ändernden Gegebenheiten anzupassen. § 5 ArbSchG in Verbindung mit § 3 ArbStättV konkretisiert die Pflichten des Arbeitgebers dahingehend, dass er auch eine Gefährdungs-

beurteilung der Arbeitsstätten vorzunehmen hat, wobei alle möglichen Gefährdungen der Sicherheit und der Gesundheit der Beschäftigten zu beurteilen sind, bei der ebenfalls die physischen und psychischen Belastungen zu berücksichtigen sind. Dementsprechend müssen entsprechende Maßnahmen zum Schutz der Beschäftigten getroffen werden. Eine Spezialregelung für Mütter findet sich in § 9 MuSchG, wonach der Arbeitgeber bei der Gestaltung der Arbeitsbedingungen einer schwangeren oder stillenden Frau alle auf Grundlage einer Gefährdungsbeurteilung erforderlichen Maßnahmen für den Schutz der psychischen und physischen Gesundheit der Mutter sowie des Kindes zu treffen hat, die Maßnahmen auf die Wirksamkeit zu prüfen und erforderlichenfalls den sich ändernden Gegebenheiten anzupassen hat.

Daneben sind allgemeine gesetzliche Pflichten des Arbeitgebers zu berücksichtigen, die ihn zum Schutz der Gesundheit der Arbeitnehmer verpflichten (so z.B. §§ 617 ff. BGB und noch relevanter § 62 HGB).[999] Nicht nur gesetzliche Pflichten, sondern auch arbeitsvertragliche (Fürsorge-)Pflichten können den Arbeitgeber zur Erhebung von Gesundheitsdaten berechtigen und verpflichten; § 26 Abs. 3 S. 1 BDSG ist nicht auf gesetzliche Pflichten beschränkt.[1000] So nennt die Gesetzesbegründung ausdrücklich das Beispiel der Verarbeitung von Daten zur Beurteilung der Arbeitsfähigkeit.[1001]

Eine effektive Überprüfung der Wirksamkeit sowie die Reaktion auf verändernde Gegebenheiten ist dem Arbeitgeber aber nur möglich, wenn er bestimmte Gesundheitsdaten des Arbeitnehmers verarbeiten kann. Aus diesem Grund wird man insbesondere im Bereich des Gesundheitsschutzes eine Zulässigkeit der Verarbeitung sensitiver Daten aus den arbeitsschutzrechtlichen Spezialgesetzen in Verbindung mit § 26 Abs. 3 BDSG herleiten müssen. Um nicht nur retroaktiv, sondern aus prospektiv handeln zu können, sind SPA erforderlich, um ggf. steigende Gefährdungen oder verändernde Umstände frühzeitig zu erkennen und gegebenenfalls erforderliche Maßnahmen einleiten zu können. Allerdings muss in diesem Zusammenhang genau darauf geachtet werden, *welche Daten* zwingend für den Gesundheitsschutz erforderlich sind, denn nur solche dürfen nach § 26 Abs. 3 BDSG durch Arbeitgeber im Rahmen von Simple People Analytics verarbeitet werden. Bei diesen Daten sprechen auch gewichtige Belange der Beschäftigten (z.B. das Grundrecht auf körperliche Unversehrtheit aus

999 *Martini/Botta*, NZA 2018, 625 (632 f.).
1000 *Wybitul*, NZA 2017, 413 (417); *Martini/Botta*, NZA 2018, 625 (633).
1001 BT-Drs. 18/11325, S. 98.

Art. 3 Abs. 1 EU-GRC bzw. Art. 2 Abs. 2 S. 1 GG) für eine Verarbeitung der Daten; hier ist weitestgehend von einem Gleichlauf der Interessen auszugehen, sodass eine Verarbeitung der Daten für diese Zwecke unter den genannten Voraussetzungen grundsätzlich als zulässig zu betrachten ist.

Sollen Daten hingegen nur zur Gesundheitsvorsorge verarbeitet werden, so ist darauf zu achten, dass eine solche Verarbeitung nicht durch den Arbeitgeber selbst vorgenommen werden darf, sondern gem. § 22 Abs. 1 Nr. 1 lit. b BDSG nur von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen. Möglich ist auch eine Verarbeitung unter deren Verantwortung (Auftragsverarbeitung).

c) Möglichkeit des Abschlusses einer Betriebsvereinbarung

Als weitere Möglichkeit der Legitimation der Datenverarbeitung bietet sich auch der Abschluss einer Betriebsvereinbarung nach § 26 Abs. 4 S. 1 BDSG an, in denen die Betriebspartner nach Maßgabe von Art. 88 DSGVO *spezifischere* Vorschriften zur Datenverarbeitung treffen können.[1002] Da weder § 26 Abs. 4 BDSG noch Art. 88 Abs. 1 DSGVO eine Ermächtigungsgrundlage für die Vereinbarung von Betriebsvereinbarungen vorsehen, sondern lediglich statuieren, dass durch Kollektivvereinbarungen Datenvereinbarungen legitimiert werden können, müssen die allgemeinen Voraussetzungen des § 77 BetrVG eingehalten werden.[1003] So bestimmt § 77 Abs. 2 BetrVG, dass Betriebsvereinbarungen von Betriebsrat und Arbeitgeber gemeinsam zu beschließen und schriftlich niederzulegen sind. Sie müssen von beiden Seiten unterzeichnet werden, sofern sie nicht auf einem Spruch der Einigungsstelle beruhen und im Betrieb an geeigneter Stelle ausgelegt werden. Nach § 77 Abs. 4 BetrVG haben sie normative Wirkung und gelten somit für alle Arbeitsverhältnisse im betreffenden Betrieb, ohne dass es hierfür einer individualvertraglichen Implementierung bedarf. Wie schon unter **D. § 2 I** erörtert, werden People Analytics-Verfahren selten nur auf Betriebsebene umgesetzt, sodass nach § 50 Abs. 1 BetrVG der Gesamtbetriebsrat (sofern vorhanden) oder gar nach § 58 Abs. 1 BetrVG der Konzernbetriebsrat – je nach Reichweite der Imple-

1002 Siehe grundlegend bereits **D. § 1 V. 1**.

1003 *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 247.

mentierung derartiger Verfahren – richtiger Ansprechpartner für solche Vereinbarungen ist.

Betriebsvereinbarungen können ebenfalls – wie § 26 Abs. 4 S. 1 BDSG ausdrücklich klarstellt – die Verarbeitung sensitiver Daten legitimieren.

aa) Einhaltung der Datenschutzgrundsätze erforderlich

Aufgrund der Formulierung in Art. 88 Abs. 1 DSGVO, aber auch der Voraussetzung des § 26 Abs. 4 S. 2 BDSG i.V.m. Art. 88 Abs. 2 DSGVO können die Betriebspartner weder auf den Grundsatz der Datenminimierung noch auf die grundsätzliche Zweckbindung und Rechtmäßigkeit der Datenverarbeitung verzichten.[1004]

Ebenfalls muss die Verarbeitung aufgrund einer Betriebsvereinbarung für alle Beschäftigten transparent sein. Es müssen auf jeden Fall die Datenverarbeitungsgrundsätze aus Art. 5 DSGVO eingehalten werden, wobei – wie bereits erläutert[1005] – den Betriebspartnern den Betriebspartnern eine Einschätzungsprärogative zusteht.

bb) Erfasster Personenkreis geringer als nach § 26 Abs. 8 BDSG

Der Betriebsrat kann im Rahmen von Betriebsvereinbarungen nur die in § 5 BetrVG genannten Personen vertreten. Nach Absatz 1 sind dies Angestellte, Auszubildende sowie in der Hauptsache für den Betrieb tätige Heimarbeiter.[1006] Es sind daher nicht alle in § 26 Abs. 8 BDSG genannten Personen wie beispielsweise Bewerber oder arbeitnehmerähnliche Personen erfasst. Die wichtigste Ausnahme dürfte § 5 Abs. 3 BetrVG statuieren: Die Ausnahme für leitende Angestellte; für deren Belange ist der Sprecherausschuss nach § 25 Abs. 1 SprAuG zuständig.

Auch für diese Personengruppen kann jedoch durch Betriebsvereinbarung eine Erhöhung des Datenschutzniveaus zu erreicht werden, indem Arbeitgeber und Betriebsrat statuieren, dass die Vereinbarung wie ein Vertrag zugunsten Dritter gem. § 328 BGB wirken soll, an welchen (le-

1004 Ausführlich hierzu **D. § 1 IV**.
1005 Siehe **D. § 1 V. 2**.
1006 *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 252.

diglich) der Arbeitgeber gebunden ist.[1007] Mangels normativer Wirkung für diese Gruppen, kann eine Betriebsvereinbarung jedoch datenschutzrechtlich nicht legitimierend wirken.[1008] Sprecherausschüsse können mit Sprechausschussrichtlinien nach § 28 SprAuG eigene Verarbeitungsgrundlagen schaffen.[1009]

Relevant ist diese Beschränkung jedoch vor allem für Bewerberdaten, denn hier können Betriebsrat und Arbeitgeber keine spezifischen Regelungen treffen, die Nachteile für die Bewerber bringen könnten, da es sich insoweit um einen unzulässigen Vertrag zu Lasten Dritter handeln würde bzw. die unmittelbare Regelungswirkung des § 77 Abs. 4 BetrVG sich gerade nicht auf diese Personengruppe erstreckt.[1010] Zwar hat der Betriebsrat aus den §§ 92, 94 f. und 99 BetrVG Mitwirkungsrechte auch bezüglich Bewerbern, dennoch lässt sich hieraus kein (datenschutzrechtliches) Mandat für die Gruppe der Bewerber ableiten.[1011] Geregelt werden können daher allenfalls datenschutzrechtliche Bestimmungen für die Daten, die dem Betriebsrat zu übermitteln sind, wobei auch hier die Einschränkung gilt, dass lediglich ein zusätzlicher Schutz zum bereits durch das gesetzliche Datenschutzrecht vorhandenen geschaffen werden darf (z.B. Verkürzung von Speicherfristen für Bewerberunterlagen, weitergehende Auskunfts- und Informationspflichten des Arbeitgebers), nicht hingegen Spezialregelungen, die die gesetzlichen Regelungen (teilweise) verdrängen.

cc) Möglicher Inhalt der Betriebsvereinbarung

In der Betriebsvereinbarung können Arbeitgeber und Betriebsrat festlegen, dass sie die Verarbeitung von Arbeitnehmerdaten zum Zwecke von SPA als erforderlich ansehen und daher die Verarbeitung durch die BV legiti-

---

1007 So z.B. für Abfindungen aus einem Sozialplan auch für leitende Angestellte bereits BAG, Urt. v. 31.01.1979 – 5 AZR 454/77, BAGE 31, 266 = NJW 1979, 1621 Ls. 2.

1008 Für leitende Angestellte *Dzida/Grau*, DB 2018, 189 (191).

1009 *Dzida/Grau*, DB 2018, 189 (191); BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 53.

1010 Wie hier *Bausewein*, DuD 2016, 139 (140).

1011 So aber *Kort*, NZA-Beilage 2016, 62 (65), der hierbei auch auf die Möglichkeit des Abschlusses einer freiwilligen Betriebsvereinbarung hinweist, ohne hierauf einzugehen, dass auch solche nur für die in § 5 BetrVG genannten Personen eine rechtlich bindende Wirkung nach § 77 Abs. 4 BetrVG entfalten kann.

mieren. In diesem Rahmen werden dann spezifische Vorschriften zum Umgang mit den Arbeitnehmerdaten sowie zu den SPA selbst festgelegt.

Da nach der obigen Definition von SPA lediglich bereits vorhandene Werte fortgeschrieben werden und keine weiteren Daten z.B. durch Analyse von Logdateien von Computern o.ä. gesammelt oder generiert werden, besteht für die Analytics kein Mitbestimmungsrecht aus § 87 Abs. 1 BetrVG in Bezug auf die analysierten Arbeitnehmer.[1012] Zwar handelt es sich grundsätzlich um Personalplanungsmaßnahmen im Sinne von § 92 Abs. 1 BetrVG; allerdings hat der Betriebsrat aber nur einen Anspruch auf umfassende und rechtzeitige Unterrichtung.[1013] Es besteht aber ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG im Hinblick auf die Nutzung der Software durch das HR-Management. Beim Zugriff auf die Software werden nämlich IT-Daten generiert, die Rückschlüsse auf die Leistung oder das Verhalten der Personalsachbearbeiter haben könnten.

Über den Inhalt der Analysen von SPA kann der Betriebsrat aber dennoch keine Betriebsvereinbarung erzwingen. Möglich bleibt aber der freiwillige Abschluss. § 88 BetrVG verdeutlicht jedoch die Möglichkeit des Abschlusses freiwilliger Betriebsvereinbarungen für soziale Angelegenheiten.[1014] In dieser können aufgrund der normativen Wirkung, die auch bei freiwilligen Betriebsvereinbarungen besteht (§ 77 Abs. 4 S. 1 BetrVG nimmt insofern keine Unterscheidung vor), legitimierende Regelungen für die Datenverarbeitung für SPA nach § 26 Abs. 4 S. 1 BDSG geschaffen werden.

d) Zwischenergebnis

Die Nutzung von personenbezogenen Arbeitnehmerdaten für *Simple People Analytics* ist im Regelfall erforderlich. Wenn möglich, ohne dass die Aussagekraft der Analysen darunter leidet, müssen die Daten jedoch anonymisiert werden. In jedem Falle sind die Daten aber durch technisch-organisatorische Maßnahmen zu schützen. Hierzu gehört eine Pseudonymisierung (worunter auch entsprechende Verschlüsselung fällt) sowie eine Zugriffs-

1012 Zu den Mitbestimmungsrechten aus § 87 Abs. 1 BetrVG, siehe **D. § 2 II. 1.**

1013 Zum Mitbestimmungsrecht aus § 92 BetrVG, siehe **D. § 2 II. 4.**

1014 Die Aufzählung in § 88 BetrVG ist nicht abschließend, wie sich bereits aus dem offenen Wortlaut („insbesondere") ergibt; h.M., vgl. BAG, Beschl. v. 18.08.1987 – 1 ABR 30/86, AP BetrVG 1972 § 77 Nr. 23; BAG GS, Beschl. v. 07.11.1989 – GS 3/85, AP BetrVG 1972 § 77 Nr. 46; ferner ErfK/*Kania*, § 88 BetrVG Rn. 1 m.w.N.

kontrolle, um die Daten vor unbefugten Zugriffen Dritter zu schützen. Auch im Falle der Anonymisierung vor der Durchführung von Analytics ist zu prüfen, ob die zur Anonymisierung genutzten Daten tatsächlich für die späteren Analysevorgänge erforderlich sind. Sind sie dies nicht, so ist bereits die Nutzung der Daten für den zu legitimierenden Vorgang der Anonymisierung unzulässig. Im Rahmen der Zweckvereinbarkeitsprüfung nach Art. 6 Abs. 4 DSGVO sind unter anderem die möglichen Folgen für den Beschäftigten zu berücksichtigen; hier darf bei SPA davon ausgegangen werden, dass der Kompatibilitätstest positiv ausfällt, da grundsätzlich keine neuen persönlichkeitsrelevanten Daten geschaffen werden, sondern lediglich mit Hilfe einfachster statistischer Methoden die Daten fortgeschrieben werden; eine Nachvollziehbarkeit ist hier auch ohne mathematische Kenntnisse grundsätzlich gegeben.

Für SPA dürfen unter bestimmten Umständen auch sensitive Daten im Sinne des Art. 9 DSGVO genutzt werden. Dies gilt etwa im Bereich des Arbeitsschutzes und der Gesundheitsvorsorge, da hier den Arbeitgeber nicht zuletzt aus seiner Fürsorgepflicht gem. § 241 Abs. 2 BGB Pflichten treffen, die eine Verarbeitung der Daten erforderlich machen und somit nach § 26 Abs. 3 S. 1 BDSG legitimieren. Diese Daten bedürfen nach § 22 Abs. 2 BDSG eines besonderen Schutzes, der durch technisch-organisatorische Maßnahmen herzustellen ist.

Obwohl in dieser Arbeit die Auffassung vertreten wird, dass die Nutzung personenbezogener Arbeitnehmerdaten für SPA erforderlich ist nach § 26 Abs. 1 BDSG, ist die bevorzugende Variante der Abschluss einer (die Datenverarbeitung legitimierenden) Betriebsvereinbarung, die den Komplex der Simple People Analytics ausführlich regelt. Hierfür sprechen mehrere Gründe: Einerseits erhöht dies die Akzeptanz für *Analytics*-Maßnahmen bei den Beschäftigten[1015], andererseits können rechtliche Unsicherheiten bei der Einschätzung hierdurch aus dem Weg geschaffen werden. Die Betriebsvereinbarung schafft einen spezifischen Legitimationstatbestand, sodass im Streitfall ein Gericht nicht die Erforderlichkeit von SPA bezweifeln, sondern lediglich die Einhaltung der Grundsätze aus Art. 88 Abs. 2, Art. 5 DSGVO sowie der Grenzen aus § 75 Abs. 2 BetrVG überprüfen kann.

1015 *Bodie et al.*, Colorado Law Review 2017, 961 (1036 f.).

2. Fortgeschrittene People Analytics

In Abgrenzung zu den Simple People Analytics sind fortgeschrittene People Analytics oder **Advanced People Analytics** (im Folgenden: **APA**) Methoden, die nicht mehr mit Hilfe einfacher Statistik (z.B. linearer Regression) zu bewerkstelligen sind. Mithilfe komplexer Algorithmen (z.B. multivariate Regression, Einsatz künstlicher Intelligenz bzw. neuronaler Netze) und Auswertung von Echtzeit-Daten sollen Vorhersagen über das (Arbeits-)Verhalten oder sonstige Eigenschaften der Arbeitnehmer getroffen werden. Dies kann so weit führen, dass Arbeitnehmer „gescored" werden und mit Hilfe dieses Scores in bestimmte Kategorien eingeordnet werden (z.B. zuverlässiger Arbeitnehmer, unzuverlässiger Arbeitnehmer, leistungsfähiger aber unzuverlässiger Arbeitnehmer etc.).

Der Score stellt beispielsweise eine Zahl zwischen 1 und 10 dar, die einen Wahrscheinlichkeitswert für zukünftiges Verhalten repräsentiert und aus den verschiedenen zugrundeliegenden Daten anhand eines bestimmten Algorithmus (unter Vergleichsbetrachtung zu anderen Arbeitnehmern) generiert wird. Hierdurch können im Anschluss Personalverantwortliche z.B. im Falle des Einsatzes künstlicher Intelligenz die Vorschläge des Algorithmus bewerten und ggf. nachbessern, aus welchen der Algorithmus dann wiederum „lernt", indem er den Input zum Output erneut in die Berechnungen einfließen lässt.

Mit Hilfe von APA sollen Daten geschaffen oder Umstände aufgedeckt werden, die mit klassischen Methoden oder durch nur durch menschliche Rechenarbeit nur schwer oder unmöglich erkennbar sind. In aller Regel ist für solche Analysen eine sehr große Datenbasis (*Big Data*) notwendig. Dies rührt aus dem Umstand, dass zu Beginn der Analysen oftmals nicht feststeht, welche Daten letztendlich von Relevanz sind.

Bei Advanced People Analytics liegt in aller Regel ein Profiling nach Art. 4 Nr. 4 DSGVO vor, da hier – anders als bei den SPA – eine Bewertung persönlicher Aspekte durch automatisierte Verarbeitung im Vordergrund steht.[1016]

Im Folgenden müssen mehrere Schritte geprüft werden, um eine rechtliche Bewertung von APA vornehmen zu können: Zunächst muss in einem ersten Schritt (a) die Datengrundlage geklärt werden. Da bei APA deutlich mehr Daten herangezogen werden müssen, sind etwaige Grenzen aus dem Datenschutz- und insbesondere auch (aufgrund der vorherrschenden

1016 Siehe bereits **E. § 1 II.**

Auffassung der Datenschutzbehörden[1017]) Telekommunikationsrecht zu beachten. In einem weiteren Schritt muss die grundsätzliche Zulässigkeit solcher Auswertungen (*Profiling*) durch Arbeitgeber eingeschätzt werden (b), bevor im weiteren Verlauf die Erstellung von Scores als Grundlage für weitere Analytics (c) analysiert und rechtlich beurteilt wird. Ferner soll – analog der Vorgehensweise bei einfachen People Analytics – geklärt werden, inwiefern eine Einwilligung ein tauglicher Legitimationstatbestand darstellen könnte, ob solch weitgehende Analysen als „erforderlich" im Rahmen von § 26 Abs. 1 BDSG angesehen werden oder ob ggf. andere Legitimationstatbestände aus Art. 6 DSGVO herangezogen werden müssen. Zum Abschluss wird wiederum analysiert, ob APA grundsätzlich durch Betriebsvereinbarungen legitimiert werden können.

a) Die Datengrundlage bei fortgeschrittenen People Analytics

aa) Stark erweiterte Datenbasis durch Digitalisierung der Arbeitswelt (Arbeit 4.0)

Neben den klassisch vorhandenen Stamm- und Leistungsdaten (etwa aus Leistungsbeurteilungen) benötigt APA eine deutlich größere Datenbasis. Insbesondere, wenn etwa „Live-Auswertungen" erstellt werden sollen, ist es nicht ausreichend, dass nur etwa monatlich, quartalsweise oder nur jährlich erfolgende Leistungsbeurteilungen der Arbeitnehmer das Datenbasis herangezogen werden, da hierdurch nur sehr träge auf etwaige Veränderungen reagiert werden könnte. Aus diesem Grund müssen Datensätze gesucht werden, die ein aktuelles Abbild des Verhaltens oder der Leistung der Beschäftigten abbilden, wie etwa IT-Nutzungs- und Sensordaten.[1018] Aufgrund der zunehmenden Digitalisierung des Arbeitslebens[1019] fallen

1017 Diese sind der Auffassung, dass bei erlaubter Privatnutzung von betrieblicher Infrastruktur der Arbeitgeber Telekommunikationsanbieter im Sinne des TKG ist; diese Auffassung ist zwar nicht überzeugend, aufgrund der Rechtsunsicherheit und der strafrechtlichen Sanktionsgefahr ist dies in der Praxis aber weiterhin zu beachten, vgl. hierzu **D. § 3**.

1018 Eine beispielshafte Aufzählung möglicher Datensätze für *People* oder *Workforce Analytics* ist unter **C. § 1** zu finden; weitere Beispiele nennt *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 4 DSGVO Rn. 7.

1019 *Däubler*, Digitalisierung und Arbeitsrecht, S. § 1 Rn. 11 ff.; *Däubler*, AuR Sonderausgabe Juli 2016, 2; speziell zu Big Data *BMAS*, Weißbuch Arbeiten 4.0, S. 62 ff.

nicht nur an Computerarbeitsplätzen, sondern an jeglichen Arbeitsplätzen entsprechende IT-Daten an.[1020] Sei es beim Außendienstmitarbeiter durch das Mobiltelefon oder ein im Kfz eingebautes Ortungsmodul, bei der Kassiererin an der Supermarktkasse das digitale Kassensystem, das die Eingaben erfasst oder beim Lagermitarbeiter die benutzten Scanner zur Warenerfassung[1021]. Mit zunehmender Digitalisierung kommen weitere Daten beispielsweise von Smart Glasses, anderen *Wearables* oder digitalen Assistenten hinzu.[1022] Da Wearables eine besonders neuartige Erscheinung sind, werden diesen in der nachfolgenden Analyse besondere Beachtung geschenkt.

bb) Zulässigkeit der Erhebung von IT-Nutzungs- und -Sensordaten

Anders als bei SPA, wo die zulässige Erhebung der Daten für die Zwecke dieser Arbeit angenommen wird, ist bei APA zunächst zu untersuchen, inwiefern Sensordaten erhoben und für weitere Analyticszwecke verwendet werden dürfen. Dies hat den Hintergrund, dass diese Daten nicht primär für die Personalverwaltung erhoben wurden, sondern mitunter für ganz andere Zwecke wie beispielsweise der Aufrechterhaltung der Funktionsfähigkeit und Integrität von IT-Systemen oder deren Sicherheit sowie der Möglichkeit des Datenmissbräuche nachverfolgen zu können. Aufgrund der hohen Relevanz und datenschutzspezifischen Besonderheiten ist daher im Folgenden genauer darauf einzugehen, wobei in einem ersten Schritt die Erhebung solcher Daten zum Zwecke der Analytics geprüft wird, be-

1020 Diese Daten werden auch als „Metadaten" bezeichnet, vgl. *Götz*, Big Data im Personalmanagement, S. 26.

1021 So erfassen die Handscanner von Amazon angeblich nicht nur Scandaten, sondern enthalten wie Smartphones Kameras und Mikrofone und speichern detaillierte Bewegungsdaten. Zwar gibt Amazon an, keine individualisierten Evaluierungen von Bewegungsdaten zu erfassen und die Mikrofone nicht zu nutzen, andererseits berichten Beschäftigte, in Personalgesprächen mit Daten über die individuelle Arbeitsleistung konfrontiert zu werden, sodass vermutet wird, dass im Hintergrund ein automatisierter Bewertungsalgorithmus laufe, der die Daten auswerte und so Einzelbewertungen erstelle, vgl. *Staab/Nachtwey*, APuZ 2016, 24 (27).

1022 *Krause*, Forschungsbericht 482 - Digitalisierung und Beschäftigtendatenschutz, <www.bmas.de/SharedDocs/Downloads/DE/PDF-Publikationen/Forschungsberichte/fb482-digitalisierung-und-beschaeftigtendatenschutz.pdf?__blob=publicationFile&v=1>, S. 12 ff.

vor in einem zweiten Schritt auf die Verwendung von für andere Zwecke erhobenen Daten eingegangen wird.

Zuvor aber muss aber noch auf zwei Datenschutzgrundsätze, die bei der Bewertung eine maßgebliche Rolle spielen (nachfolgend (1)), kurz eingegangen sowie die maßgebliche Legitimationsnorm als Dreh- und Angelpunkt der Zulässigkeitsuntersuchung (2) herausgearbeitet werden.

(1) Privacy by Design und Privacy by Default

Der europäische Gesetzgeber hat den in Art. 5 Abs. 1 lit. c DSGVO festgelegten Grundsatz der Datenminimierung und den in lit. e niedergeschriebenen Grundsatz der Speicherbegrenzung positivrechtlich durch die Aufnahme der Grundsätze *Privacy by Design* und *Privacy by Default* als technisch-organisatorische Maßnahmen in Art. 25 DSGVO gestärkt.[1023] Hiernach müssen nach Möglichkeit und Risiko bereits entsprechende technische Maßnahmen wie eine Pseudonymisierung in die Software integriert werden sowie datenschutzfreundliche Einstellungen als Standard ausgewählt sein. Diese Ansätze verfolgen das Ziel, dass die datenschutzrechtlichen Anforderungen am effektivsten umgesetzt werden können, wenn sie bereits in frühen Planungsphasen der Datenverarbeitungssysteme berücksichtigt und integriert werden.[1024] Allerdings ist diese Vorschrift auf den ersten Blick misslungen, da sie die Datenverarbeiter und nicht die Hersteller, die gerade solche Systeme konzipieren und programmieren, in die Pflicht nimmt.[1025] Im Ergebnis werden aber die Verarbeiter die Hersteller dazu drängen, ihre Systeme entsprechend zu konzipieren, da sie diese ansonsten nicht einsetzen dürfen. Mittelbar wird die Vorschrift also Auswirkungen auf die Hersteller haben und somit das damit verfolgte Ziel erreicht werden können.

Aufgrund dieser Vorgaben ist davon auszugehen, dass nicht alle für fortgeschrittene People Analytics nützliche Daten bereits automatisch von

---

1023 *Hackenberg*, Teil 15.2 Big Data und Datenschutz, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Rn. 44.

1024 Paal/Pauly/*Martini*, Art. 25 DSGVO Rn. 10; *Jandt*, DuD 41(9) (2017), 562; *EDPS*, Opinion 7/2015 - Meeting the challenges of big data, <edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf>, S. 14 f.; so bereits *Roßnagel*, MMR 2005, 71 (74): "*Die Einhaltung von Verarbeitungsregeln zu kontrollieren, darf nicht eine permanente persönliche Aufmerksamkeit erfordern, sondern muss automatisiert erfolgen.*"

1025 Kritisch daher auch *Jandt*, DuD 41(9) (2017), 562 (563).

den Systemen erfasst werden und einfach zweckändernd weiterverarbeitet werden können. Eine Speicherung solcher Daten ist in der Regel aktiv vom Arbeitgeber zu veranlassen. Aufgrund dieser Grundsätze, aber auch aufgrund § 26 Abs. 1 BDSG bzw. Art. 6 Abs. 1 lit. f DSGVO ist im Detail zu prüfen, welche Daten erforderlich sind.

(2) Maßstab der Beurteilung der Rechtmäßigkeit: § 26 Abs. 1 BDSG und/oder Art. 6 Abs. 1 lit. f DSGVO

Die Erforderlichkeit der Daten für die Entscheidung über die Begründung, die Durchführung oder Beendigung des Beschäftigungsverhältnisses ist – wie im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO – im Ergebnis eine Verhältnismäßigkeitsprüfung,[1026] die auf einer Abwägung der jeweiligen Grundrechte und Interessen basiert.

Neben der Spezialregelung gem. § 26 Abs. 1 S. 1 BDSG zum Beschäftigtendatenschutz kann die „Auffangklausel" des Art. 6 Abs. 1 lit. f DSGVO eingreifen,[1027] wenn es sich um Daten handelt, die nicht für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich sind, die Daten also anderen Zwecken dienen. Ein Beispiel hierfür wäre, dass Beschäftigtendaten im Rahmen einer Due Diligence bei einem Unternehmenskauf verarbeitet werden.[1028] Mangels Regelungskompetenz der Mitgliedstaaten kann es in diesem Bereich auch bei Beschäftigtendaten nicht zu einem Ausschluss der allgemeinen Erlaubnistatbestände kommen.[1029] Wie das Beispiel zeigt, dürfte der Rückgriff auf Art. 6 DSGVO aber deswegen eher die Ausnahme sein,[1030] da die Zweckbestimmung „Durchführung des Arbeitsverhältnisses" sehr weit zu verstehen ist.[1031] Es gibt jedoch auch Fälle, in denen die Datenverarbeitung von Daten eines bestimmten Arbeitnehmers nicht für die Durchführung

1026 Zu den Kriterien der Erforderlichkeit im Rahmen von § 26 Abs. 1 BDSG, siehe **D. § 1 IV. 2. b)** sowie **E. § 1 I. 1. b)**.

1027 ErfK/*Franzen*, § 26 BDSG Rn. 4 f.; *Kainer/Weber*, BB 2017, 2740 (2743); *Kort*, NZA 2018, 1097 (1099 f.); *Kramer*, NZA 2018, 637 (638); *Ströbel et al.*, CCZ 2018, 14 (19); so wohl auch LAG Hamm, Beschl. v. 19.09.2017 – 7 TaBV 43/17, ZD 2018, 129 (131) Rn. 35.

1028 *Kort*, NZA 2018, 1097 (1099).

1029 *Ströbel et al.*, CCZ 2018, 14 (19).

1030 So auch *Kramer*, NZA 2018, 637 (638).

1031 *Zöll*, in: Taeger/Gabel, DSGVO - BDSG, § 26 BDSG Rn. 38 Hierzu bereits oben **E. § 1 I. 1. b) bb)**.

dessen Arbeitsverhältnisses erforderlich sind, sondern für die Zwecke eines anderen Beschäftigungsverhältnisses verarbeitet werden sollen.[1032] Das wäre beispielsweise dann der Fall, wenn für ein Scoring aggregierte Daten als Vergleichsbasis herangezogen werden sollen.[1033] Für den Anonymisierungsvorgang der Daten eines anderen Arbeitnehmers ist nicht § 26 Abs. 1 BDSG die einschlägige Legitimationsgrundlage, sondern Art. 6 Abs. 1 lit. f DSGVO.

Die beiden Tatbestände schließen sich insofern auch gegenseitig aus: Werden die Daten für die Zwecke des Beschäftigungsverhältnisses verarbeitet, ist § 26 Abs. 1 BDSG die einschlägige Norm zur Beurteilung der Rechtmäßigkeit, während für alle anderen Zwecke die allgemeinen Tatbestände aus Art. 6 Abs. 1 DSGVO anwendbar bleiben. Im Endeffekt führt dies – jedenfalls bei Maßnahmen, die nicht der Aufdeckung von Strafdaten dienen[1034] – zum selben Ergebnis: Wie bereits gezeigt wurde, ist auch im Rahmen von § 26 Abs. 1 S. 1 BDSG die Erforderlichkeit mehr als ein Abwägungsgebot zu verstehen als eine strikte Erforderlichkeit, wobei die Verarbeitungsinteressen des Arbeitgebers mit den Geheimhaltungsinteressen des Arbeitnehmers abzuwägen und praktische Konkordanz herzustellen ist. Nichts anderes gilt im Rahmen der Interessensabwägung nach Art. 6 Abs. 1 lit. f DSGVO, mit der Folge, dass Arbeitgeber zwar bei der Angabe der Legitimationsgrundlage im Verzeichnis der Verarbeitungstätigkeiten die korrekte Norm nennen müssen, sich aber inhaltlich an der Abwägungsentscheidung nichts ändert.[1035]

Wenn eine Maßnahme nach § 26 Abs. 1 S. 1 BDSG zulässig ist, so ist sie es auch außerhalb des Kontextes des konkreten Beschäftigungsverhältnisses im Rahmen von Art. 6 Abs. 1 lit. f DSGVO und vice versa, wenn

---

1032 Dagegen WHWS/*Byers*, B. VII. GPS-Ortung, Rn. 27: Zu den Rechten aus dem Beschäftigungsverhältnis gehört auch die Organisation des Betriebs, weshalb eine hierfür erforderliche Datenverarbeitung ebenfalls unter § 26 Abs. 1 S. 1 BDSG zu subsumieren ist.

1033 So wohl auch *Rudkowski*, NZA 2019, 72 (73).

1034 Repressive Maßnahmen sind dem Bereich der *Compliance* zuzuordnen und daher nicht Teil dieser Untersuchung.

1035 Dies kann mitunter auch damit begründet werden, dass auch im Rahmen der Abwägung von § 26 Abs. 1 BDSG subsidiär die Grundrechte aus der EU-GRC den Abwägungsmaßstab festlegen. Selbst wenn unterschiedliche Grundrechte herangezogen würden, wäre von einem Gleichlauf der Interessensabwägung bei europäischen und nationalen Grundrechten auszugehen (so wohl auch der deutsche Gesetzgeber, der die bisherige Regelung des § 32 BDSG a.F. schlicht fortführen wollte, vgl. BT-Drs. 18/11325, S. 96 f.); siehe hierzu bereits **D. § 1 IV. 2. b**).

die beiderseitigen Interessen identisch sind.[1036] Auch bei der Abwägung der berechtigten Interessen ist das besondere Abhängigkeitsverhältnis zwischen Arbeitgeber und Arbeitnehmer zu berücksichtigen, sodass keine milderen Voraussetzungen gelten.

cc) Erhebung von IT-Nutzungs- und Sensordaten für Analyticszwecke

(1) Log-Daten von IT-Systemen

Wie bereits angedeutet, fallen bei der Nutzung von IT-Systemen gewisse System- und Logdaten an, die von der jeweiligen Anwendung bzw. dem Betriebssystem zum Zwecke der Fehleranalyse für einen gewissen Zeitraum gespeichert werden.[1037] Der Umgang des Systems mit den Log-Files kann in aller Regel durch den Systemadministrator konfiguriert werden.[1038]

Bereits nach dem alten Datenschutzrecht war anerkannt, dass auch für Log-Dateien die Grundsätze der Erforderlichkeit, Angemessenheit und Zweckbindung der Daten einzuhalten sind, wobei im Hinblick auf die Zweckbindung bereits im Vorfeld präzise Aussagen zur Zielstellung von Protokollen erforderlich und allgemeine Formulierungen wie „Gewährleistung der Datensicherheit und Sicherungszwecke" unzureichend sind.[1039] Aus diesem Grund dürfen auch nur so wenig personenbezogene Daten gespeichert werden, wie möglich; wenn der Zweck es zulässt, ist zu anonymisieren und/oder – falls eine Anonymisierung ausscheidet – pseudonymisieren.[1040]

1036 *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 18 unter Verweis auf BAG, Urt. v. 12.02.2015 – 6 AZR 845/13, NZA 2015, 741 Das Gericht ließ es hierbei im Rahmen einer Verdachtskündigung dahinstehen, ob § 32 Abs. 1 S. 1 BDSG a.F. oder § 28 Abs. 1 S. 1 Nr. 2 BDSG a.F. einschlägig ist.

1037 Vgl. hierzu auch HdbIT-DSR/*Conrad/Schneider*, § 14 Softwarepflege und Support, Rn. 127.

1038 Bei Linux beispielsweise durch das in alle Distributionen integrierte Tool „logrotate", mit welchem solche Dateien automatisch komprimiert, nach einem bestimmten Zeitraum gelöscht oder an bestimmte Personen gesendet werden können, vgl. https://linux.die.net/man/8/logrotate (letzter Abruf am:: 30.01.2020); zur Praxis der Systemprotokollierung bei UNIX-basierten Systemen, siehe *Seeger*, DuD 2006, 285; zu den Grundlagen der Windows-Protokollierung, siehe *Marnau*, DuD 2006, 288.

1039 *Knorr*, DuD 2006, 268.

1040 *Knorr*, DuD 2006, 268; *Kort*, NZA 2011, 1319 (1320 f.).

Wesentlich ist, dass Logdateien also nicht ausschließlich anonyme Systemdaten erfassen, sondern mitunter auch personenbezogene, wenn die jeweilige Anwendung bzw. das System die Benutzererkennung bei der Speicherung miterfasst oder sich aus anderen Umständen ergibt, dass ein bestimmter Arbeitnehmer gerade das System benutzt hat.

Beispiel: Eine Website löst einen Darstellungsfehler aus, die vom Browser erfasst wird. Der Browser speichert die Fehlermeldung inklusive der Adresse der Website im Fehlerlog. Anhand einer späteren Auswertung des Systemlogs und der Kenntnis, dass ein bestimmter Arbeitnehmer in dieser Zeit den Computer nutzt, lässt sich – ohne den Browserverlauf explizit zu prüfen – feststellen, dass Arbeitnehmer X zu einer ganz bestimmten Uhrzeit die Website aufgerufen hat. Ist beispielsweise die Privatnutzung des Internets verboten, so ließe sich allein durch die Fehlermeldung ein Verstoß gegen arbeitsvertragliche Pflichten feststellen.

Solche Log-Daten können (unerwünschte) Login-Versuche, E-Mail-Transport- und -Abruf-Daten, Zugriffe auf Webseiten oder Dateien, Nutzungen von Anwendungen, Firewall-Daten etc. enthalten. Der Anfall an solchen Daten ist vielfältig und mitunter sehr weitreichend.

Grundsätzlich kann davon ausgegangen werden, dass die Daten zur Gewährleistung eines sicheren und fehlerfreien IT-Betriebs erforderlich sind.[1041] Problematisch ist, dass im betrieblichen Bereich die Administratoren unter Druck gesetzt werden könnten, zur Überwachung der Arbeitsleistung oder aus anderen Gründen auf die Logdateien, die bestimmte Mitarbeiter betreffen, zuzugreifen.[1042] Allerdings sieht bereits die DSGVO gewisse Protokollierungen vor, wenn sie den Verarbeitern in Art. 32 im Rahmen der technisch-organisatorischen Maßnahmen vorschreibt, Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzuführen.[1043] Datenschutzverstöße müssen nach Art. 33 an die Behörden und nach Art. 34 an die Betroffenen gemeldet werden, was ohne eine Protokollierung der Zugriffe nur schwer möglich ist. Für sensitive Daten im Sinne des Art. 9 DSGVO schreibt § 22 Abs. 2 S. 2 Ziff. 2 BDSG als mögliche Garantie sogar explizit

1041 *Heidrich/Wegener*, MMR 2015, 487.

1042 *Heidrich/Wegener*, MMR 2015, 487 (490).

1043 So gehört Protokollierung zur Sicherstellung der Kontrolle der Ordnungsgemäßheit der Datenverarbeitung, bspw. durch die Revision, vgl. *Hof*, 5 Datenschutz mittels IT-Sicherheit, in: Tinnefeld et al., Einführung in das Datenschutzrecht, S. 523 Rn. 124; als mögliche TOM auch *Wolff*, E. Technisch-Organisatorische Pflichten, in: Schantz/Wolff, Das neue Datenschutzrecht, Rn. 829.

vor, dass nachträglich überprüft und festgestellt werden können muss, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind. Für öffentliche Stellen regelt § 76 BDSG bei automatisierten Verarbeitungsvorgängen bestimmte Protokollpflichten; eine vergleichbare Vorschrift gibt es für nicht-öffentliche Stellen allerdings nicht.

Sieht man die Erhebung und Speicherung von Log-Daten also als technisch-organisatorische Schutzmaßnahme zum Datenschutz an, so ist die Legitimationsgrundlage für die Erhebung solcher Daten Art. 6 Abs. 1 lit. c DSGVO. Diese Daten werden jedoch nicht für die Zwecke der *People Analytics*, sondern für die Gewährleistung der Integrität und Funktionsfähigkeit von IT-Systemen erhoben und sind daher entsprechend zweckgebunden; sie dürfen also grundsätzlich nicht für andere Zwecke verarbeitet werden.

(2) Spezifische Datenerhebung für People Analytics

Im Rahmen der Datenerhebung für People Analytics sind daher in einem ersten Schritt nur solche Erhebungs- und Verarbeitungsvorgänge zu analysieren, die nicht ohnehin bereits durch die Systeme erfasst werden. Für diese Vorgänge ist Legitimationsgrundlage der Erhebung § 26 Abs. 1 S. 1 BDSG, da diese Daten bereits mit dem Zweck der Durchführung des Beschäftigungsverhältnisses erhoben werden.[1044] Es kommt daher bereits bei der Erhebung auf die Erforderlichkeit und Angemessenheit der Datennutzung für den konkreten Zweck an, d.h. bereits vor Erhebung der Daten muss geprüft werden, ob schutzwürdige Arbeitgeberinteressen solchen des Arbeitnehmers überwiegen. Dabei muss darauf geachtet werden, dass die Erhebung von IT-Systemdaten nicht zu einer unzulässigen Dauerüberwachung führt.[1045] 2017 hat der BGH in der bekannten *Keylogger*-Entscheidung[1046] seine ständige Rechtsprechung erneut bestätigt: (Präventive) Überwachungsmaßnahmen sind grundsätzlich zulässig, sofern bei den Betroffenen kein solcher psychischer Anpassungsdruck erzeugt wird, dass

1044 Zum Zweck der Durchführung des Beschäftigungsverhältnisses siehe **E. § 1 I. 1. b) bb)**.

1045 Vgl. hierzu BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205 (1211) Rn. 30 zu § 75 II BetrVG; im Rahmen von § 26 I BDSG kann ebenso kein milderer Maßstab gelten.

1046 BAG, Urt. v. 27.07.2017 – 2 AZR 681/16, NZA 2017, 1327 = BAGE 159, 389 = CR 2018, 27.

diese bei objektiver Betrachtung in der Ausübung ihrer Freiheit und ihrem Handeln aus eigener Selbstbestimmung wesentlich gehemmt werden.[1047]

Wenn allerdings für People Analytics auch Kommunikationsdaten ausgewertet werden sollen, müssen Arbeitgeber die §§ 88 ff. TKG im Blick haben. Aufgrund der mangels höchstrichterlichen Rechtsprechung bestehenden Unsicherheit ist dem Arbeitgeber anzuraten, nach Möglichkeit die Privatnutzung des Firmennetzwerks zu verbieten, wenn diese Daten für People Analytics-Zwecke genutzt werden sollen.

Für sensitive Daten, insbesondere Gesundheitsdaten, sind die zusätzlichen Vorgaben aus Art. 9 DSGVO, § 22 Abs. 2 BDSG zu beachten.[1048] Da solche Daten nur dann genutzt werden dürfen, wenn Arbeitgeber dadurch ihre Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erfüllen oder eine Einwilligung oder Betriebsvereinbarung hierzu vorliegt, sind die Daten nur bedingt für Advanced People Analytics geeignet: Im Bereich des Arbeits- und Gesundheitsschutzes können solche Daten erhoben werden, wenn sie spezifisch diesem Zweck dienen. Eine Einwilligung im Hinblick dieser Daten ist auch im Beschäftigungsverhältnis nach § 26 Abs. 3 S. 2 BDSG grundsätzlich möglich, wobei die Freiwilligkeit problematisch sein kann.[1049] Ist sichergestellt, dass Arbeitgeber und Arbeitnehmer die gleichen Interessen verfolgen oder Analysen nur Vorteile für die Arbeitnehmer bringen, und werden diese nicht vom Arbeitgeber unter Druck gesetzt, die Einwilligung hierzu abgeben, so kann – sofern keine anderen Anhaltspunkte bestehen – von einer Zulässigkeit der Einwilligung ausgegangen werden (§ 26 Abs. 2 S. 2 BDSG). Ebenfalls möglich ist nach § 26 Abs. 4 S. 1 DSGVO der Abschluss einer Betriebsvereinbarung für die Erhebung von IT-Systemdaten (inklusive sensitiver Daten), wobei keine maßgeblichen Abweichungen vom Schutzniveau der DSGVO möglich sind. Dennoch können Spezialregelungen getroffen werden.[1050] Dies hat aber zur Folge, dass auch im Rahmen von Kollektivvereinbarungen Vorgänge der Verarbeitung von Gesundheitsdaten für Analytics-Zwecke nicht generell legitimiert werden dürfen. Vielmehr muss

---

1047 St. Rspr., vgl. statt aller BAG, Urt. v. 27.07.2017 – 2 AZR 681/16, NZA 2017, 1327 (1330) = BAGE 159, 389 = CR 2018, 27 Rn. 31; Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205; Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (Rn. 15) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54 m.w.N.

1048 Grundlegend hierzu bereits **E. § 1 III. 1. b) bb) (2)**.

1049 Zur Freiwilligkeit der Einwilligung im Beschäftigungsverhältnis, siehe **D. § 1 III. 2. a)** und **E. § 1 III. 1. a)**.

1050 Zum Verhältnis zwischen Betriebsvereinbarung und DSGVO, siehe **D. § 1 IV** und **D. § 1 V. 2**.

die gesetzgeberische Wertung beachtet werden, sensitive Daten nur zur Erfüllung arbeitsrechtlicher Pflichten zu erfassen und nutzen. Solche Pflichten des Arbeitgebers können jedoch– wie § 26 Abs. 1 S. 1 a.E. BDSG zeigt – auch durch eine Betriebsvereinbarung geschaffen werden. Hierbei haben aber die Betriebspartner die Persönlichkeitsrechte der Arbeitnehmer zu wahren (§ 75 Abs. 2 BetrVG).[1051] Dementsprechend wäre es nicht möglich, das Datenschutzrecht dergestalt zu umgehen, dass umfassende Pflichten zur Verarbeitung sensitiver Daten in der Betriebsvereinbarung zu regeln und hierdurch sogar nach § 26 Abs. 1 BDSG gesetzlich zu legitimieren. Der Maßstab im Rahmen von § 75 Abs. 2 BetrVG ist dem der Abwägung in § 26 Abs. 1 BDSG vergleichbar,[1052] wobei bei ersterer zusätzlich noch die Gesamtbelastung des Kollektivs betrachtet werden muss.[1053]

Beispiel: Während die Verarbeitung eines personenbezogenen Datums für einzelne Arbeitnehmer aufgrund ihrer Position im Unternehmen noch nicht zu einem unzulässigen Überwachungsdruck führen muss, kann bei einer Betrachtung aller Arbeitnehmer des Betriebs hingegen ein solcher vorliegen, sodass die Datenverarbeitung nach § 75 Abs. 2 BetrVG als unzulässig einzustufen ist und eine entsprechende Betriebsvereinbarung beispielsweise nicht geschlossen werden dürfte.

(3) Sensordaten von Wearables

Eine weitere, für Beschäftigungszwecke neuartige Datenquelle können Wearables darstellen, die Vitalfunktionen des Beschäftigten aufzeichnen. Das können Smartwatches oder Fitness Tracker sein. Inzwischen gibt es auch „smart clothes", die u.a. Vitalwerte aufzeichnen, aber auch andere Daten wie beispielsweise die Umgebungstemperatur oder -feuchtigkeit bei Schutzanzügen (beispielsweise der Feuerwehr) aufzeichnen können.[1054]

1051 Für eine entsprechende Abwägungspflicht auch bei gesetzlichen Pflichten, *Böhm*, NZA-RR 2019, 530 (531); *Wybitul*, NZA 2017, 413 (415 f.); dagegen BAG, Beschl. v. 07.05.2019 – 1 ABR 53/17, NZA 2019, 1218 (1222) Rn. 42.

1052 Vgl. BAG, Beschl. v. 29.06.2004 – 1 ABR 21/03, NZA 2004, 1278 (1280 f.) = BAGE 111, 173 = AP BetrVG § 87 1972 Überwachung Nr. 41 (m. Anm. Ehmann) zu den Kriterien der Abwägung.

1053 Hierzu **D. § 2 II. 1. b) ee)**.

1054 *Blinn*, Wearables und Arbeitnehmerdatenschutz - Vom freiwilligen Selbstoptimierer zum Kontrollinstrument des Arbeitgebers?, in: Taeger, Smart world - smart law?, S. 519 ff.; weitere Beispiele bei *Putschli*, DuD 2017, 721.

Diese Geräte haben gemein, dass sie Gesundheitsdaten im Sinne von Art. 4 Nr. 15 DSGVO[1055] und somit sensitive Daten nach Art. 9 DSGVO bzw. § 26 Abs. 3 S. 1 BDSG erheben und verarbeiten. Solche Daten geben besonders tiefe Einblicke in das Privatleben der Nutzer[1056] und unterliegen – wie bereits mehrfach aufgezeigt – besonders strengen Verarbeitungsbeschränkungen.[1057]

Arbeitgeber können beispielsweise Fitnessarmbänder an Arbeitnehmer verteilen, um diesen einen Anreiz zu geben, gesünder zu leben, ohne die hierdurch gewonnen Daten zu verarbeiten. Ein solcher Einsatz ist aus Arbeitgebersicht datenschutzrechtlich irrelevant. Sobald allerdings die von den Armbändern generierten Daten auch für People Analytics genutzt werden sollen, muss die Verarbeitung von solchen Daten am Maßstab des § 26 Abs. 1 S. 1, Abs. 4 S. 1 BDSG gemessen werden.

Im Bereich des Arbeitsschutzes, beispielsweise bei Sensoren in der Kleidung von Rettungs- und Feuerwehrleuten, dürfte eine datenschutzrechtliche Abwägung zugunsten des Arbeitgebers ausfallen: Die Daten werden nicht zur Leistungskontrolle, sondern zum Zwecke des Schutzes von Leib und Leben der Beschäftigten verarbeitet. Voraussetzung ist, dass nur solche Daten erhoben werden, die zum Schutz des Beschäftigten auch erforderlich sind. Zwar greift Art. 9 Abs. 2 lit. c DSGVO als Erlaubnistatbestand nicht, da dieser es erfordert, dass die betroffene Person außerstande ist, die Einwilligung zu erteilen. Legitimationsgrundlage hierfür kann aber § 26 Abs. 3 S. 1 BDSG sein, da Arbeitgeber verpflichtet sind, im Rahmen des Arbeitsschutzes, ihre Beschäftigten zu schützen. Ein weiteres Beispiel wäre das Agieren mit gefährlichen Stoffen.[1058] In diesem Fall dient die Aufzeichnung der Sensordaten nicht nur dem Schutz des konkret betroffenen Arbeitnehmers, sondern auch der anderen Beschäftigten.

Beispiel: Ein Arbeitnehmer hantiert im Labor mit einem gefährlichen Stoff, wobei hiervon eine kleine Menge dieses Stoffes austritt. Dieser Stoff ist hoch reizend, erste Symptome treten aber erst nach wenigen Minuten auf. Der Laborant merkt diesen Austritt des Stoffes nicht sofort. Die Sensoren in der smarten Kleidung erfassen den Austritt, woraufhin automatisiert ein Alarm im Labor ausgelöst wird, sodass alle im Labor Beschäftig-

1055 Auch die Schrittanzahl lässt Rückschlüsse auf den Gesundheitszustand zu und ist daher von Art. 9 DSGVO umfasst, vgl. *Blinn*, Wearables und Arbeitnehmerdatenschutz - Vom freiwilligen Selbstoptimierer zum Kontrollinstrument des Arbeitgebers?, in: Taeger, Smart world - smart law?, S. 528.

1056 *Putschli*, DuD 2017, 721.

1057 Siehe bereits **E. § 1 III. 1. b) bb) (2)**.

1058 *Kopp/Sokoll*, NZA 2015, 1352 (1356).

ten das Labor schnellstmöglich räumen können. Ohne diesen Alarm wäre es bei allen Laboranten zu einer Reizung der Augen und Schleimhäute gekommen, was eine Arbeitsunfähigkeit von mindestens zwei Tagen nach sich gezogen hätte.

Wie sich aus der Wertung des Art. 9 Abs. 2 lit. c DSGVO ergibt, sind Arbeitgeber grundsätzlich gehalten, eine Einwilligung einzuholen, falls die Sensorik ausschließlich dem Schutz des mit dieser ausgestatteten Beschäftigten dient: Art. 9 Abs. 2 lit. c DSGVO schreibt vor, dass eine Verarbeitung zum Schutz *lebenswichtiger* Interessen des Betroffenen nur zulässig ist, wenn dieser außerstande ist, eine Einwilligung zu geben. Für andere Verarbeitungen, die ausschließlich dem Schutz dienen, muss dies also erst recht gelten. Sollen hingegen auch andere Beschäftigte geschützt werden, so dient die Sensorik dem höheren Zweck der Betriebssicherheit und Schutz von Gesundheit und Leib und Leben vieler Beschäftigten, sodass das Arbeitgeberinteresse an einer Verarbeitung solcher Daten (Daten von Sensoren in der Kleidung von Beschäftigten zur Messung der Luftbelastung) überwiegt. Diese Wertung ergibt sich bereits aus § 26 Abs. 3 S. 1 sowie aus Art. 9 Abs. 2 lit. b DSGVO, wonach der Verarbeiter die Daten verarbeiten darf, wenn diese erforderlich sind, um seine Pflichten aus dem Arbeitsrecht (und somit dem Arbeitsschutz) zu erfüllen.

Zu beachten ist, dass die Daten aus dem obigen Beispiel jedoch anonymisiert werden müssten, da keine Zuordnung der Daten zu einem Beschäftigten erforderlich ist, um eine Warnung auszulösen. Ist das Labor besonders groß und müsste daher nur ein bestimmter Bereich geräumt werden, so könnten die Daten trotz Anonymisierung personenbezogen sein (wenn beispielsweise nur ein Beschäftigter in diesem konkreten Bereich arbeitet). Dies wäre aber unschädlich, da die Verarbeitung der Lokalisationsdaten, die zu einer Zuordenbarkeit führen, erforderlich ist, um den mit der Verarbeitung verfolgten Schutzzweck zu erfüllen und insofern das Interesse des Beschäftigten nicht überwiegt. Letztlich dient die Verarbeitung auch zu seinem eigenen Schutz.

Etwas anderes gilt, wenn etwa Fitness-Armbänder für betriebliche Gesundheitsprogramme eingesetzt werden sollen, um etwa *Health-Scores* generieren, die es ermöglichen, dass sich Arbeitnehmer in den internen Wettbewerb zu anderen Arbeitnehmern zu stellen. Aufgrund der besonderen Sensibilität der Vitaldaten und mangels Legitimationsgrundlage zur Verarbeitung kommt eine Verarbeitung auf rein gesetzlicher Grundlage nicht in Betracht. Ebenfalls scheiden eine zwingende Verarbeitung und Pflicht zur Teilnahme per Betriebsvereinbarung aus (§ 75 Abs. 2 BetrVG). Eine Verarbeitung, die so stark in die Persönlichkeitssphäre des Arbeitneh-

mers eingreift und deren Zweck ebenfalls mehr in der Privatsphäre als im Interesse des Arbeitgebers liegt, kann nicht ohne Einwilligung des Arbeitnehmers stattfinden.

Letztlich bleibt nur daher noch die Einwilligung als Legitimation für die Datenerhebung und -verarbeitung. Zu beachten ist, dass das Angebot tatsächlich freiwillig sein muss und nicht an ein Bonusprogramm o.ä. gekoppelt sein sollte, da hierdurch ein emotionaler oder gar wirtschaftlicher Druck erzeugt werden könnte. Ein solcher könnte auch betriebsintern entstehen. Die Veröffentlichung der Daten an Kollegen o.ä. kann mangels Erforderlichkeit nur auf Grundlage einer Einwilligung erfolgen. Werden Preise für die Teilnahme ausgeschrieben und muss ein Arbeitgeber dafür Daten verarbeiten, so empfiehlt es sich, diese nur auf Abteilungsebene und nicht für individuelle Arbeitnehmer auszuschreiben, da ein Zugriff des Arbeitgebers auf diese sensiblen Daten auf das Mindestmaß beschränkt sein muss; in Betracht kommt eine anonyme, aggregierte Datenbasis für den Zugriff des Arbeitgebers.[1059]

(4) Abwägungsmaßstab

Der generelle Abwägungsmaßstab zur Zulässigkeit der Erhebung und Nutzung von Daten, die geeignet sind, einen Überwachungsdruck zu erzeugen, wurde durch die Rechtsprechung des BAG und BVerfG über Jahre konkretisiert. Maßgeblicher Faktor ist die sog. Eingriffsintensität der Maßnahme. Nach ständiger Rechtsprechung sind verschiedene Kriterien bei der Beurteilung der Maßnahme zu berücksichtigen: Anlassbezogenheit[1060] (also hat der Arbeitgeber einen konkreten Grund, die Daten zu erheben; hat der Arbeitnehmer möglicherweise die Verarbeitung sogar selbst veran-

1059 So wohl *Kopp/Sokoll*, NZA 2015, 1352 (1357).

1060 BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (1190) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54; Beschl. v. 29.06.2004 – 1 ABR 21/03, NZA 2004, 1278 = BAGE 111, 173 = AP BetrVG § 87 1972 Überwachung Nr. 41 (m. Anm. *Ehmann*).

lasst), Dauer der Überwachung[1061], Inhalt/Persönlichkeitsrelevanz[1062] bzw. Kernbereichsbezug[1063], Folgen[1064] und Heimlichkeit[1065].

(a) Belastungsstatistik-Entscheidung des BAG v. 25.04.2017

Eine aktuelle und besonders aufschlussreiche Entscheidung zum Thema Überwachung für Analytics stellt der Beschluss des BAG aus dem Jahr

1061 BAG, Beschl. v. 29.06.2004 – 1 ABR 21/03, NZA 2004, 1278 = BAGE 111, 173 = AP BetrVG § 87 1972 Überwachung Nr. 41 (m. Anm. Ehmann).

1062 BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54; BVerfG, Urt. v. 13.06.2007 – 1 BvR 1550/03, 2357/04, 603/05, BVerfGE 118, 168 (196 f.) – Kontostammdaten; Beschl. v. 04.04.2006 – 1 BvR 518/02, BVerfGE 115, 320 (348) = NJW 2006, 1939 – Rasterfahndung II; Urt. v. 14.07.1999 – 1 BvR 2226/94, 2420/95, 2437/95, BVerfGE 100, 313 (376) – Telekommunikationsüberwachung I; Urt. v. 03.03.2004 – 1 BvR 2378/98, 1084/99, BVerfGE 109, 279 (353) – Großer Lauschangriff.

1063 BVerfG, Urt. v. 27.02.2008 – 1 BvR 370, 595/07, BVerfGE 120, 274 (335 f.) – Online-Durchsuchungen; Urt. v. 03.03.2004 – 1 BvR 2378/98, 1084/99, BVerfGE 109, 279 (313) – Großer Lauschangriff; Beschl. v. 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367 (373 f.) – Tagebuch; BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (1189) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54.

1064 BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (1190) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54; BVerfG, Urt. v. 11.03.2008 – 1 BvR 2074/05, 1 BvR 1254/07, BVerfGE 120, 378 (403) = NJW 2008, 1505 – Automatische Kennzeichenerfassung; Urt. v. 13.06.2007 – 1 BvR 1550/03, 2357/04, 603/05, BVerfGE 118, 168 (197) – Kontostammdaten; Beschl. v. 04.04.2006 – 1 BvR 518/02, BVerfGE 115, 320 (351) = NJW 2006, 1939 – Rasterfahndung II; Urt. v. 03.03.2004 – 1 BvR 2378/98, 1084/99, BVerfGE 109, 279 (353) – Großer Lauschangriff; Urt. v. 14.07.1999 – 1 BvR 2226/94, 2420/95, 2437/95, BVerfGE 100, 313 (376) – Telekommunikationsüberwachung I.

1065 Grundlegend BVerfG, Urt. v. 03.03.2004 – 1 BvR 2378/98, 1084/99, BVerfGE 109, 279 – Großer Lauschangriff; ferner Beschl. v. 04.04.2006 – 1 BvR 518/02, BVerfGE 115, 320 (353) = NJW 2006, 1939 – Rasterfahndung II; Urt. v. 13.06.2007 – 1 BvR 1550/03, 2357/04, 603/05, BVerfGE 118, 168 (197) – Kontostammdaten; Urt. v. 11.03.2008 – 1 BvR 2074/05, 1 BvR 1254/07, BVerfGE 120, 378 (402 f.) = NJW 2008, 1505 – Automatische Kennzeichenerfassung; Urt. v. 27.02.2008 – 1 BvR 370, 595/07, BVerfGE 120, 274 (325) – Online-Durchsuchungen; spezifisch zum Arbeitnehmerdatenschutz BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (1189) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54.

2017 zu einer *Belastungsstatistik*[1066] dar, der im Folgenden näher betrachtet werden soll:

Im Rechtsstreit stand die Wirksamkeit eines Einigungsstellenspruchs im Fokus. Die Arbeitgeberin, ein Versicherungsunternehmen mit bundesweit 38 Schadenaußenstellen, hat mit dem Gesamtbetriebsrat nach einem Einigungsstellenverfahren per Spruch eine „Gesamtbetriebsvereinbarung zur Belastungsstatistik von Schadenaußenstellen" geschlossen. Die Zielsetzung dieser Vereinbarung war, Ungleichgewichte in der Belastungssituation der Außenstellen, der Gruppen und der Mitarbeiter zu erkennen und analysieren, um steuernd eingreifen zu können, sodass die Gruppenleiter eine gleichmäßigere Verteilung der Arbeitslast sowie eine sach- und mitarbeitergerechte Arbeitssteuerung vornehmen können. Ebenso sollte den einzelnen Sachbearbeitern ermöglicht werden, die eigene Arbeitssituation und das eigene Arbeitsverhalten zu erkennen und bewerten, um es im Bedarfsfall verändern zu können, sodass die Rahmenbedingungen der Arbeit verbessert werden. Hierfür sollte eine Reihe von spezifischen Kennzahlen ermittelt werden, bei denen jeweils Schwellenwerte hinterlegt sind. Auf diese Daten haben lediglich die Mitarbeiter in Bezug auf ihre eigenen Daten Zugriff sowie die Gruppenleiter im Rahmen ihrer Zuständigkeit für ihre Mitarbeiter. Erfasst wurden hierbei ausschließlich die Arbeitsmengen, unerledigten Rückstände der einzelnen Sachbearbeiter sowie die Merkmale der Leistungserbringung und Belastung nach einem in der Betriebsvereinbarung vorgegebenem Schema. Diese Werte wurden dann ins Verhältnis zu dem entsprechenden Durchschnittswert aller Sachbearbeiter der Gruppe (differenziert nach Einsatzkriterien) gesetzt. Wenn gewisse Schwellenwerte überschritten wurden, erfolgte der Ausweis der betreffenden Sachbearbeiterdaten.

Für die wöchentlichen Berichte wurden die Daten soweit möglich anonymisiert und grundsätzlich auf Gruppenebene aggregiert. Einzelne Sachbearbeiterberichte waren nur dann zugreifbar, wenn ein Mitarbeiter bei mindestens einer Haupt-Kennzahl erheblich vom Gruppendurchschnitt abwich. In diesem Fall waren dem Gruppenleiter jedoch auch nur die Kennzahlen mit erheblicher Abweichung zugänglich.

Für alle Daten gab es bestimmte Zugriffsfristen, in welchen die Vorgesetzten darauf zugreifen konnten; danach war der Zugriff technisch gesperrt.

Hiergegen hat der Gesamtbetriebsrat Klage erhoben und die Unwirksamkeit des Einigungsstellenspruchs geltend gemacht: Die Statistik führe

1066 BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205.

zu einer umfassenden Leistungs- und Verhaltensüberwachung mit einer unverhältnismäßigen Kontrolldichte, die das nach § 75 Abs. 2 BetrVG zu beachtende Persönlichkeitsrecht der Arbeitnehmer verletze.

Das BAG hat der Klage stattgegeben und den Einigungsstellenspruch für unwirksam erklärt. Zunächst führte es zum allgemeinen Persönlichkeitsrecht gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG aus und stellte fest, dass Eingriffe am Grundsatz der Verhältnismäßigkeit zu messen seien, welcher die Verpflichtung nach § 75 Abs. 2 BetrVG konkretisiere (Rn. 19). Weiterhin folge aus dem Normzweck des § 87 Abs. 1 Nr. 6 BetrVG, dass Arbeitnehmer vor Beeinträchtigungen des Persönlichkeitsrechts durch den Einsatz technischer Überwachungseinrichtungen bewahrt werden müssen, sofern diese nicht durch schützenswerte Belange des Arbeitgebers gerechtfertigt oder unverhältnismäßig sind.

Der Grundsatz der Verhältnismäßigkeit erfordere eine Regelung, die geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen ist, um den erstrebten legitimen Zweck zu erreichen (Rn. 21). Es dürfen keine anderen, gleich wirksamen Mittel zur Verfügung stehen, die das Persönlichkeitsrecht des Arbeitnehmers weniger einschränken. Eine Verhältnismäßigkeit sei gegeben, wenn die „Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht“[1067] (Rn. 21).

Es handle sich zwar um ein legitimes Anliegen des Arbeitgebers, eine unterschiedliche Belastungssituation der Arbeitnehmer und deren Ursachen in Erfahrung zu bringen, um steuernd eingreifen zu können und die Effizienz zu steigern (Rn. 25). Allerdings sei bereits zweifelhaft, ob das Mittel der „Belastungsstatistik“ auf dieses Ziel gerichtet sei. Durch die Belastungsstatistik würden ausschließlich Daten zur Erledigung von Arbeitsaufgaben erfasst, ohne Berücksichtigung der Komplexität der Aufgabe und der Qualität des Arbeitsergebnisses. Aus diesem Grund spreche bereits viel dafür, dass das eingesetzte Mittel untauglich sei, den erstrebten Zweck zu fördern.

Zwar könne man zugunsten der Arbeitgeberin davon ausgehen, dass die erhobenen Statistiken für den Zweck erforderlich seien. Dem stehe jedenfalls nicht entgegen, dass der jeweilige Gruppenleiter den „digitalen Arbeitskorb“ ebenfalls überwachen und steuern könne. Denn dies sei nur

1067 Ebenso BAG, Beschl. v. 15.04.2014 – 1 ABR 2/13 (B), NZA 2014, 551 (555) = BAGE 148, 26 = AP BetrVG 1972 § 29 Nr. 9 Rn. 41 unter Verweis auf BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, BVerfGE 115, 320 (1941 f.) = NJW 2006, 1939 – Rasterfahndung II Rn. 88.

„tagesaktuell" möglich, die Statistik hingegen solle eine Einschätzung über einen längeren Zeitraum ermöglichen.

Im Ergebnis seien die Eingriffe durch die Belastungsstatistik allerdings unverhältnismäßig im engeren Sinne (unangemessen), da sie einen schwerwiegenden Eingriff in das Persönlichkeitsrecht des betroffenen Arbeitnehmers darstellten, der durch schützenswerte Interessen des Arbeitgebers nicht zu rechtfertigen sei:

Durch die Gesamtbetriebsvereinbarung werde eine lückenlose, dauerhafte und sehr detaillierte Erfassung des wesentlichen Arbeitsspektrums der Sachbearbeiter geregelt (Rn. 29), sodass der einzelne Arbeitnehmer während der gesamten Dauer seiner Arbeitszeit in der Schadenaußenstelle davon ausgehen müsse, dass sein „wesentliches Arbeitsspektrum auf elektronischem Wege anhand einer Vielzahl von quantitativen Kriterien (Haupt- und Analysekennzahlen) im Rahmen der einzelnen ‚Arbeitsauslöser' durchgehend detailliert erfasst und einer Auswertung auf den Ebenen einer 1-Wochen-, 4-Wochen- und 26-Wochen-Sicht zugeführt würden. Sämtliche Auswertungen würden wochenweise fortgeschrieben und stünden jeweils am Ende der Arbeitswoche zur Verfügung. Dies führe zu einem ständigen Überwachungs- und daran anknüpfenden Anpassungs- und Leistungsdruck in allen wesentlichen Arbeitsbereichen." (Rn. 30). Arbeitnehmer würden dazu gedrängt, möglichst in allen maßgebenden Arbeitsbereichen in Bezug auf die Kennzahlen unauffällig zu arbeiten, um nicht aufgrund „erheblicher Abweichungen" in Personalgespräche zitiert zu werden oder personellen Maßnahmen ausgesetzt zu sein (Rn. 32).[1068]

Erschwerend komme hinzu, dass der einzelne Sachbearbeiter nur bei erheblichen Abweichungen seine Werte sehen könne und dann nur retrospektiv am Ende der jeweiligen Woche; die „erhebliche Auswertung" sei ferner nicht von einem fest bestimmten Wert abhängig, sondern von der jeweiligen Zusammensetzung der Gruppe und deren Ergebnisse, auf die der einzelne Arbeitnehmer keinen Einfluss habe (Rn. 33). Dazu komme, dass nur die Abweichungen ausgewiesen würden, nicht aber alle Werte, sodass der Sachbearbeiter in einzelnen Kennzahlen auch überdurchschnitt-

1068 Das BVerfG spricht hierbei von Freiheitsbeschränkung durch „Einschüchterungseffekten" aufgrund des Gefühls des „Überwachtwerdens", vgl. BVerfG, Urt. v. 11.03.2008 – 1 BvR 2074/05, 1 BvR 1254/07, BVerfGE 120, 378 (402) = NJW 2008, 1505 – Automatische Kennzeichenerfassung Rn. 78 m.w.N.; unter Verweis auf das Urteil des BVerfG ebenso BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (Rn. 1191) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54 Rn. 29.

lich sein könnte, was dann dem Gruppenleiter und ihm selbst nicht zugänglich wäre (Rn. 34).

(b) Bewertung

Die Entscheidung verdeutlicht, dass Überwachungsmaßnahmen nicht per se unverhältnismäßig sind, sondern es auf die konkrete Ausgestaltung ankommt. Arbeitgeber haben ein anerkanntes Interesse daran, Leistungs- und Verhaltenskontrollen im Rahmen der Durchführung vorzunehmen.[1069] Dabei ist „weniger nicht immer mehr": Ein entscheidender Punkt in der Verhältnismäßigkeit im engeren Sinn war, dass die Arbeitnehmer unter der Woche keinen Zugriff auf die aktuellen Daten hatten, sondern nur bei Überschreiten bestimmter Grenzwerte die Überschreitungen angezeigt bekommen haben (ebenso die Gruppenleiter). Die Anzeige anderer Daten hätte mitunter die Überdurchschnittlichkeit in anderen Bereichen aufzeigen und somit die Transparenz erhöhen können, mit dem Ergebnis eines geringeren Eingriffs in das Persönlichkeitsrecht. Im Kern der Entscheidung stand allerdings, dass die lückenlose Überwachung der Primärleistungspflicht zu einem Überwachungsdruck führt, die die Arbeitnehmer an der Wahrnehmung ihrer Freiheitsrechte hindern könnte, da aus dem „Überwachtwerden" ein Anpassungsdruck folgen könnte. Ausschlaggebende Kriterien nach eingangs dargestelltem Maßstab waren daher die Dauer der Überwachung sowie die (nicht hinreichende) Anlassbezogenheit.

In einem früheren Fall hat das BAG 1996 für sog. „Bedienerplatzreports" von Call-Center-Mitarbeitern hingegen die datenschutzrechtliche Zulässigkeit solcher Auswertungen angenommen.[1070] In diesen Reports konnten jeweils die Länge der Anrufe, die Verteilung der Anrufe auf die einzelnen Bedienplätze und nicht angenommene Anrufe dargestellt werden. Hintergrund der Entscheidung dürfte sein, dass sich die Erfassung lediglich auf den Arbeitsbereich und auf schlichte Zahlen und Fakten beschränkt, sodass nur eine fernliegende Gefahr eines allumfassenden Persönlichkeitsprofils bestand. Die Persönlichkeitsrelevanz war im Vergleich zur Belastungsstatistik daher geringer. Hinzu kommt das Kriterium der

1069 So auch *Schürmann*, Auswertung von Mitarbeiterdaten - (Any)/(No)thing possible?, in: Taeger, Smart world - smart law?, S. 503 m.w.N.

1070 BAG, Beschl. v. 30.08.1995 – 1 ABR 4/95, NZA 1996, 218.

Anlassbezogenheit: In Call-Centern ist eine Steuerung der Arbeitsplätze und Telefonate unabdingbar.[1071]

Wendet man die Schlüsse aus diesen Entscheidungen in Bezug auf die eingangs genannten Kriterien auf *Advanced People Analytics*-Maßnahmen an, so folgt daraus, dass die Analytics über die Primärleistungspflicht mit dem Zweck der Verbesserung der Arbeitssituation/Effizienzsteigerung, aber auch Leistungsüberwachung im Ausgangspunkt als legitim beachtet werden können, da sie einen bestimmten und berechtigten Anlass haben. Arbeitgeber verfolgen bei ersteren nicht nur selbstgelagerte Interessen, sondern auch solche seiner Arbeitnehmer. Für diese kann sich eine solche Überwachung zu ihren Gunsten auswirken, falls hierdurch eine Verringerung der Belastung stattfindet bzw. Überbelastungen erkannt und vermieden werden.

Voraussetzung ist aber in jedem Fall, dass die erhobenen Daten auch tatsächlich geeignet sind, das erstrebte Ziel zu fördern. Wird hierzu eine unzureichende oder falsche Datenbasis verwendet, so sind die Analytics bereits nicht tauglich. Zwar haben sich die Arbeitgeber am Grundsatz der Datenminimierung zu orientieren; dieser darf aber nicht derart ad absurdum geführt werden, dass die Daten ihre Aussagekraft verlieren und somit erst hierdurch ein unverhältnismäßiger Eingriff in das Persönlichkeitsrecht erfolgt. Bei IT-Nutzungsdaten muss daher genau überprüft werden, ob diese Daten im Hinblick auf das erstrebte Ziel aussagekräftig sind.

Beispiel: Die Erfassung der täglichen Bildschirmarbeitszeit (am PC angemeldet und nicht ausgeloggt) wäre kein taugliches Mittel zur Erfassung der Arbeitsbelastung oder Arbeitszeit, da es Zeiten geben kann, in welchen ein Arbeitnehmer zwar arbeitet, aber gerade telefoniert oder nicht am PC sitzt. Umgekehrt kann es Zeiten geben, in welchen der Arbeitnehmer zwar am PC angemeldet ist, jedoch nicht aktiv einer Arbeit nachgeht. Hingegen kann bei einem Call-Center-Mitarbeiter die Überwachung der Bildschirmarbeitszeit, zusammen mit der Auswertung von Anruflisten und dem Terminkalender des einzelnen Arbeitnehmers durchaus ein mögliches Mittel sein, etwaigen Arbeitszeitenbetrug aufzudecken oder zumindest Anhaltspunkte für die Leistungsfähigkeit des Arbeitnehmers zu geben (die Verhältnismäßigkeit nun außer Acht gelassen).

Abseits der Primärleistungspflichten, im Bereich der arbeitsvertraglichen Fürsorgepflicht nach § 241 Abs. 2 BGB, können Analytics anhand der gezeigten Maßstäbe jedoch in weiterem Maße durchgeführt werden,

1071 *Schürmann*, Auswertung von Mitarbeiterdaten - (Any)/(No)thing possible?, in: Taeger, Smart world - smart law?, S. 506.

sofern der Persönlichkeitsbezug möglichst geringgehalten wird. Hier ist der durch die Überwachung von bestimmten Daten erzeugte „Anpassungsdruck" deutlich geringer; personelle Maßnahmen sind in aller Regel nicht zu befürchten. Solche Auswertungen sind vor allem im Bereich der Personalentwicklung und der Gesundheitsvorsorge bzw. des Arbeitsschutzes auf Individualebene denkbar.

Beispiel: Anhand der ausgewerteten Bildschirmarbeitszeit könnte analysiert werden, wieviel Zeit der einzelne Arbeitnehmer vor dem Bildschirm verbringt. Nach § 5 der Bildschirmarbeitsverordnung (BildSchArbV) hat der Arbeitgeber die Tätigkeit der Beschäftigten so zu organisieren, dass die tägliche Arbeit an Bildschirmgeräten regelmäßig durch andere Tätigkeiten oder durch Pausen unterbrochen wird, die jeweils die Belastung durch die Arbeit am Bildschirmgerät verringern. Durch eine Analyse der Screen-Time (nicht des Bildschirminhalts!) kann der Arbeitgeber seiner arbeitsvertraglichen Fürsorgepflicht nachkommen und – sollte er feststellen, dass entsprechende Unterbrechungen nicht stattfinden – dem Arbeitnehmer entsprechend andere Zwischen-Tätigkeiten zugewiesen / angeboten werden oder beispielsweise durch eine eigene Software[1072] Pausen vorgeschlagen werden. Ebenso könnte die Screen-Time als Indikator genutzt werden, ob ein Arbeitnehmer viel sitzt (z.B., wenn keine höhenverstellbaren Schreibtische vorhanden sind) und diesem entsprechende Bewegungsangebote angeboten werden. Alternativ könnte der Arbeitgeber auch durch diese Kennzahl ermitteln, für welche Arbeitnehmer höhenverstellbare Schreibtische sinnvoll sind, um Haltungsschäden vorzubeugen und Bewegung anzuregen.

Zu beachten ist, dass die für die Ausübung der Fürsorgepflichten gesammelten Daten auch ausschließlich für diese Zwecke genutzt und nicht für Leistungskontrollen missbraucht werden dürfen. Hier müssen technisch-organisatorische Maßnahmen vorgesehen werden. Diese sollten dem Arbeitnehmer möglichst transparent und verständlich erklärt werden, um eventuelle „Überwachungsängste" zu vermeiden.[1073]

1072 Hierfür gibt es bereits unzählige, kostenlose Tools. Als Beispiele können EyeLoveU, Workrave (das darüber hinaus auch vor schlechter Haltung warnen soll), Time Out oder Eye Saver genannt werden.

1073 Eine Gefahr des Überwachungsdrucks bei der Nutzung von Sensordaten sehen auch *Brecht/Steinbrück/Wagner*, PinG 2018, 10 (11).

b) Die Nutzung von IT-Daten für Advanced People Analytics

Für die Nutzung von IT-Daten für *Advanced People Analytics* gilt derselbe Maßstab wie für die Erhebung. Dennoch muss eine Unterscheidung getroffen werden zwischen Daten, die der Arbeitgeber speziell für diese Zwecke aktiv erhebt und solchen, die aus anderen Gründen erhoben wurden, beispielsweise zum Zwecke der Gewährleistung der Funktionsfähigkeit und Integrität von IT-Systemen. Bei ersteren wurde die erforderliche Abwägung bereits vor der Erhebung der Daten getroffen und es ändert sich daher durch den weiteren Verarbeitungsvorgang für diesen Zweck grundsätzlich nichts an der Abwägung.

Bei letzteren hingegen wurden die Daten auf Basis einer anderen Legitimationsgrundlage und zu einem anderen Zweck erhoben, sodass einerseits die weiteren Voraussetzungen der Zweckänderung (sog. Kompatibilitätstest) nach Art. 6 Abs. 4 DSGVO[1074] und andererseits das Vorliegen der Voraussetzungen der neuen Legitimationsgrundlage (insbesondere die Erforderlichkeit für die Durchführung des Beschäftigungsverhältnisses nach § 26 Abs. 1 S. 1 BDSG bzw. zur Wahrnehmung berechtigter Interessen des Arbeitgebers nach Art. 6 Abs. 1 lit. f DSGVO)[1075] geprüft werden müssen.

aa) Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO

Sofern APA auf aggregierter und somit anonymer Basis stattfinden, d.h. die Ergebnisse nicht personenbezogen und ferner nicht auf Einzelpersonen angewandt werden, greift die unwiderlegliche Vermutung der Zweckvereinbarkeit gem. Art. 5 Abs. 1 lit. b i.V.m. Erwägungsgrund 152 und 162 DSGVO („Statistik-Ausnahme“).[1076] Dies ist insbesondere dann der Fall, wenn der Arbeitgeber Unternehmens-/Betriebs- oder Abteilungskennzahlen durch *Advanced People Analytics* berechnet und diese nicht für weitergehende Einzelmaßnahmen einsetzt. Hier stehen also die mittel- und langfristige Planung statt kurzfristiger Maßnahmen im Mittelpunkt.

Für alle anderen Auswertungen, also solche, die auf individualisierter Basis vorgenommen werden oder deren Ergebnisse auf Einzelpersonen angewandt werden, ist ein Kompatibilitätstest vorzunehmen. Aufgrund

1074 Ausführlich hierzu **E. § 1 I. 2.**
1075 Zum Streitstand bezüglich der Erforderlichkeit einer Legitimationsgrundlage bei einer zweckkompatiblen Weiterverarbeitung, siehe **E. § 1 I. 2. a**).
1076 Siehe bereits **E. § 1 I. 2. c**).

der strikteren Erlaubnistatbestände einer Zweckänderung im Vergleich zu Art. 6 Abs. 1 DSGVO bzw. § 26 Abs. 1 BDSG unterliegt die Weiterverarbeitung besonderen Hürden.[1077]

So muss geprüft werden, ob die Weiterverarbeitung mit den ursprünglichen Erhebungszwecken vereinbar ist, wobei unter anderem die Verbindung zwischen den Verarbeitungszwecken, der Zusammenhang zwischen Erhebung und Weiterverarbeitung, die Art der personenbezogenen Daten, die möglichen Folgen sowie das Vorhandensein vorhandener Garantien im Rahmen des Kompatibilitätstests untersucht werden müssen.[1078]

(1) Kriterien der Zweckvereinbarkeit

Bei der Verwendung von Log-Dateien ist zu beachten, dass der Zusammenhang zwischen Erhebung und Weiterverarbeitung grundsätzlich ein komplett verschiedener ist, die Zwecke also mithin nicht sehr eng verbunden sind (z.B. wie im Falle, wenn bereits erhobene Arbeitnehmerdaten für die Durchführung des Beschäftigungsverhältnisses für Analytics weiterverwendet werden sollen). Der Erhebungszweck von IT-Systemdaten dient – wie bereits erläutert – der Sicherstellung der Funktionsfähigkeit und Integrität von Informationssystemen und nicht primär dem Arbeitsverhältnis. Wenn man berücksichtigt, dass der Betroffene bei den IT-Systemdaten, sofern er zuvor nicht darauf aufmerksam gemacht wurde, nicht mit einer Verarbeitung für APA-Zwecke rechnet, so ist dies bereits ein Anhaltspunkt gegen eine Zweckvereinbarkeit.[1079] Hinzu kommt, dass nach Art. 6 Abs. 4 lit. b DSGVO auch die gegenseitige Abhängigkeit beachtet werden muss, da in dieser Konstellation möglicherweise kein „Gleichgewicht der Entscheidungsfreiheit" besteht:[1080] Der Arbeitnehmer ist zur Erfüllung seiner Leistungspflicht aus dem Arbeitsvertrag gezwungen, die IT-Systeme des Arbeitgebers zu nutzen und ist daher davon abhängig. Umgekehrt ist auch der Arbeitgeber verpflichtet, gewisse Systemdateien zu sammeln; damit muss ein Arbeitnehmer rechnen. Nicht hingegen muss er, sofern er bei Erhebung nicht darauf aufmerksam gemacht wurde, damit rechnen,

1077 EuArbRK/*Franzen*, Art. 6 DSGVO Rn. 13.

1078 Zu den Kriterien im Einzelnen, siehe die Ausführungen unter **E. § 1 I. 2. d**).

1079 Vgl. *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 187; siehe hierzu bereits **E. § 1 I. 2. d**) **aa**) m.w.N.

1080 *Monreal*, ZD 2016, 507 (510).

dass diese Daten später für die Beurteilung seiner persönlichen Leistung genutzt werden, also für Zwecke außerhalb des technischen Kontextes.

Gegen eine Zweckkompatibilität sprechen ferner die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen (Art. 6 Abs. 4 lit. d DSGVO). Zwar sind in diesem Zusammenhang nicht nur negative, sondern auch positive Folgen zu beachten. Eine Rolle spielen hierbei aber nicht nur rechtliche, sondern auch emotionale Folgen, wie beispielsweise die Angst, die Kontrolle über die eigenen Daten zu verlieren oder überwacht zu werden.[1081] Gerade, wenn notwendige IT-Systemdaten später für People Analytics und einer damit verbundenen Leistungsbeurteilung eingesetzt werden sollen, könnte dies die Angst der Arbeitnehmer vor unkontrollierbarer Überwachung schüren. Dies wären bereits negative Folgen, die berücksichtigt werden müssen. Dazu kommt, dass auch personelle Einzelmaßnahmen abgeleitet werden könnten, wenn in den Auswertungen festgestellt wird, dass gegen arbeitsvertragliche Pflichten oder das Gesetz verstoßen wird.

(2) Vertragliches Verarbeitungsverbot als geeignete Garantie zur Herstellung von Zweckkompatibilität?

Um eine Verarbeitung dennoch zu ermöglichen, ist daher die Frage aufzuwerfen, ob eine solche Zweckkompatibilität auf Basis von Art. 6 Abs. 4 lit. e DSGVO auch durch geeignete *juristische* Garantien wie beispielsweise einem vertraglich oder in einer Betriebsvereinbarung niedergelegten Verarbeitungsverbot hergestellt werden könnte. Wie bereits herausgearbeitet[1082], siedelt die DSGVO die Verarbeitungs-Garantien im Rahmen der Zweckkompatibilitätsprüfung vor allem auf der technischen Seite, bei den technisch-organisatorischen Maßnahmen an. Diese Garantien (außer eine Anonymisierung, die im Rahmen von People Analytics bereits Zweckkompatibilität herstellen würde[1083]) können die aufgeworfenen Probleme allerdings nicht beseitigen.

Fraglich ist daher, ob auch juristische Garantien wie beispielsweise eine Betriebsvereinbarung, die ein Beweisverwertungsverbot statuiert oder eine Gesamtzusage des Arbeitgebers, aus den hieraus gewonnenen Erkenntnis-

1081 *Article 29 Data Protection Working Party,* WP 203, S. 25 f.; vgl. auch im Detail **E. § 1 I. 2. d) dd)**.
1082 Vgl. oben **E. § 1 I. 2. d) ee)**.
1083 Siehe **E. § 1 I. 2. c)**.

sen keine negativen Folgen für den Arbeitnehmer herzuleiten, die Zweckkomptabilität herstellen können. Grundsätzlich werden in der Literatur rechtliche Vorkehrungen als mögliche Garantien erachtet.[1084] Allerdings beschränken sich die Vorschläge vor allem auf Geheimhaltungs- und Löschpflichten.[1085]

In Art. 46 DSGVO, der Regelung von Datenübermittlungen vorbehaltlich geeigneter Garantien, kommt ebenfalls derselbe Terminus vor, wobei dort in Abs. 2 lit. a auch rechtliche Garantien explizit genannt werden, z.B. ein rechtlich bindendes und durchsetzbares Dokument zwischen öffentlichen Stellen. Aus Erwägungsgrund 108 geht hervor, dass die Garantien im Rahmen von Art. 46 DSGVO dazu dienen sollen, dass die Datenschutzvorschriften und Rechte der betroffenen Personen auf eine der Verarbeitung innerhalb der Union angemessene Art und Weise beachtet werden sollen.

Aus der Systematik der DSGVO lässt sich nicht viel für die Beantwortung dieser Frage herleiten. Wenn man jedoch berücksichtigt, dass die Garantien im Zusammenhang mit dem Kriterium der möglichen Folgen für den Betroffenen zu sehen ist und der Datenschutzansatz risikobasiert ist,[1086] so müssen in dieser Folge auch Verarbeitungsverbote grundsätzlich eine taugliche Garantie darstellen. Dieser Ansatz wird durch den Wortlaut des Art. 35 Abs. 1 DSGVO bekräftigt, der von einem „hohen Risiko für die Rechte und Freiheiten natürlicher Personen spricht". Es kommt dabei nicht nur auf das Risiko eines Datenverlustes oder einer unbefugten Nutzung von Daten an, sondern insbesondere darauf, ob natürliche Personen (Betroffene) Rechts- und Freiheitseinbußen befürchten müssen, wenn der Verarbeiter die vorhandenen Daten über die Kompatibilitätsklausel des Art. 6 Abs. 4 DSGVO weiterverarbeitet. Als Risiko kann man allgemein „das Bestehen der Möglichkeit eines Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder das zu einem

1084 *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 60; *Sander/Schumacher/Kühne*, ZD 2017, 105 (109); dagegen wohl *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 209.

1085 Sydow/*Reimer*, Art. 6 DSGVO Rn. 60; *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 6 Abs. 4 DSGVO Rn. 60; wohl auch *Sander/Schumacher/Kühne*, ZD 2017, 105 (109).

1086 Vgl. hierzu bereits **E. § 1 I. 2. d) ee)**.

weiteren Schaden für eine oder mehrere natürliche Personen führen kann" bezeichnen.[1087]

Dies entspricht auch dem in Art. 1 Abs. 2 DSGVO ausdrücklich festgelegten Ziel: Der Schwerpunkt der DSGVO liegt zwar auf dem Schutz der personenbezogenen Daten, ferner aber auch auf dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen.

Aus diesem Grund kann ein Verarbeitungsverbot im Rahmen einer Zusicherung durch den Arbeitgeber durchaus eine geeignete Garantie im Rahmen von Art. 6 Abs. 4 DSGVO darstellen.

(3) Keine Zweckkompatibilität von IT-Systemdaten mit People Analytics

Zwar können Verarbeitungsverbote grundsätzlich eine geeignete Garantie darstellen, für den Fall der People Analytics stellt sich allerdings die Frage, ob eine Zusage des Arbeitgebers, keine nachteiligen Folgen aus den für Analytics verwendeten IT-Systemdaten für Arbeitnehmer zu generieren, den bereits genannten Gefahren hinreichend begegnen kann, um zu einer Zweckkompatibilität zwischen Erhebungszweck und Weiterverarbeitungszweck zu kommen.

Dies ist zu verneinen: Einerseits wäre es dann Arbeitgebern möglich, auch rückwirkend Daten zu Analyticszwecken heranzuziehen, bei denen die Arbeitnehmer noch keine Kenntnis davon hatten, dass diese Daten für weitere Zwecke genutzt werden könnten. Andererseits ist dem Arbeitgeber auch bei späterer Einführung von (Advanced) People Analytics zuzumuten, die Daten erst ab diesem Zeitpunkt zu erheben (z.B. indem eine bestimmte Datenaufzeichnung erst dann aktiviert wird) und in diesem Rahmen der Erhebung den weitergehenden Verarbeitungszweck für IT-Systemdaten festzulegen, sodass es einer zweckkompatiblen Weiterverarbeitung nicht bedarf. Eine vertragliche Zusicherung kann die hieraus resultierenden Überwachungsängste der Betroffenen nicht verhindern.

Hingegen wäre es auch möglich, die retrospektiven Daten auf anonymer Basis auszuwerten (in diesem Fall wird die Zweckkompatibilität unwiderleglich vermutet), um festzustellen, ob die Auswertungen hilfreiche Erkenntnisse für das Personalwesen erzeugen können. Bei einer solchen Auswertung haben Arbeitnehmer keine Folgen zu befürchten, da Rück-

1087 *DSK*, Kurzpapier Nr. 18 - Risiko für die Rechte und Freiheiten natürlicher Personen, <www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf> , S. 1 unter Rückgriff auf die Erwägungsgründe 75 und 94 S. 2.

schlüsse auf die einzelne Person nicht möglich sind. Für Datenpunkte, bei denen relevante Korrelationen feststellbar sind, können Verarbeiter, respektive Arbeitgeber, im Anschluss an die Feststellung für die weitere zukünftige Erhebung festlegen, dass diese auch für die Zwecke von People Analytics in personenbezogener Form genutzt werden (die weiteren Rechtmäßigkeitsvoraussetzungen aus § 26 Abs. 1 BDSG müssen selbstverständlich vorliegen). Somit sind zwar keine personenbezogenen rückblickenden Analytics (bezogen auf IT-Daten vor dem Zeitpunkt der Zweckerweiterung des jeweiligen Datenpunkts) möglich, hingegen aber für die Zukunft. Dies erfordert aber auch der Schutz der Rechte und Freiheiten des Arbeitnehmers, der zumindest im Rahmen der Erhebung bereits damit rechnen können muss (Stichwort: „*Missing Link*"), dass diese Daten auch für das Personalwesen von Bedeutung sein können bzw. im Rahmen des Human Ressource Managements verarbeitet werden.

Bei der Einführung von APA sollten Arbeitgeber daher möglichst mit Hilfe anonymisierter Daten mögliche relevante Zusammenhänge, die sich aus einer Verarbeitung von IT-Systemdaten ergeben können, erkennen, bevor eine Zweckerweiterung bei der Datenerhebung vorgenommen wird. Erst nach erfolgter Zweckerweiterung vor der zukünftigen Erhebung der jeweiligen Datenpunkte stellen solche Daten eine geeignete Grundlage für Advanced People Analytics dar. Somit ist die Geeignetheit der Datenverarbeitung sichergestellt und kann durch den Arbeitgeber im Rahmen seiner Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO auch nachgewiesen werden.

bb) Zulässigkeit der Nutzung von IT-Daten für Advanced People Analytics

Ist eine Zweckerweiterung im Rahmen der Datenerhebung vorgenommen worden (und der Arbeitnehmer nach Art. 13 f. DSGVO darüber informiert worden), muss die Nutzung der Daten am Maßstab des § 26 Abs. 1 BDSG gemessen werden, wenn die Daten für APA genutzt werden sollen. Hierbei gilt derselbe Maßstab wie bei der Erhebung von IT-Systemdaten (siehe **E. § 1 III. 2. a) cc) (4)**).

(1) Legitimation für den Vorgang der Anonymisierung erforderlich

Für die Daten, die für die Nutzung anonymisiert werden, ist nach der Anonymisierung kein Datenschutzrecht mehr anwendbar, sodass die Verarbeiter diese Daten frei verarbeiten können, sofern durch die Verknüpfung unterschiedlicher anonymer Datensätze keine personenbezogenen Daten entstehen.[1088] Der Vorgang der Anonymisierung selbst muss jedoch legitimiert sein, da hierfür (zunächst) personenbezogene Daten als Grundlage für einen Verarbeitungsvorgang dienen. Hier darf analog der Anonymisierung bei Simple People Analytics mangels entgegenstehender Interessen des Arbeitnehmers (keine Rückführbarkeit mehr möglich, somit keine Beeinträchtigung von Freiheiten und Rechte) von einer Zulässigkeit des Verarbeitungsvorgangs ausgegangen werden.[1089] Legitimationsgrundlage dürfte in aller Regel mangels Bezugs der Auswertungen zu einem konkreten Beschäftigungsverhältnis Art. 6 Abs. 1 lit. f DSGVO sein, andernfalls § 26 Abs. 1 S. 1 BDSG.

(2) Besonderheiten bei der Nutzung von TK- und Standortdaten

Nach der hier vertretenen Auffassung stellt auch das Telekommunikationsrecht keine weiteren Grenzen bei der Nutzung von IT-Systemdaten für People Analytics, da der Arbeitgeber in jenem Bereich, wo etwaige nützliche Daten erhoben würden (Arbeitsrechner des Beschäftigten) nicht als Diensteanbieter im Sinne des TKG anzusehen ist.[1090] Da jedoch insbesondere die Datenschutzbehörden der Auffassung sind, dass die §§ 88 ff. TKG bei erlaubter Privatnutzung anwendbar sind, sollten sich Arbeitgeber der Risiken (insbesondere in strafrechtlicher Hinsicht, § 206 StGB) bewusst sein, wenn sie Telekommunikationsdaten für APA auswerten. Von § 88 Abs. 1 TKG sind nicht nur der Inhalt der Telekommunikation, sondern auch die näheren Umstände wie Telekommunikationsteilnehmer (E-Mail-Absender und Empfänger) sowie alle sonstigen Daten erfasst, die nicht schon als Inhalt erfasst werden; es besteht ein umfassender Schutz.[1091] § 88 Abs. 3 TKG regelt genau, für welche Zwecke die Daten genutzt werden dürfen: Grundsätzlich dürfen solche Daten nur für das für die geschäftsmä-

1088 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 256.
1089 Vgl. **E. § 1 III. 1. a) aa)**.
1090 Zum Streitstand siehe bereits **D. § 3 I**.
1091 *Bock*, in: Geppert/Schütz, Beck'scher TKG-Kommentar, § 88 TKG Rn. 14.

ßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß verwendet werden. Dies inkludiert beispielsweise die Fehlerbehebung, elektronische Erfassung von Telefonaten für die Abrechnung oder die Erkennung der missbräuchlichen Nutzung solcher Systeme.[1092]

Ebenfalls von Bedeutung ist dieser Streit für die Nutzung von Standortdaten, wenn das GPS-Modul[1093] des Mobiltelefons dafür genutzt werden soll, diese zu erfassen und auszuwerten. Ist der Arbeitgeber als Diensteanbieter im Sinne des TKG anzusehen, so könnte für die Verarbeitung von Standortdaten § 98 TKG Anwendung finden, mit der Folge, dass eine Einwilligung zum Abruf dieser Daten beim Arbeitnehmer eingeholt werden müsste. Standortdaten sind nach § 3 Nr. 19 TKG solche Daten, die in einem Telekommunikations-Netz erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines TK-Dienstes für die Öffentlichkeit angeben. Unter den Begriff des TK-Netzes (vgl. § 3 Nr. 27 TKG) ist jedoch nicht das Sattelitennetz, über welches GPS funktioniert, zu fassen.[1094] Hintergrund hierfür ist, dass keine Datenübermittlung im Satellitennetz stattfindet, sondern das Mobiltelefon lediglich die Standortdaten von bestimmten Satelliten zu bestimmten Zeiten erfasst und die Positionsbestimmung ausschließlich im Endgerät stattfindet; es werden also keine Nachrichten über das Satellitennetz übermittelt.[1095]

Da jedoch die Ortung bei modernen Mobiltelefonen nicht mehr ausschließlich satellitenbasiert, sondern auch über nahegelegene drahtlose Netzwerke (WLAN)[1096] sowie Mobilfunknetze stattfindet,[1097] ist die obige

---

1092 Beispiele aus *Bock*, in: Geppert/Schütz, Beck'scher TKG-Kommentar, § 88 TKG Rn. 27; für das letzte Beispiel ergibt sich die Legitimation nicht bereits aus § 88 Abs. 3 S. 1, sondern aus S. 2 i.V.m. § 100 Abs. 3 TKG.

1093 Von dem Begriff „GPS" werden für die Zwecke dieser Arbeit nicht nur Ortungen über das GPS-System, sondern über sämtliche satellitenbasierte Systeme erfasst (so also auch Ortungen über GLONASS/GALILEO).

1094 Plath/*Jenny*, § 98 TKG Rn. 10; a.A. *Steidle*, MMR 2009, 167 (168); *Eckhardt*, in: Spindler/Schuster, Recht der elektronischen Medien, § 98 TKG Rn. 9, der seine Auffassung mit der Gegenauffassung belegt und nicht weiter begründet.

1095 Plath/*Jenny*, § 98 TKG Rn. 10; *Maier/Ossoinig*, VuR 2015, 330 (333 f.).

1096 Sogenanntes Wi-Fi Positioning System (WPS); dies funktioniert so, dass in einer Geo-Datenbank die Lokalisationsdaten der einzelnen Zugangspunkte gespeichert werden und das Mobiltelefon die sich in der Nähe befindlichen Access-Points mit der Datenbank abgleicht, wodurch der Standort ziemlich genau ermittelt werden kann, vgl. *Maier/Ossoinig*, VuR 2015, 330 (334) Eine solche Datenbank ist beispielsweise www.wigle.net.

1097 Siehe hierzu https://www.heise.de/ct/hotline/FAQ-Ortung-auf-dem-Smartphone-2450476.html (letzter Abruf am: 07.02.2020).

Diskussion weitgehend obsolet, da in der Regel die Software nicht darauf programmiert ist, ausschließlich das integrierte GPS-Modul zu nutzen. Sobald Mobilfunk-Stationsdaten verwendet werden, ist § 98 TKG anwendbar, mit der Folge, dass diese Daten entweder anonymisiert erfasst werden müssen oder die Einwilligung des Teilnehmers eingeholt werden muss.

Bei der Inanspruchnahme von Dienstleistern für Location Based Services (LBS), wie beispielsweise der Ortung von Diensthandys des Arbeitgebers durch den Mobilfunkanbieter, ist Teilnehmer der Arbeitgeber, der die Dienste in Anspruch nimmt.[1098] Dieser muss dann allerdings seine Arbeitnehmer als Nutzer nach § 98 Abs. 1 S. 7 TKG über die erteilte Einwilligung zur Standorterfassung informieren.[1099] Sofern auf Standortdaten aufgrund einer Einwilligung des Teilnehmers zugegriffen wird, ist bei jedem Standortzugriff eine Textmitteilung (SMS) an das Endgerät zu senden, § 98 Abs. 1 S. 2 TKG.

Werden LBS hingegen durch den Arbeitgeber selbst durchgeführt, findet § 98 TKG keine Anwendung, da nach allgemeiner Meinung der Arbeitgeber bei rein dienstlicher Kommunikation kein Diensteanbieter im Sinne des TKG ist.[1100]

Unabhängig der Anwendbarkeit des Telekommunikationsrechts ist es in jedem Fall erforderlich, die Verarbeitung solcher Daten an § 26 Abs. 1 S. 1 BDSG zu messen. Die Standort-Überwachung von Arbeitnehmern unterliegt aufgrund des gravierenden Eingriffs in die Persönlichkeitsrechte hohen Voraussetzungen, die im Einzelfall anhand der dargestellten Kriterien zur Erforderlichkeit zu prüfen sind. Es sind allerdings keine Fälle denkbar, in denen solche – außerhalb der Zwecke des § 26 Abs. 2 S. 2 BDSG – heimlich erfolgen könnte.[1101] Zudem muss ausgeschlossen sein, dass der private Bereich des Beschäftigten mitüberwacht wird, z.B. wenn dieser das Dienst-Telefon auch mit nach Hause nehmen darf oder eine Pause macht. In Frage kommt eine Standorterfassung vor allem dann, wenn diese für die Sicherheit des Beschäftigten oder für den Schutz äußerst wertvoller Gegenstände des Arbeitgebers erforderlich ist.[1102] Abweichendes kann dann

1098 *Steidle*, MMR 2009, 167 (169).
1099 *Gola*, ZD 2012, 308 (309); *Seifert*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 88 DSGVO Rn. 142.
1100 Siehe **D. § 3 I. 1**; unklar *Seifert*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 88 DSGVO Rn. 142, der die Notwendigkeit einer Einwilligung und der Information des Beschäftigten ohne nähere Differenzierung annimmt.
1101 So auch WHWS/*Byers*, B. VII. GPS-Ortung, Rn. 27.
1102 *Seifert*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 88 DSGVO Rn. 142.

gelten, wenn diese anonymisiert werden. Hier muss jedoch in aller Regel an der Wirksamkeit der Anonymisierung gezweifelt werden: Standortdaten in Verbindung mit den Schichtplänen der jeweiligen Arbeitnehmer führen in aller Regel wieder zu einer Identifizierbarkeit. Der praktische Anwendungsbereich ist daher allenfalls marginal.

Etwas anderes gilt für die Ortung selbstverständlich dann, wenn diese auf Basis eines Gesetzes erfolgt, beispielsweise im Rahmen der digitalen Tachographen.[1103] In diesem Fall besteht eine Legitimation für die Verarbeitung nach Art. 6 Abs. 1 lit. c DSGVO, soweit diese zur Erfüllung der Pflicht erfolgt. Teilweise wird eine Fahrzeug-Ortung zur Optimierung der Ressourcennutzung im Rahmen des Flottenmanagements als zulässig erachtet, wenn sie offen und ausschließlich während der Arbeitszeit mit genauer Zweckfestlegung erfolgt.[1104] Darüberhinausgehende Auswertungen beispielsweise für People Analytics sind hiervon aber nicht gedeckt.

Da ein sinnvoller Anwendungsbereich für eine zulässige Ortung mittels LBS für People Analytics nicht ersichtlich ist, bleibt dieses Feld in dieser Arbeit außer Betracht.

c) Profiling und Scoring im Rahmen von Advanced People Analytics

Sollen die zulässigerweise erhobenen IT-Daten für Profiling genutzt werden, so handelt es sich hierbei um einen gesonderten Verarbeitungsvorgang[1105], der eigens an den Maßstäben des § 26 Abs. 1 BDSG gemessen werden muss. Dieser Vorgang des Profilings ist bei Advanced People Analytics von besonderer Bedeutung, da die erhobenen Daten nicht bloß menschenlesbar dargestellt, sondern durch eine inhaltliche Bewertung der Daten auch ein Mehrwert generiert werden soll. Hierzu ist es in aller Regel erforderlich, diese ins Verhältnis zu anderen Beschäftigten zu setzen, um eine Vergleichbarkeit herzustellen (hierzu bereits **E. § 1 II. 3** und **4**).

1103 *Kort*, RdA 2018, 24 (28); HdbIT-DSR/*Conrad/Treeger*, § 34 Recht des Datenschutzes, Rn. 301.

1104 WHWS/*Byers*, B. VII. GPS-Ortung, Rn. Rn. 29, 36 f.

1105 Siehe **E. § 1 II. 2**.

aa) Zweckbestimmung der Daten

Da die Verarbeitung zum Zwecke des Profilings ein eigener Verarbeitungsvorgang ist, muss dieser bereits bei der Erhebung der Daten vom Zweck umfasst sein, andernfalls ist eine Kompatibilitätsprüfung nach Art. 6 Abs. 4 DSGVO vorzunehmen. Bei der Zweckfestlegung ist darauf zu achten, dass dieser eindeutig und klar verständlich bestimmt ist.

(1) Spezifität der Zweckbestimmung

Sofern die Verarbeitung nicht auf den gesetzlichen Erlaubnistatbestand des § 26 Abs. 1 S. 1 BDSG gestützt wird, sondern aufgrund einer Einwilligung oder Betriebsvereinbarung erfolgen soll, müssen die Vorgaben zur Zweckbestimmung bei der Erhebung beachtet werden.[1106] Da feststellbar sein muss, welche Verarbeitungsvorgänge vom Zweck erfasst sind,[1107] dürfen auch im Rahmen einer Betriebsvereinbarung nicht zu vage Zwecke festgelegt werden. Aus diesem Grund wird es nicht ausreichend sein, wenn in einer Betriebsvereinbarung lediglich geregelt wird, dass die Daten zum Zwecke der *People Analytics* oder *Advanced People Analytics* verarbeitet werden, da diese ein sehr breites Feld darstellen und wie sich bereits aus den bisherigen Ausführungen zeigt, eine Vielzahl von Verarbeitungsvorgängen erfasst werden können.

Geboten ist daher eine Angabe, welche Analysen mit den Daten (insbesondere bei personenbezogenen Daten) angestrebt werden und ob Profiling-Maßnahmen stattfinden. Nur so kann überprüft werden, ob die Vorgänge auch vom in der Betriebsvereinbarung statuierten Zweck erfasst sind. Andernfalls müsste eine Definition des Begriffs „People Analytics" stattfinden, der die Zweckbestimmung weiter konkretisiert und die Verarbeitungsvorgänge so konkret wie möglich nennt, ohne zur Unverständlichkeit der Zweckbestimmung zu führen.

Beispielsweise könnte eine zulässige Zweckbestimmung lauten: „*Die Erfassung des Werts der Bildschirmzeit erfolgt zum Zwecke der Gesundheitsförderung des Arbeitnehmers durch Verhinderung von unergonomischen Bildschirm-*

1106 In aller Regel ist der Zweck der People Analytics für das konkrete Beschäftigungsverhältnis bereits durch die gesetzliche Zweckbestimmung in § 26 Abs. 1 S. 1 BDSG erfasst; hierzu bereits **E. § 1 I. 1. a**).

1107 *Article 29 Data Protection Working Party*, WP 203, S. 15; ebenso wohl EuArbRK/*Franzen*, Art. 5 DSGVO Rn. 5.

zeiten im Rahmen der durchgeführten People Analytics. Hierbei wird im Vergleich zu anderen Arbeitnehmern ein Vergleichswert generiert, der signifikante Abweichungen (mehr als 20 % über der durchschnittlichen Bildschirmzeit) erfasst und bewertet."

(2) Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO

Wurden die Daten bereits zum Zwecke der Durchführung des Arbeitsverhältnisses erhoben und sind weitergehende Analytics nicht mehr rechtssicher durch § 26 Abs. 1 S. 1 BDSG erfasst, sollte für die weitere Verarbeitung (das Profiling) eine Betriebsvereinbarung abgeschlossen werden. In diesen Fällen ist ein Kompatibilitätstest vorzunehmen. Etwas anderes gilt bei der (erneuten) Einwilligung zur Verarbeitung, da eine solche eine Legitimation zur Zweckänderung darstellen kann (Art. 6 Abs. 4 S. 1 DSGVO). Diese Privilegierung gilt allerdings nicht für Kollektivvereinbarungen, da Art. 6 Abs. 4 S. 1 DSGVO explizit eine Rechtsvorschrift der Union oder der Mitgliedsstaaten, die den Zielen des Art. 23 DSGVO dient, erfordert.

Anders als bei der Nutzung von IT-Systemdaten für People Analytics-Zwecke sind die Erhebungs- und Verarbeitungszwecke, wenn die Daten bereits zur Durchführung des Beschäftigungsverhältnisses erhoben wurden, sehr ähnlich und stehen in enger Verbindung, wenn die weiterführenden *People Analytics* zur Optimierung des Beschäftigungsverhältnisses oder der Arbeitsbedingungen genutzt werden sollen.

Mangels differenzierter höchstrichterlicher Rechtsprechung zum Themenkomplex *People Analytics* könnten Arbeitgeber Zweifel daran haben, ob ein Gericht im Streitfall die weitere Datenverarbeitung als „erforderlich" im Rahmen von § 26 Abs. 1 S. 1 BDSG erachten würde. Aus diesem Grund wird in der Praxis vielfach das Mittel der Betriebsvereinbarung gewählt und versucht, eine diesbezügliche Einigung mit dem Betriebsrat zu erzielen. Auch hier müssen die Betriebspartner aufgrund § 75 Abs. 2 BetrVG eine dem § 26 Abs. 1 S. 1 BDSG entsprechende Abwägung vorzunehmen; bei der Gewichtung der einzelnen Interessen steht ihnen jedoch ein (gerichtlich nur begrenzt überprüfbarer) Einschätzungsspielraum zu,[1108] sodass keine identische Erforderlichkeits- bzw. Verhältnismäßig-

1108 BAG, Beschl. v. 29.06.2004 – 1 ABR 21/03, NZA 2004, 1278 (1280) = BAGE 111, 173 = AP BetrVG § 87 1972 Überwachung Nr. 41 (m. Anm. Ehmann) im Hinblick auf die Erforderlichkeit der Datenverarbeitung im Rahmen der Abwägung nach § 75 Abs. 2 BetrVG.

keitsprüfung durch die Gerichte stattfindet, in welcher die gegenseitigen Interessen vom Gericht abschließend gewichtet werden. In gewissem Maß kann eine Parallele zur „Richtigkeitsgewähr des Tarifvertrags" durch den Schutz des Kollektivs gezogen werden.[1109]

Prüfungsgegenstand der gerichtlichen Kontrolle ist dann insbesondere das Überschreiten des eigenen Ermessensspielraums bei der Beurteilung, wodurch ein höheres Maß an rechtlicher Sicherheit geschaffen werden kann. Ebenfalls können weitere Zwecke außerhalb der Durchführung des Beschäftigungsverhältnisses durch eine Betriebsvereinbarung legitimiert werden. Da diese in der Regel eng mit dem Erhebungszweck zusammenhängen, ist eine Zweckvereinbarkeit – anders als bei IT-Systemdaten – nicht von vornherein ausgeschlossen, sondern in aller Regel gegeben.

Im Vergleich zum zuvor bei den Systemdaten vorgenommenen Kompatibilitätstest liegt gerade kein „*Missing Link*" vor, denn die Arbeitnehmer müssen damit rechnen, dass ihre personenbezogenen Daten auch für Zwecke der Optimierung der Geschäftsabläufe und Effektivierung der Arbeit durch Arbeitgeber genutzt werden.

Um allerdings den potenziellen negativen Folgen, die ein solches Profiling mit sich bringt, Rechnung zu tragen, müssen Arbeitnehmer bei zweckkompatibel verarbeiteten Daten – soweit es der konkrete Verarbeitungszweck zulässt – vor negativen Folgen geschützt werden. Grund hierfür ist, dass die Arbeitnehmer bei dieser Form der Verarbeitung – anders als wenn bereits die Daten auf Grundlage einer „weiten" Betriebsvereinbarung erhoben werden – bei der Erhebung noch nicht informiert wurden, dass ein Profiling mit ihren Daten stattfinden wird. Hierzu können in der Betriebsvereinbarung juristische Garantien für die Arbeitnehmer vorgesehen werden (**E. § 1 III. 2. b**) (**2**)).

bb) Rechtliche Vorgaben für das Profiling: Anwendbarkeit des § 31 Abs. 1 BDSG

Die DSGVO bestimmt für den in Art. 4 Nr. 4 definierten Begriff des *Profilings* keine weiteren Rechtmäßigkeitsvoraussetzungen, wie beispielsweise der nationale Gesetzgeber in § 31 BDSG für das Scoring. Nach § 31 Abs. 1 ist die „*Verwendung eines Wahrscheinlichkeitswerts über ein bestimmtes zukünftiges Verhalten einer natürlichen Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses*

1109 BeckOK DatenSR/*Riesenhuber*, Art. 88 DSGVO Rn. 68.

mit dieser Person (Scoring) nur zulässig, wenn […] 2. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit erheblich sind".

Scoring beruht auf der Grundhypothese, dass der Eintritt eines ähnlichen Verhaltens umso wahrscheinlicher ist, je mehr Faktoren einer Vergleichsgruppe in einer Person vereint sind.[1110] Score-Werte stellen Auffassung des BGH Meinungsäußerungen dar.[1111]

Ausweislich der Gesetzesbegründung[1112] und der Überschrift „Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften" hatte der Gesetzgeber nur das Kredit-Scoring im Blick, obwohl der Wortlaut des § 31 Abs. 1 BDSG jegliches Scoring bzw. Profiling erfasst.[1113] Es stellt sich also die Frage, ob die strengen Vorgaben zum Scoring auch für Maßnahmen im Rahmen von *People Analytics* anzuwenden sind.[1114] § 31 Abs. 2 BDSG kann hierbei außer Betracht bleiben, da sich diese Vorschrift auch materiell ausschließlich auf die Zahlungsfähig- und Zahlungswilligkeit einer Person bezieht.

(1) Europarechtswidrigkeit der Vorschrift

Überwiegend wird vorgebracht, dass die Vorschrift mangels entsprechender Öffnungsklausel in der DSGVO europarechtswidrig sei.[1115] § 31 Abs. 1

1110 *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 105.

1111 Zum Bonitätsscore BGH, Urt. v. 22.02.2011 – VI ZR 120/10, NJW 2011, 2204; zu Score-Werten allgemein *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 105.

1112 BT-Drs. 18/11325, S. 101 f.

1113 Gegen eine Anwendbarkeit daher *Rudkowski*, NZA 2019, 72 (75); so wohl auch *Kainer/Weber*, BB 2017, 2740 (2747); für eine Anwendbarkeit (von § 28b BDSG a.F.) wohl *Diercks*, PinG 2016, 30 (31); aufgrund des Wortlauts von § 28b BDSG a.F. ebenso im Grundsatz *Eschholz*, DuD 2017, 180.

1114 Für eine solche Interpretation *Hoeren*, MMR 2016, 8 (10).

1115 *Ehmann*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Anh. 2 zu Art. 6 DSGVO Rn. 17; wohl ebenso *Lapp*, in: Gola/Heckmann, BDSG, § 31 BDSG Rn. 4; unklar *Schulz*, zfm 2017, 91 (95 f.); im Ergebnis ebenso *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 6 DSGVO Rn. 166; *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, § 31 BDSG Rn. 4 f.; kritisch hierzu auch *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 110: Allenfalls als verbraucherschützende Vorschrift in unionsrechtskonformer Auslegung; a.A. *von Lewin-*

BDSG spezifiziert die Vorgaben für Scoring als einen Sonderfall des Profiling über die Vorgaben der Art. 6 und 22 DSGVO hinaus, ohne dass die jeweiligen Normen eine entsprechende Öffnungsklausel enthalten; auch Art. 22 Abs. 2 S. 1 lit. b DSGVO sei nicht anwendbar, da dies nur Fälle betreffe, in denen das Scoring Grundlage einer automatisierten Einzelfallentscheidung sei, während die Regelung des § 31 BDSG auch Profiling-Vorgänge ohne Entscheidung erfasse.[1116] Dagegen wird argumentiert, dass es auch „implizite Öffnungsklauseln" bei nicht abschließenden oder unvollständigen Regelungen in der DSGVO gebe und der deutsche Gesetzgeber einen solchen Gestaltungsspielraum in Anspruch genommen habe.[1117] In der Gesetzesbegründung nennt der Gesetzgeber jedenfalls keine Öffnungsklausel, auf die er sich stützt.[1118] Teilweise wird erwogen, § 31 Abs. 1 BDSG auf die Öffnungsklausel des Art. 6 Abs. 4 S. 1 i.V.m. Art. 23 Abs. 1 lit. i DSGVO zu stützen.[1119] Hiernach wäre eine Zweckänderung zulässig, wenn dies eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme darstellt, um den Schutz der betroffenen Personen oder der Rechte und Freiheiten anderer Personen sicherzustellen. Anwendbar wäre dann die Vorschrift jedoch nur, wenn das vorgenommene Scoring nicht bereits Erhebungszweck ist; § 31 Abs. 1 BDSG geht jedoch darüber hinaus und stellt allgemeine Regelungen für das Scoring auf, nicht nur für die Zweckänderung, sodass die Norm von dieser Öffnungsklausel nicht mehr erfasst ist. Auch das Argument der Unterkomplexität der DSGVO und der hierdurch geschaffenen „impliziten Öffnungsklauseln" überzeugt nicht: Gesetzlich vorweggenommene und abschließende Wertungen nationaler Gesetzgeber sind in Bezug auf abstrakte Formulierungen des europäischen Gesetzgebers unzulässig.[1120]

---

ski/Pohl, ZD 2018, 17 (19): § 31 BDSG beruhe auf einer impliziten Öffnungsklausel.

1116 *Ehmann*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Anh. 2 zu Art. 6 DSGVO Rn. 20; *Abel*, ZD 2018, 103 (105); Plath/*Kamlah*, Art. 22 DSGVO Rn. 9; a.A. HK DSGVO/BDSG/*Atzert*, Art. 22 DSGVO Rn. 93 ohne weitere Begründung.

1117 *von Lewinski/Pohl*, ZD 2018, 17 (19).

1118 BT-Drs. 18/11325, S. 101 f.

1119 *Schulz*, zfm 2017, 91 (94); *Hoeren/Niehoff*, RW 2018, 47 (64) stellen auf lit. e ab; ebenso *Taeger*, RDV 2017, 3 (7).

1120 So sogar zu einer Richtlinie: EuGH, Urt. v. 19.10.2016 – C-582/14, NJW, 2016, 3579 (3582) – Breyer Rn. 62 ff.; vgl. *Ehmann*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Anh. 2 zu Art. 6 DSGVO Rn. 21 m.w.N. aus der Rechtsprechung.

Selbst wenn man § 31 BDSG als Diskriminierungsschutz anstatt als datenschutzrechtliche Vorschrift sieht,[1121] bestehen aufgrund der Verortung im BDSG und dem Vereinheitlichungsgedanken der DSGVO erhebliche Bedenken: Die DSGVO soll ein (weitgehend) einheitliches Datenschutzniveau schaffen und § 31 BDSG würde etwaig vorgesehene Interessensabwägungen im Rahmen der DSGVO gesetzlich vorwegnehmen.[1122]

Einen anderen Ansatz bietet *Maamar*, der verdeutlicht, dass der Anknüpfungspunkt von § 31 BDSG im Vergleich zu § 28b BDSG a.F. ein anderer ist: § 31 BDSG stelle keine Legitimationsgrundlage zur Verarbeitung der Daten zu einem Score dar, sondern knüpfe an die folgende Verwendung des Scores zur Entscheidungsfindung an, wie sich bereits aus dem Wortlaut der Norm „Verwendung eines Wahrscheinlichkeitswerts" ergebe. Zudem verdeutliche auch § 31 Abs. 1 Nr. 3 BDSG, der von den Daten, die zur Berechnung „genutzt" wurden, spricht, dass die Berechnung des Scores bereits abgeschlossen sei, wenn der Anwendungsbereich der Vorschrift eröffnet wird.[1123] Da § 31 BDSG selbst nicht die Zulässigkeit der Score-Ermittlung regle, sei sie dementsprechend auch nicht unionsrechtswidrig.[1124]

Dies überzeugt allerdings nicht, da der Score ebenfalls ein personenbezogenes Datum darstellt[1125] und nach der Definition des Begriffs „Verarbeitung" in Art. 4 Nr. 2 DSGVO auch die Verwendung erfasst ist; mithin regelt § 31 BDSG eine datenschutzrechtliche Frage, für die es in der DSGVO keine Öffnungsklausel gibt.

§ 31 Abs. 1 BDSG ist unionsrechtswidrig und daher unanwendbar. Es ist im Folgenden dennoch die Frage nach den Voraussetzungen und Rechtsfolgen des § 31 BDSG aufzuwerfen, um zu überprüfen, ob die durch § 31 BDSG zusätzlichen Erfordernisse bereits in den allgemeinen Regelungen der DSGVO enthalten sind und – falls nicht – es zweckmäßig wäre, eine vergleichbare Regelung für Scoring im Bereich der (Advanced) People Analytics in einer eventuellen Betriebsvereinbarung vorzusehen.

1121 So z.B. *Kühling*, NJW 2017, 1985 (1988), der eine unionsrechtskonforme Auslegung mangels Öffnungsklausel vornehmen will; ähnlich *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 110, aber ohne klarem Ergebnis.

1122 *Abel*, ZD 2018, 103 (105).

1123 *Maamar*, CR 2018, 820 (825 f.).

1124 So wohl *Maamar*, CR 2018, 820 (828), indem er darauf abstellt, das die Vorschrift andernfalls unionsrechtswidrig sei.

1125 *Helfrich*, Teil IX. Kapitel 3, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Rn. 7.

(2) Regelungsgehalt des § 31 Abs. 1 BDSG

Nach § 31 BDSG muss die Verwendung des Wahrscheinlichkeitswerts über das zukünftige Verhalten einer Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dieser Person erfolgen, wobei nicht vorausgesetzt wird, dass es sich hierbei um eine automatisierte Einzelfallentscheidung im Sinne des Art. 22 DSGVO handelt. Die Bildung von Wahrscheinlichkeitswerten für Marketing-Maßnahmen (beispielsweise für gezielte Werbung oder zur Marktsegmentierung) unterliegt daher mangels Vertragsbezug nicht dem § 31 Abs. 1 BDSG.[1126] Auch bloße statistische Korrelationen sind nicht als Wahrscheinlichkeitswert zu verstehen, da solche Korrelationen, insbesondere mangels Ursache-Wirkungs-Beziehung keine Aussagekraft haben.[1127]

Zu beachten ist, dass der Gesetzgeber zwar nur das Kredit-Scoring bei der Schaffung der Vorschrift im Blick hatte, dem Wortlaut nach aber eine solche materielle Beschränkung für Abs. 1 nicht gilt, sodass auch andere Wahrscheinlichkeitswerte, die im Rahmen von Vertragsverhältnissen zur Anwendung kommen, erfasst werden.[1128] So ist § 31 Abs. 1 BDSG demnach anwendbar auf (Vor-)Auswahlentscheidungen im Bereich der Mitarbeitergewinnung.[1129] Nicht hingegen wird eine reine Potentialanalyse im Rahmen des Beschäftigungsverhältnisses erfasst, wenn diese nicht Grundlage einer Entscheidung wird oder werden soll.[1130]

Da sich der Wortlaut auf die „Verwendung des Wahrscheinlichkeitswerts“ beschränkt, finden die Voraussetzungen des § 31 Abs. 1 BDSG nicht bereits auf die Erhebung und Berechnung des Wertes Anwendung, sondern lediglich auf die Nutzung für die genannten Zwecke; für diese

1126 *Ehmann*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Anh. 2 zu Art. 6 DSGVO Rn. 31.

1127 *Ehmann*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Anh. 2 zu Art. 6 DSGVO Rn. 31.

1128 *Helfrich*, Teil IX. Kapitel 3, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Rn. 27, wo als Beispiele "Matchingwerte" im Rahmen von Partnervermittlungen oder Wahrscheinlichkeiten eines bestimmten Produkterwerbs durch einen bestimmten Kunden genannt werden; letzteres Beispiel ist jedoch im Hinblick auf den Vertragsbezug zweifelhaft.

1129 Plath/*Kamlah*, § 31 BDSG Rn. 18; *Klar*, BB 2019, 2243 (2251); a.A. *Kainer/Weber*, BB 2017, 2740 (2747).

1130 Plath/*Kamlah*, § 31 BDSG Rn. 20.

müssen die Daten den weiteren Voraussetzungen des § 31 Abs. 1 Nrn. 2 - 4 BDSG genügen.[1131]

So müssen nach § 31 Abs. 1 Nr. 2 BDSG die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sein.[1132] Diesbezüglich ist der Wortlaut deckungsgleich mit § 28b Nr. 1 BDSG a.F. Der Gesetzgeber zielte darauf ab, den materiellen Schutzstandard der Vorgängerregelung beizubehalten.[1133]

Die Voraussetzung, dass die Daten nachweisbar erheblich sein müssen, ergibt sich bereits aus dem in Art. 5 Abs. 1 lit. c DSGVO normierten Grundsatz der Datenminimierung. Da Ziel der Vorschrift ist, einen möglichst genauen Wahrscheinlichkeitswert zu erreichen, ist der Begriff der Erheblichkeit in einem statistisch-fachlichen Sinn zu verstehen, sodass alle Daten erheblich sind, die das Rechenergebnis beeinflussen.[1134] § 31 Abs. 1 Nr. 2 BDSG stellt somit keine zusätzlichen Erfordernisse in Bezug auf die Erheblichkeit der Daten auf.

Darüber hinaus ist die Vorschrift methodenneutral, da kein bestimmtes mathematisch-statistisches Verfahren vorgeschrieben wird. Es muss allerdings wissenschaftlich anerkannt sein.[1135] Nicht erforderlich ist, dass das Verfahren durch Prüfsiegel oder Zertifikate nachgewiesen wird, es muss aber Gegenstand wissenschaftlicher Untersuchungen gewesen sein und allgemein als zutreffende Bewertung der Wahrscheinlichkeitswerte für zukünftiges Verhalten eingestuft werden.[1136] Dies ist jedoch keine allzu hohe Anforderung: Rechtswidrig sind nur solche Verfahren, die auf reinem Zufall, auf nicht rationalisierbaren Intuitionen des Scorers oder fehlerhaften statistischen Verfahren beruhen. Somit wird keine bestimmte

1131 So auch *Helfrich*, Teil IX. Kapitel 3, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Rn. 79.

1132 *Ehmann*, in: Simitis, Bundesdatenschutzgesetz, § 28b BDSG Rn. 24, 27.

1133 BT-Drs. 18/11325, S. 101.

1134 *Ehmann*, in: Simitis, Bundesdatenschutzgesetz, § 28b BDSG Rn. 34 ff.; *Ehmann*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Anh. 2 zu Art. 6 DSGVO Rn. 46.

1135 Zur Kritik hierzu siehe ausführlich *Ehmann*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Anh. 2 zu Art. 6 DSGVO Rn. 39 ff.

1136 *Lapp*, in: Gola/Heckmann, BDSG, § 31 BDSG Rn. 29; in Bezug auf die Wissenschaftlichkeit des Verfahrens ebenso *Ehmann*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Anh. 2 zu Art. 6 DSGVO Rn. 42; *Klar*, BB 2019, 2243 (2251): Ein Algorithmus muss zumindest ursprünglich auf hinreichenden fachlichen bzw. wissenschaftlichen Standards beruhen.

Ergebnisgüte vorgeschrieben, ebenso wenig müssen die Verfahren auf dem „Stand der Technik" sein, wie manch andere Vorschrift das fordert.[1137] Es wird also nur eine gewisse „Basisrationalität" des Verfahrens gefordert,[1138] indem das Gesetz ein wissenschaftliches Verfahren verlangt, aber hierzu keine weiteren Vorgaben trifft, außer dass die Daten nachweislich für die Berechnung erheblich sein müssen, also in die Formel miteinfließen. An die Ergebnisgüte selbst werden keine Anforderungen gestellt. Diese Voraussetzung dürfte für zu generierende Scores in der Praxis nur von geringer Bedeutung sein, da Arbeitgeber ohnehin ein hohes Eigeninteresse haben, aussagekräftige Algorithmen zu verwenden, die eine hohe „Trefferquote" bzw. Genauigkeit besitzen.[1139]

Letztlich muss das Verfahren auch der Prognose zukünftigen Verhaltens dienen; insofern findet sich hier eine Einschränkung zum allgemeinen Profiling gem. Art. 4 Nr. 4 DSGVO für welches es ausreicht, dass bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, bewertet werden. Aufgrund der geforderten Prospektivität wird teilweise vertreten, dass § 31 BDSG keine Anwendung auf Auswahlentscheidungen im Arbeitsverhältnis finde, da hier in der Vergangenheit erworbene Kenntnisse und Fähigkeiten evaluiert werden sollen und weniger das zukünftige Verhalten.[1140] Dies überzeugt allerdings nicht, da Arbeitgeber gerade in Auswahlverfahren zwar ausschließlich auf Basis retrospektiver Daten entscheiden können, diese aber inhaltlich ausschließlich zukunftsgerichtet sind.[1141] Etwas anderes könnte allenfalls dann gelten, wenn im Falle von Mitarbeiterbeurteilungen im laufenden Arbeitsverhältnis die Leistung oder das Verhalten des vergangenen Jahres bewertet werden soll (z.B. zur Bemessung des Bonus oder zur (manuellen) Festlegung von Zielen).

Insofern würde § 31 Abs. 1 BDSG auf die untersuchten People Analytics-Verfahren Anwendung finden, ließe man die Europarechtswidrigkeit außer Betracht.

1137 *Gerberding/Wagner*, ZRP 2019, 116 (118), die sich insgesamt kritisch zur gesetzlich geforderten Qualität der Algorithmen äußern.

1138 *Gerberding/Wagner*, ZRP 2019, 116 (119).

1139 So auch *Schürmann*, Auswertung von Mitarbeiterdaten - (Any)/(No)thing possible?, in: Taeger, Smart world - smart law?, S. 513.

1140 *Sommer*, CuA 2014, 4; Plath/*Kamlah*, § 31 BDSG Rn. 26.

1141 So auch *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, S. 255.

(3) Vergleich mit den Vorgaben der DSGVO

Bereits aus dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) in Verbindung mit der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) ergibt sich, dass nur solche Daten für Scoring-Verfahren genutzt werden dürfen, die nachweisbar für das Ergebnis erheblich sind. Eine Regelung zur Wissenschaftlichkeit der genutzten Verfahren besteht nicht. Diese Anforderung könnte sich aus dem Grundsatz der Transparenz nach Art. 5 Abs. 1 lit. a DSGVO in Verbindung mit dem Grundsatz der Richtigkeit (Art. 5 Abs. 1 lit. d DSGVO) ergeben.

Der nicht-normative Teil der DSGVO enthält in Erwägungsgrund 71 S. 6 eine dem § 31 Abs. 1 Nr. 2 BDSG vergleichbare Regelung: So soll der Verantwortliche, um der betroffenen Person eine faire und transparente Verarbeitung zu gewährleisten, *geeignete mathematische oder statistische Verfahren für das Profiling verwenden* sowie technische und organisatorische Maßnahmen treffen, mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen Ergebnissen führen, korrigiert werden und das Risiko von Fehlern minimiert wird.

Der Grundsatz der Transparenz erfordert, dass es dem Betroffenen möglich sein muss, die Datenverarbeitung Schritt für Schritt nachvollziehen zu können; dies betrifft sowohl den Prozess der Verarbeitung selbst als auch den Zusammenhang zwischen den verschiedenen Elementen der Datenverarbeitung (was, wann, warum und wofür).[1142] Ausfluss des Prinzips sind die Rechte der Betroffenen auf Auskunft, Berichtung und Löschung (Art. 12 ff. DSGVO).[1143] So bestimmt beispielsweise Art. 13 Abs. 2 lit. f DSGVO, dass *zumindest* in Fällen der automatisierten Entscheidungsfindung einschließlich Profiling aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung im Rahmen einer Auskunft zur Verfügung werden müssen.

Unklar ist die Reichweite der Informationspflicht in Bezug auf den Inhalt. Aus dem Zusatz „zumindest" ist davon auszugehen, dass die Pflicht nur in den Fällen des Art. 22 DSGVO besteht, in anderen Fällen jedoch freiwillig möglich ist.[1144]

Eine inhaltliche „Basisrationalität" des Verfahrens wird jedoch vom Grundsatz der Transparenz nicht umfasst, sondern allenfalls die Transpa-

1142 Paal/Pauly/*Frenzel*, Art. 5 DSGVO Rn. 21.
1143 EuArbRK/*Franzen*, Art. 5 DSGVO Rn. 4.
1144 So BeckOK DatenSR/*Schmidt-Wudy*, Art. 15 DSGVO Rn. 77.

renz in Bezug auf die verwendeten Verfahren, die nicht notwendigerweise zu einem zumindest im Ansatz treffenden Ergebnis führen müssen. Selbst eine inhaltliche Transparenz in Bezug auf die konkret verwendeten Formeln dürfte in Anbetracht der BGH-Rechtsprechung zur Score-Formel der SCHUFA[1145] sehr geringen Anforderungen unterliegen. Diese ist zwar noch zum alten BDSG ergangen, wird aber von einem Teil der Literatur aus Gründen des Geschäftsgeheimnisschutzes weiterhin für anwendbar erachtet.[1146] Zwar hat der europäische Gerichtshof die abschließende Auslegungskompetenz für Normen der DSGVO, inhaltlich dürfte aber zumindest die Rechtsprechung weiter Geltung beanspruchen, da auf Seiten des Verantwortlichen ein gewichtiges Interesse besteht, die genaue Formel geheim zu halten und zu schützen und dieses Interesse auch im Wege von Auskunftsbegehren zu berücksichtigen ist, wie Erwägungsgrund 63 S. 5 verdeutlicht. Zudem wäre dem Betroffenen mit der Mitteilung des genauen Algorithmus aufgrund der hohen Komplexität nur wenig geholfen.

Aus dem Grundsatz der Richtigkeit könnte sich jedoch die Notwendigkeit eines wissenschaftlich-anerkannten Verfahrens ergeben. Diesem Grundsatz wird zwar – leider – datenschutzrechtlich eher geringe Aufmerksamkeit geschenkt,[1147] hat jedoch mit der DSGVO aufgrund der Bewehrung mit Bußgeld eine andere Qualität gewonnen.[1148] Dieser Grundsatz erfordert nicht nur die Richtigkeit der zugrundeliegenden Daten, sondern auch der Prognosen und Korrelationen.[1149] Schwierig ist es jedoch festzulegen, ab wann ein Verfahren und dessen Ergebnisse als „richtig" zu beurteilen sind. Hier hilft die englische Sprachfassung der DSGVO weiter, die nicht von „correct", sondern von „*accurate*" spricht und somit vielschichtiger ist; gemeint ist daher die Zielgerichtetheit, Genauigkeit und Exaktheit des Verfahrens im Sinne der Mathematik.[1150] Gleiches lässt

1145 BGH, Urt. v. 28.01.2014 – VI ZR 156/13, ZD 2014, 306.

1146 *Klar*, BB 2019, 2243 (2251); *von Lewinski/Pohl*, ZD 2018, 17 (23); kritisch BeckOK DatenSR/*Schmidt-Wudy*, Art. 15 DSGVO Rn. 78.3.

1147 Ausführlich zur Anforderung der Datenqualität im Datenschutzrecht, *Hoeren*, ZD 2016, 459.

1148 Auch wenn dieser Grundsatz nach Maßgabe des Art. 103 Abs. 2 GG inhaltlich zu unbestimmt sein dürfte, um Strafen oder Bußgelder unter Maßgabe zu verhängen, vgl. *Hoeren*, ZD 2016, 459 (461 f.).

1149 BeckOK DatenSR/*Schantz*, Art. 5 DSGVO Rn. 27; unklar *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 5 DSGVO Rn. 140: nur auf Tatsachenangaben anwendbar; Werturteile können nicht richtig oder falsch sein; ebenso *Herbst*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 5 DSGVO Rn. 60.

1150 *Hoeren*, ZD 2016, 459 (462).

sich aus der spanischen („*exactos*“) und französischen Fassung („*exactes*“) herleiten, die von „exakt“ und nicht „korrekt“ oder „richtig“ sprechen.[1151]

Hieraus ergibt sich, dass das Verfahren zumindest – analog den Anforderungen des § 31 Abs. 1 Nr. 2 BDSG – eine gewisse „Basisrationalität“ besitzen muss, um zielgerichtet und genau im Sinne der (sachlichen) Richtigkeit gem. Art. 5 Abs. 1 lit. d DSGVO zu sein. Insofern stellt das nationale Datenschutzrecht an das Scoring im Rahmen von People Analytics keine höheren Anforderungen als die DSGVO. § 31 Abs. 1 BDSG führt letztlich „nur“ zu einer Beweislastumkehr betreffend die Anwendung geeigneter mathematischer und statistischer Verfahren,[1152] nicht aber zu einer Änderung inhaltlicher Vorgaben.

(4) Zwischenergebnis

Obwohl § 31 BDSG aufgrund der Unionsrechtswidrigkeit und des zweifelhaften Anwendungsbereiches außerhalb des Kreditscorings nicht unmittelbar auf People Analytics-Verfahren anwendbar ist, sind die inhaltlichen Vorgaben des § 31 Abs. 1 Nr. 2 BDSG der Sache nach auch nach dem Unionsrecht zu beachten. Diese Anforderungen ergeben sich unmittelbar aus den Datenschutzgrundsätzen der Datenminimierung und Richtigkeit, sind jedoch im nationalen Recht genauer umschrieben. Ohnehin werden Arbeitgeber ein Interesse daran haben, bei den eingesetzten Verfahren korrekte Ergebnisse zu erzielen.[1153] Dieselbe Verpflichtung dürfte sich auch aus den arbeitsvertraglichen Pflichten in Verbindung mit dem Grundsatz aus Treu und Glauben (§ 242 BGB) ergeben. Letztendlich müssen Arbeitgeber darauf achten, nur solche Verfahren einzusetzen, die zumindest im Ansatz nachweisbar zum gewünschten Ergebnis führen und dabei nur solche Daten in den Algorithmus einfließen zu lassen, die für die Berechnung und das Ergebnis von Relevanz sind. Es versteht sich von selbst, dass diskriminierende oder willkürliche Algorithmen bereits aufgrund § 7 AGG bzw. des arbeitsrechtlichen Gleichbehandlungsgrundsatzes nicht eingesetzt werden dürfen und daher darauf geachtet werden muss, dass es auch nicht

1151 Anders aber beispielsweise wieder die polnische Fassung, die von „*prawidłowe*“ spricht, das übersetzt wiederum „korrekt“ bedeutet.

1152 Hierzu *Hoeren/Niehoff*, RW 2018, 47 (63).

1153 So auch *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, S. 256.

zu versteckten Diskriminierungen kommt und der Algorithmus plausible Ergebnisse erzeugt.[1154]

cc) Einsatz künstlicher Intelligenz möglich?

Eine Frage, die sich in diesem Zusammenhang stellt, ist, ob der Einsatz künstlicher Intelligenz für Scoringmaßnahmen möglich ist. Hiergegen könnte, wie bereits oben unter **C. § 3 II** dargestellt, die mangelnde Nachvollziehbarkeit der Entscheidungen unter dem Aspekt der Transparenz der Datenverarbeitung sprechen.

Durch den Einsatz von neuronalen Netzen stellt die involvierte Logik für den Menschen eine Art „Black Box" dar, die nur schwer bis gar nicht nachvollziehen lässt, weshalb ein solches System zu einer bestimmten Entscheidung kommt bzw. warum welche Kriterien welche Gewichtung erhalten sind.[1155]

Gefordert wird von der DSGVO für Scoring-Verfahren allerdings nur eine gewisse „Basisrationalität" sowie eine Zielgerichtetheit und Genauigkeit des mathematischen Verfahrens, keine vollständige Transparenz aller einzelnen Schritte. Dies wird außerhalb des Kontextes von automatisierten Einzelfallentscheidungen auch durch die beschränkten Informationspflichten nach Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO bestätigt, die dort gerade *keine* Informationspflicht über die involvierte Logik statuieren. So müssen die anwandte Formel und letztendlich ausschlaggebenden Kriterien und deren Gewichtung dem Betroffenen auch nicht mitgeteilt werden. Obwohl die deutsche SCHUFA-Rechtsprechung nicht einfach auf die europäische Ebene übertragen werden kann (teilweise – jedenfalls im Rahmen von § 31 BDSG – weiterhin für anwendbar erklärt wird[1156]), dürfte, die Abwägung auf der europäischen Ebene identisch sein.[1157]

1154 Siehe auch Erwägungsgrund 71 S. 6 a.E. DSGVO.

1155 Zur Funktionsweise von Künstlicher Intelligenz bereits oben, **C. § 2 II. 2.** Erste Ansätze für erklärbare KI-Systeme sind bereits vorhanden, hierzu *Körner*, 2.4 Nachvollziehbarkeit von KI-basierten Entscheidungen, in: Kaulartz/Ammann/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, Rn. 24.

1156 *Klar*, BB 2019, 2243 (2251); *von Lewinski/Pohl*, ZD 2018, 17 (23); a.A. wohl BeckOK DatenSR/*Schmidt-Wudy*, Art. 15 DSGVO Rn. 78.3.

1157 Siehe oben **E. § 1 III. 2. c) bb) (3)**.

Zu beachten ist, dass Verfahren der künstlichen Intelligenz nicht auf personenbezogene Daten angewandt werden, sondern auf anonymisierte Trainingssätze, aus denen Korrelationen erkannt werden sollen.[1158] Für letztere gilt ohnehin kein Datenschutzrecht (mehr). Die Frage ist hier lediglich, ob die Ergebnisse und Gewichtungen, die durch ein Training des Systems mit *Machine Learning* und KI entstanden sind, für Scoring für Personalentscheidungen verwendet werden dürfen.

Dies ist grundsätzlich zu bejahen, weil die personenbezogenen Daten mit Hilfe der durch KI errechneten Kriterien klar und nachvollziehbar gewichtet werden, letztendlich also nur noch die Ergebnisse des KI-Prozesses angewandt werden.

Beispiel: Für die Vorhersage der Zuverlässigkeit eines Bewerbers wurde bisher als maßgeblicher Faktor die Durchschnittsnote aus bisherigen Arbeitszeugnissen herangezogen (Gewichtung von allen Kriterien 0,6). Durch den Einsatz eines KI-Systems, das auf anonymisierter Basis die Daten aller vorhandenen Arbeitnehmer ausgewertet hat, wurde festgestellt, dass die Note aus dem Arbeitszeugnis gar keine so große Vorhersagekraft für die zukünftige Zuverlässigkeit hat. Festgestellt und berechnet wurde ein Faktor von 0,443. Dieser Faktor wird nun auf zukünftige Bewerbungen angewandt.

Bei der Anwendung der Ergebnisse handelt es sich vielmals um einen simplen Rechenvorgang (wie im obigen Beispiel die Multiplikation des Faktors mit der Durchschnittsnote), der auch nachvollziehbar ist. Weshalb das System diese Gewichtung als korrekt ermittelt hat, muss im Rahmen von Rechenschaft und Transparenz nicht genau feststehen. Ausreichend ist eine „Basisrationalität". Auch bei menschlichen Entscheidungen kann die Entscheidung nicht mit 100 %iger Genauigkeit an bestimmten Faktoren festgemacht werden; insofern darf hier von einer Maschine auch nicht mehr gefordert werden als von einem Menschen. Das Scoring mit KI bietet im Vergleich zur menschlichen Entscheidung sogar ein „Mehr" an Transparenz, weil es die Entscheidung an bestimmten Faktoren und Gewichtungen klar festmachen kann, auch wenn dies dem Betroffenen nicht offengelegt werden muss.

1158 Kritisch hierzu *Götz*, Big Data im Personalmanagement, S. 152 f. mit rein folgenbezogenen Erwägungen.

dd) Legitimation des Profilings im Rahmen von Advanced People Analytics

Als neuer Verarbeitungsvorgang muss das Profiling bzw. Scoring ebenfalls unter eine Legitimationsgrundlage subsumiert werden können. Hier kommen drei praxisrelevante Legitimationsgrundlagen in Betracht: (1) Einwilligung durch den Arbeitnehmer, (2) Erforderlichkeit nach § 26 Abs. 1 BDSG bzw. Art. 6 Abs. 1 lit. f DSGVO und (3) Legitimation durch eine Betriebsvereinbarung. Diese sollen im Folgenden untersucht werden.

(1) Legitimation des Profilings durch eine Einwilligung des Arbeitnehmers

Während die Einwilligung für Profiling im Rahmen von Online-Diensten[1159] die gängige Legitimationsform der Datenverarbeitung ist, sind die Anforderungen an eine wirksame Einwilligung im Arbeitsverhältnis faktisch deutlich höher, da das bestehende Abhängigkeitsverhältnis zwischen Arbeitnehmer und Arbeitgeber besondere Berücksichtigung findet.[1160] Anders als bei der Einwilligung im Rahmen von Simple People Analytics[1161] ist die Eingriffsintensität durch die erfolgende Bewertung von Persönlichkeitsaspekten deutlich höher. Zudem kann die Transparenz geringer ausfallen, wenn beispielsweise die konkrete Formel und Gewichtung der einzelnen maßgeblichen Faktoren nicht mitgeteilt wird.

Einwilligungen in solche Verfahren sind daher unter dem Aspekt der Rechtssicherheit als höchst kritisch zu betrachten, zumal Arbeitnehmer Ihre Einwilligung jederzeit widerrufen können (Art. 7 Abs. 3 DSGVO, § 26 Abs. 2 S. 4 BDSG) und somit für zukünftige Auswertungen die personenbezogenen Daten des betroffenen Arbeitnehmers nicht mehr genutzt werden dürfen. Dies stellt mitunter einen enormen administrativen Aufwand dar, wenn Daten in eine Vielzahl von Auswertungsvorgängen einfließen bzw. eingeflossen sind (bei retrospektiver Betrachtung). Zwar gilt der Widerruf nur für die Zukunft und berührt daher die bisher auf der Einwilli-

1159 Bspw. bei Facebook, Instagram, WhatsApp oder sonstigen Netzwerken, auch wenn diese mitunter in den seitenlangen Datenschutzerklärungen von den Benutzern nicht wirklich wahrgenommen werden.

1160 Zu den Anforderungen an eine wirksame Einwilligung siehe bereits **D. § 1 III. 2. a**).

1161 Hierzu **E. § 1 III. 1. a**).

gung durchgeführten Datenverarbeitungsvorgänge nicht (Art. 7 Abs. 3 S. 2 DSGVO), dennoch dürfen die durchgeführten Auswertungen, sofern diese nicht anonymisiert sind und somit nicht mehr dem Datenschutzrecht unterliegen, zukünftig nicht mehr für weitere Verarbeitungsvorgänge genutzt werden, da hierfür keine Legitimationsgrundlage mehr besteht.[1162]

Ob eine Einwilligung zulässig ist, ist jeweils im Einzelfall zu entscheiden; sie sollte jedoch auch für solche Verfahren nur als allerletzte Option in Betracht gezogen werden (siehe aber **E. § 1 III. 2. c) dd) (2) (c)**).

(2) Erforderlichkeit nach § 26 Abs. 1 BDSG

Eine weitere Legitimationsgrundlage könnte die Erlaubnisnorm für Datenverarbeitungen im Arbeitsverhältnis, § 26 Abs. 1 S. 1 BDSG, darstellen, wenn personenbezogene Daten eines Arbeitnehmers für Profiling und Scoring genutzt werden sollen. Zu beachten ist, dass für die weitere Beurteilung davon ausgegangen werden muss, dass die Daten bereits rechtmäßig erhoben wurden (hierzu siehe bereits **E. § 1 III. 2. a) cc)**). Eine Zweckkompatibilitätsprüfung muss in diesem Fall nicht mehr stattfinden, da für APA-Profiling erforderlich ist, dass die Daten für den Zweck der Durchführung des Beschäftigungsverhältnisses erhoben wurden und eine zweckkompatible Verarbeitung anderweitig erhobener Daten (z.B. Sensor-/Systemdaten) ausscheidet.[1163]

Für die im Rahmen von § 26 Abs. 1 S. 1 BDSG vorzunehmende Abwägung kommt es daher ausschließlich auf den Vorgang des Profilings oder Scorings unter Zugrundelegung der erhobenen personenbezogenen Daten an. Es muss also mit anderen Worten geprüft werden, ob die erhobenen personenbezogenen Daten nicht nur zum Zwecke der Durchführung des Beschäftigungsverhältnisses (ggf. zweckändernd), sondern auch zum Zwecke der Erstellung eines Persönlichkeitsprofils genutzt werden dürfen.

Anders als bei Simple People Analytics handelt es sich nicht mehr um eine reine Fortschreibung bereits vorliegender Daten mit einfachen mathematischen Verfahren, sondern um die inhaltliche Bewertung von

---

1162 So wohl auch EuArbRK/*Franzen*, Art. 7 DSGVO Rn. 6 m.w.N.: Ein in der Vergangenheit erstellter Werbefilm, in welchem der Arbeitnehmer kurz im Rahmen eines Gruppenbildes gezeigt wird, darf entgegen bisheriger Rechtsprechung (BAG, Urt. v. 11.12.2014 – 8 AZR 1010/13, NZA 2015, 604) zum BDSG a.F. wohl nicht mehr weiterverwendet werden.

1163 Siehe ausführlich **E. § 1 III. 2. b) (3)**.

Persönlichkeitsmerkmalen wie beispielsweise Verhalten und Leistung und somit die Generierung von grundsätzlich neuen[1164] personenbezogenen Daten mit hoher Persönlichkeitsrelevanz. Die Anforderungen an einen solchen Verarbeitungsvorgang müssen daher deutlich höher gesetzt werden als bei der simplen Fortschreibung bestehender Werte durch einfache statistische Methoden. Zudem können sich solche Aussagen und Prognosen als individuell falsch, ungerecht bzw. willkürlich oder diskriminierend erweisen, sodass die Persönlichkeitsrechte erheblich beeinträchtigt werden können.[1165]

Maßgeblich ist vor allem die Eingriffsintensität beim Betroffenen.[1166] Durch die Profilbildung können Risiken des Kontextverlustes sowie der Unrichtigkeit entstehen, wenn aus dem Vorliegen bestimmter Eigenschaften auf das Vorhandensein anderer Eigenschaften geschlossen wird. Diese Gefahr besteht insbesondere, wenn die zugrundeliegenden Daten nicht mehr aktuell sind oder falsch erfasst wurden. Zudem können einzelne spezifische Datensätze sehr einfach zu einem Gesamtprofil zusammengefasst werden, was zu persönlichem Überwachungsdruck führen könnte,[1167] weil hierdurch mitunter neue Daten generiert werden, die aussagekräftigte Vorhersagen zum Verhalten der betroffenen Person treffen können. Hierdurch entsteht eine enorme Eingriffsintensität. Bereits das Erstellen eines Teilabbilds der Persönlichkeit gegen den Willen des Betroffenen ist daher, wie das Bundesverfassungsgericht in der *Volkszählungs*-Entscheidung herausgearbeitet hat, in der Regel verfassungswidrig.[1168] Werden aber auf Basis einer Einwilligung, z.B. im Rahmen des Online-Marketings oder bei sozialen Netzwerken Persönlichkeitsprofile erstellt, so sind diese nicht *per* se als verfassungswidrig zu bezeichnen.[1169] Die Abgabe der Einwilligung auch die Eingriffsintensität, zumal nicht ein staatlicher Akteur auf der anderen Seite handelt, sondern ein privater Konzern. Etwas anderes kann etwa gelten, wenn der Konzern weltweit tätig ist und aufgrund Gesetze

1164 So auch *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 4 DSGVO Rn. 6.
1165 *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 4 DSGVO Rn. 9.
1166 *Brecht/Steinbrück/Wagner*, PinG 2018, 10 (11 f.).
1167 *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 117.
1168 BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1 (53 f.) – Volkszählungsurteil Tz. 178.
1169 *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 118 m.w.N.

in anderen Ländern dem Staat einen Zugriff auf die Daten gewähren muss.[1170]

Zur Feststellung der Eingriffsintensität ist zu unterscheiden, ob ein Überwachungsdruck für eine Gruppe von Arbeitnehmern oder für einen einzelnen Arbeitnehmer entsteht. Bei ersterem kommt es im Weiteren maßgeblich darauf an, ob sich eine Identifizierbarkeit im Nachhinein ergeben kann.[1171] Ist dies nicht der Fall, liegen keine personenbezogenen Daten und somit auch kein Eingriff in das Persönlichkeitsrecht vor; das Datenschutzrecht ist nicht anwendbar. Anonymes Profiling und Scoring von Gruppen sind somit datenschutz- und verfassungsrechtlich möglich.

Steht – wie hier beim personenbezogenen Profiling – allerdings der einzelne Arbeitnehmer im Fokus, so müssen die unternehmerischen Interessen (Art. 12, 14 GG im Lichte der Art. 16 f. EU-GRC) mit dem Recht auf Privatheit des Arbeitnehmers (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG im Lichte der Art. 7 f. EU-GRC) abgewogen und in praktische Konkordanz gebracht werden,[1172] wobei die Rahmenbedingungen ebenfalls von besonderer Bedeutung sind. Insbesondere der erzeugte Überwachungsdruck bei Bewertung und Prognose des Verhaltens und der Arbeitsleistung kann einem Profiling bzw. Scoring entgegenstehen.[1173]

(a) Scoring von Bewerbern

Hohe Relevanz hat diese Diskussion im Bereich des Bewerber-Managements, insbesondere bei begehrten Stellen, wo sich viele Menschen bewerben und eine Flut an Bewerbungen eingeht. In diesen Fällen ist es für die Personalverantwortlichen kaum möglich, diese Bewerbungen alle einzeln zu sichten, sodass gewisse Vorauswahlen bzw. Einstufungen getroffen werden müssen. Eine sehr effektive Methode kann das Profiling / Scoring der Bewerber anhand der in einer Online-Maske eingetragenen oder einem CV-Parser ausgelesenen Daten sein. Das Personalmanagement gibt die Anforderungen für die Stelle an die gewünschte Person in eine Maske im

1170 Vgl. hierzu das aktuelle Urteil des EuGH zum „Privacy Shield", EuGH, Urt. v. 16.07.2020 – C-311/18, ECLI:EU:C:2020:559 – Schrems II.

1171 *Brecht/Steinbrück/Wagner*, PinG 2018, 10 (11 f.).

1172 *Brecht/Steinbrück/Wagner*, PinG 2018, 10 (12), die allerdings nur die nationalen Grundrechte in den Fokus stellen.

1173 Siehe hierzu bereits **E. § 1 III. 2. a) cc) (4)**.

System ein und das System ermittelt den Match-Wert in Form eines Scores des einzelnen Bewerbers mit den Anforderungen des Unternehmens.

Selbstverständlich muss in diesem Rahmen darauf geachtet werden, dass nur solche Daten erhoben werden, die vom Fragerecht des Arbeitgebers erfasst sind.[1174] Die zulässigerweise erhobenen Daten durchlaufen im Anschluss einen Auswahlalgorithmus, der die Bewerber nach der Eignung auf die passende Stelle reiht und jeweils mit einer Punkteanzahl oder Note versieht.[1175] Eine automatische Vorauswahl findet an dieser Stelle noch nicht statt (siehe hierzu **D. § 1 V. 3. c) aa)**).

Da eine wirksame Einwilligung in diesem Stadium des (erwünschten oder angebahnten) Beschäftigungsverhältnisses aufgrund mangelnder Freiwilligkeit ausscheidet,[1176] muss die Legimitation über § 26 Abs. 1 S. 1 BDSG erfolgen; die Datenerhebung also zum Zweck der Entscheidung über die Begründung des Beschäftigungsverhältnisses[1177] erforderlich sein. Art. 22 DSGVO, welcher die Zulässigkeit automatisierter Einzelfallentscheidungen regelt, ist bei einem reinen Ranking (noch) nicht anwendbar, sofern ein menschlicher Entscheider die Letztentscheidung auf Basis der Datengrundlage trifft.[1178]

Hierbei sind die berechtigten Interessen des Arbeitgebers an einem Scoring der Bewerber im Rahmen der Entscheidung über die Begründung des Beschäftigungsverhältnisses gegenüber entgegenstehenden Interessen der Bewerber abzuwägen. Die Arbeitgeberinteressen liegen in einer Effektivierung des Bewerbermanagements sowie (was ebenfalls im Interesse der Bewerber ist) an einer möglichst passenden und gerechten Auswahl des besten Bewerbers für die ausgeschriebene Stelle. Auf der Bewerberseite lauten die Interessen grundsätzlich dahingehend, möglichst wenig private Daten offenbaren zu müssen und insbesondere selbst entscheiden zu können, welche Daten der Arbeitgeber für die Bewertung erhält bzw. verarbeitet. Darüber hinaus hat auch der Bewerber ein Interesse daran, eine faire Chance zu bekommen und bei der Auswahl berücksichtigt zu werden.[1179]

1174 Vgl. hierzu die ausführliche Kommentierung von *Seifert*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 88 DSGVO Rn. 75 ff. m.w.N.; zur Problematik des Preisgebens von Daten, um eine bessere Chance zu erhalten, *Däubler*, Gläserne Belegschaften, S. 182 Rn. 250c.

1175 Ein Beispiel hierzu wurde bereits oben bei **C. § 3 I** genannt.

1176 Siehe hierzu bereits **D. § 1 III. 2. a) bb) (2)**; ferner *Kainer/Weber*, BB 2017, 2740 (2742).

1177 Zu dieser Zweckbestimmung siehe **E. § 1 I. 1. b) aa)**.

1178 So bereits *Blum/Kainer*, PERSONALquarterly 2019, 22 (26).

1179 Zum Interessenkonflikt im Arbeitsverhältnis, siehe **A. § 2**.

Größtes Risiko neben Persönlichkeitsdurchleuchtungen dürften in diesem Zusammenhang (versteckte) Diskriminierungen durch Algorithmen sein,[1180] auch wenn Algorithmen mitunter auch mit dem Ziel eingesetzt werden, gerade solche zu verhindern. Grundlage für solche Diskriminierungen können eine fehlerhafte Datenbasis für den Algorithmus oder Modellfehler sein, aber auch diskriminierende Entscheidungen in der Vergangenheit, aus die der Algorithmus „lernt".[1181] Hier muss nicht nur im Diskriminierungskontext darauf geachtet werden, sondern auch im datenschutzrechtlichen, denn auch diese Gefahr stellt eine mögliche negative Folge für den Betroffenen dar, die im Rahmen der Interessensabwägung zu berücksichtigen ist. Wird der Auswahlalgorithmus hingegen nur für bestimmte fachliche Kriterien verwendet und bleiben andere Merkmale außer Betracht (z.B. Auswertung des Fotos auf „Sympathie" oder Einbeziehung des Geschlechts in ein Ranking), so dürfte eine diskriminierende Entscheidung eher fern liegen. Je mehr Daten der Algorithmus jedoch als Grundlage verwendet, die nicht im rein fachlichen Bereich liegen, desto höher wird das Risiko einer unzulässigen Diskriminierung. Arbeitgeber müssen in solchen Fällen Vorkehrungen schaffen, indem die Systeme beispielsweise statistisch auf eine Voreingenommenheit getestet werden oder Quotierungen festgelegt werden (z.B. eine bestimmte Frauenquote in den Top-10-Ergebnissen der Ranking-Vorschläge).[1182]

Die Tendenz im Rahmen von People-Analytics geht allerdings dazu, statt „harten" Kriterien eher weiche Kriterien aus dem Persönlichkeitsbereich der Arbeitnehmer für Auswahlentscheidungen heranzuziehen: So könnte beispielsweise ein Unternehmen solche Softwareentwickler bevorzugt einstellen, die in ihrer Freizeit einem bestimmten Hobby nachgehen, da durch interne Auswertungen mit Hilfe von KI herausgefunden wurde, dass hier eine Korrelation besteht.[1183] Die Grenzen werden durch die (inzwischen) feingliedrige Rechtsprechung zum Fragerecht des Arbeitgebers gesetzt. In keinem Falle darf es zu Totalabbildungen der Persönlichkeit des Bewerbers kommen.

Teilweise wird in diesem Rahmen vertreten, dass allein der Wunsch nach einer besseren Personalplanung nicht von den in § 26 Abs. 1 BDSG

1180 Zu den Diskriminierungsrisiken speziell in Bezug auf das AGG beim Einsatz von Algorithmen im Bewerbungsverfahren, siehe *Dzida/Groh*, NZA 2018, 1917.

1181 *Dzida/Groh*, NZA 2018, 1917; ebenso bereits **C. § 3 III**; ferner *Culik*, Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, S. 81 ff.

1182 Vgl. *Dzida/Groh*, NZA 2018, 1917 (1922).

1183 Beispiel aus *Dzida*, NZA 2017, 541 (542).

genannten Zwecken erfasst ist, insbesondere, wenn als Grundlage (anonymisierte) Daten von Beschäftigten als Vergleichsbasis herangezogen werden.[1184] Diese Auffassung geht von einem zu engen Erforderlichkeitsbegriff aus. § 26 Abs. 1 BDSG setzt die Erforderlichkeit für die „Entscheidung über die Begründung" voraus; welche Daten der Arbeitgeber für die Entscheidung benötigt, liegt zwar nicht vollständig in seinem Ermessen, aber sofern ein berechtigtes Interesse für die Kenntnis besteht und die Interessen des Bewerbers an der Geheimhaltung nicht überwiegen, ist eine Verarbeitung zulässig.[1185]

Das Scoring auf Basis „harter Fakten" und anschließende Ranking von Bewerbern ist – jedenfalls bei einer hohen Anzahl an Bewerbungen auf eine Stelle[1186] – „erforderlich" im Sinne von § 26 Abs. 1 S. 1 BDSG, wenn Arbeitgeber ein entsprechendes System einsetzen. So müssen einerseits Bewerber damit rechnen, dass ihre Daten verarbeitet und in Relation zu den Stellenvoraussetzungen gesetzt, andererseits auch, dass sie inhaltlich bewertet werden. Es ist nahezu selbstverständlich, dass kein Personalverantwortlicher eine sehr hohe Anzahl an Bewerbungen sichten kann, zumal dies auch unwirtschaftlich wäre. Arbeitgeber sind daher bereits jetzt gezwungen, bei Bewerbungsfluten ein effektives Selektionssystem zu etablieren.

So wäre ein Aussortierungssystem, das nach dem Prinzip verfährt, dass jede zweite Bewerbung ungesichtet im Müll landet, weder nach datenschutzrechtlichen noch diskriminierungsrechtlichen Gesichtspunkten unzulässig, auch wenn es in hohem Maße unfair ist und hierdurch möglicherweise der am besten geeignete Bewerber aussortiert wird. Andererseits könnten auch Bewerbungen aussortiert werden, die beispielsweise nicht in einem PDF-Gesamtdokument gesendet wurden, sondern in unzähligen Einzeldokumenten bei einer E-Mail-Bewerbung; auch hierdurch würde man allenfalls solche Bewerber effektiv aussortieren, die keine ausreichenden PC-Kenntnisse besitzen, die Anforderungen der Stellenbeschreibung nicht korrekt lesen (oder eine entsprechende Software nicht besitzen). Zwar vermindert man hiermit ebenfalls den Aufwand in der Personalabteilung, alle Dokumente entsprechend einzeln zu sichten bzw.

1184 Noch zu § 32 BDSG a.F.: *Bissels/Mayer-Michaelis/Schiller*, DB 2016, 3042.

1185 Zum Erhebungszweck „Erforderlichkeit für die Entscheidung über die Begründung" vgl. bereits **E. § 1 I. 1. b) aa)**.

1186 Aufgrund des geringeren Eingriffs in die Rechte der Arbeitnehmer gelten geringere Anforderungen als im Rahmen der automatisierten Einzelfallentscheidung; zum Begriff der Erfordertlichkeit dort vgl. **D. § 1 V. 3. d) aa)**.

auszudrucken, die Effizienz dieses Verfahrens hängt jedoch stark von der ausgeschriebenen Stelle ab. Für eine Sekretariatsstelle könnte dies unter Umständen ein taugliches Kriterium sein, sofern dies in den Anforderungen an die Bewerbung explizit verlangt wurde.

Ein computerbasiertes System, das den Inhalt der Bewerbungen abgleicht und mit dem konkreten Stellenprofil vergleicht, ist jedenfalls effektiver als – teilweise eingesetzte – Verfahren, die dem Zufall unterliegen. Der Bewerber hat ebenfalls ein Interesse daran, keinem Zufallssystem „zum Opfer zu fallen". Ein solches System lässt eine schnelle Erstauswahl der Bewerber treffen, wobei grundsätzlich die Gefahr besteht, dass aufgrund von Eingabefehlern bzw. Auswertungsfehlern falsche Scores generiert werden und geeignete Bewerber im Ranking weit unten landen. Zu beachten ist an dieser Stelle allerdings, dass noch keine automatisierte Einzelfallentscheidung getroffen wird, sondern ein menschlicher Entscheider die „Vorauswahl" des Computers noch inhaltlich auf Basis der Datengrundlage (nicht allein des Scores) nochmals überprüfen und bestätigen muss. Ansonsten läge ein Fall des Art. 22 DSGVO vor.

Generiert die Software im obigen Beispiel also den „Scorewert 0" für solche Bewerber, so müsste der Sachbearbeiter überprüfen, ob mehrere Dateien eingegangen sind oder nur ein Gesamt-PDF vorliegt. In letzterem Fall wäre der erstellte Scorewert falsch und der Sachbearbeiter müsste manuell eine Neubewertung vornehmen.

Werden hingegen „weiche Daten" aus dem Persönlichkeitsbereich gescort, so ist zunächst erforderlich, dass der Arbeitgeber diese Daten rechtmäßig erheben durfte. Das o.g. Beispiel des Vergleichs der Hobbys des Bewerbers mit solchen von Angestellten ist in der Praxis datenschutzrechtlich unzulässig, da ein Hobby ausschließlich dem Privatleben zuzuordnen ist und für die Beschäftigung grundsätzlich[1187] ohne Relevanz.[1188] Eine Einwilligung scheidet mangels Freiwilligkeit aus, ebenso eine Legitimation durch Betriebsvereinbarung, da der Betriebsrat für die Bewerber persönlich nicht zuständig ist[1189] und eine etwaige Betriebsvereinbarung im Übrigen auch nach § 75 Abs. 2 BetrVG aufgrund des unzulässigen Eingriffs in das Persönlichkeitsrecht des Arbeitnehmers rechtswidrig wäre.

1187 Kein Grundsatz ohne Ausnahmen: Wenn ein Hobby eine Verbindung zu der Tätigkeit aufweist, dann kann eine solche Frage zulässig sein, z.B. jemand soll die Öffentlichkeitsarbeit in einem Ruderverein wahrnehmen; die Frage, ob jemand selbst in seiner Freizeit rudert, wäre also legitim.

1188 Vgl. *Kort*, NZA-Beilage 2016, 62 (67).

1189 *Bausewein*, DuD 2016, 139 (140).

Psychologische Eignungstests, z.B. im Rahmen von Assessment-Centern wurden in der höchstrichterlichen Rechtsprechung kaum behandelt,[1190] sind jedoch im Grundsatz zulässig, wenn sie solche Daten über den Bewerber generieren, die auch konkreten Bezug zur Stelle haben (so z.B. Belastbarkeit, Durchsetzungsfähigkeit, wenn ein vorheriger Stelleninhaber an diesen Merkmalen gescheitert ist[1191]),[1192] also für die Entscheidung über die Begründung erforderlich sind. Obwohl oft von den Bewerbern eine Einwilligung eingeholt wird, ist diese mangels Freiwilligkeit in den wenigsten Fällen wirksam.[1193] Man wird wohl davon ausgehen müssen, dass ein bloßes Interesse des Arbeitgebers, einen charakterlich besser passenden Bewerber einzustellen nicht ausreichen mag, wenn der Charakterzug keinen konkreten Bezug zur Arbeit hat, weil der Arbeitnehmer überwiegend nur mit der Bedienung von Maschinen beschäftigt ist und nicht im Team arbeitet.[1194] Je höher der Bewerber in der Hierarchie eingesetzt werden soll und desto mehr Personal- und Unternehmensverantwortung er letztlich hat, desto wichtiger sind seine persönlichen (Führungs-)Eigenschaften, sodass bei einem Manager ein Assessment-Center mit (weitgehenden) Persönlichkeitsanalysen eher in Betracht kommt als bei einem „einfachen Arbeitnehmer" am unteren Ende der Hierarchie.

Da bereits recht hohe Anforderungen an eine Datenerhebung bzgl. „weicher Kriterien" bestehen und dies ohnehin erst bei Bewerbern mit einem hohen Verantwortungsspektrum in Betracht kommt, darf aufgrund des nur geringfügigen weiteren Eingriffs in das Persönlichkeitsrecht im Vergleich zur Ersterhebung auch ein weitergehendes Scoring durchgeführt werden, um die erhobenen Daten entsprechend in einen Vergleich einbeziehen zu können. Ohne eine entsprechende Visualisierung der Ergebnisse der psychologischen Tests besitzen diese wenig Aussagekraft für die Entscheidung über die Begründung des Arbeitsverhältnisses. Es ist daher sogar von einer (zwingenden) Erforderlichkeit des Scorings im Anschluss an die Tests auszugehen, um die gewünschte Entscheidung als Personalverantwortlicher oder Manager (der nicht Psychologe o.ä. ist) treffen zu können.

1190 So auch *Franzen*, NZA 2013, 1 (2).
1191 Beispiel von *Bausewein*, DuD 2016, 139 (142).
1192 *Franzen*, NZA 2013, 1 (2).
1193 *Kort*, NZA-Beilage 2016, 62 (71); unklar *Bausewein*, DuD 2016, 139 (141 f.); siehe bereits **D. § 1 III. 2. a) bb) (2)**.
1194 *Bausewein*, DuD 2016, 139 (143).

Nota bene: Sofern als Daten- und Vergleichsbasis personenbezogene Daten von (erfolgreichen) und bereits angestellten Arbeitnehmern genutzt werden sollen, ist zu beachten, dass die Verarbeitung der personenbezogenen Daten der bereits angestellten Arbeitnehmer nicht mehr von der Ermächtigungsgrundlage § 26 Abs. 1 BDSG erfasst ist; die Zwecke des § 26 Abs. 1 BDSG sind nicht einschlägig, da die Daten weder zur Entscheidung über die Begründung ihres konkreten Anstellungsverhältnisses, noch für die Durchführung genutzt werden, sondern für die Optimierung des Bewerbungsverfahrens für neue potentielle Arbeitnehmer. § 26 Abs. 1 BDSG sperrt allerdings nicht den Rückgriff auf Art. 6 Abs. 1 lit. f DSGVO.[1195] Dem Arbeitgeber ist ein berechtigtes Interesse anzuerkennen, solche Daten – zumindest für die Anonymisierung zum Zwecke der Nutzung im Bewerbungsprozess – zu nutzen.[1196] Alternativ käme auch eine Einwilligung des zu vergleichenden Arbeitnehmers nach Art. 7 DSGVO in Betracht, da dieser als Positivbild zur Bewertungsgrundlage herangezogen werden soll und daher keine Nachteile aus der Datenverarbeitung zu befürchten hat, zumal die Daten auch anonymisiert werden können; Zweifel an der Freiwilligkeit bestehen daher nur in geringem Maße.

(b) Scoring der Arbeitsleistung

Nach erfolgreicher Begründung des Arbeitsverhältnisses haben Arbeitgeber ein weitergehendes Interesse auch die Arbeitsleistung der Beschäftigten zu überwachen, um eventuellen Fehlentwicklungen mit weiteren Maßnahmen gegensteuern zu können. Dem Arbeitgeber ist grundsätzlich ein Recht einzuräumen, zu kontrollieren, ob die Beschäftigten die vertraglich vereinbarte Arbeitsleistung erbringen und somit ihren Pflichten nachkommen.[1197] Hierfür ist der Einsatz technischer Hilfsmittel zulässig.[1198] Allerdings kann das Erstellen von Scores über die Leistung von Arbeitnehmern und das folgende Vergleichen der Scores mit anderen Arbeitnehmern zu einem enormen Leistungs- und Anpassungsdruck führen. So könnten beispielsweise Low-Performer schnell durch solche Maßnahmen

1195 Paal/Pauly/*Gräber/Nolden*, § 26 BDSG Rn. 10 ff.
1196 So wohl auch unter Rückgriff auf § 28 Abs. 1 S. 1 Nr. 2 BDSG a.F., *Dzida*, NZA 2017, 541 (542 f.).
1197 *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 105.
1198 *Däubler*, Gläserne Belegschaften, S. 190 Rn. 260a.

individualisiert und gekündigt werden.[1199] Dies gilt umso mehr, wenn das Scoring-Verfahren dem Arbeitnehmer nicht im Detail bekannt ist[1200] oder individualisierte Daten gar in Dashboards (dazu im Folgenden **E. § 3**) auf Gruppen-/ oder Abteilungsebene (bei Vergleichbarkeit) dargestellt werden und zu einer Mehrleistung motivieren sollen, m.a.W. schwache Mitarbeiter an den Pranger gestellt werden. Jedenfalls ausgeschlossen sind daher in diesem Zusammenhang solche Scores, die darauf beruhen, dass die Primärleistungspflicht lückenlos überwacht wird.[1201]

Etwas anderes kann aber für Profiling-Maßnahmen oder Scores ohne (dauerhafte) Überwachung der Primärleistungspflicht gelten, beispielsweise, wenn unterjährige Mitarbeitergespräche stattfinden und Zielvereinbarungen getroffenen werden und die Daten aus diesen Maßnahmen in das HRM-System eingetragen werden oder lediglich (gezielte) stichprobenartige Kontrollen durchgeführt[1202] werden.

In einem solchen Fall kommt es im Rahmen der Datenerhebung zu keiner (technischen) Überwachung; Zielvereinbarungen und Mitarbeitergespräche sind allgemein üblich und werfen keine spezifisch datenschutzrechtlichen Fragen im Rahmen von People Analytics auf.

Datenschutzrechtliche Relevanz erlangen Zielvereinbarungen und Mitarbeitergespräche im Rahmen der hier untersuchten People Analytics dann, wenn die Daten aus solchen Gesprächen bzw. Beurteilungen genutzt werden sollen, um mit Hilfe intelligenter Algorithmen neue personenbezogene Daten wie beispielsweise einen Score zu generieren, die dann ins Verhältnis zu anderen (vergleichbaren) Arbeitnehmern gesetzt werden können. Anders als bei einem automatischen Scoring durch (technische) Überwachung der Primärleistungspflicht kommt es nicht zu einem vergleichbaren Überwachungs- und Anpassungsdruck, da Grundlage des Scores (für den Beschäftigten) nachvollziehbare Daten aus den genannten Maßnahmen sind. Dennoch kann die Bildung eines Scores (und somit

---

1199 Vgl. zu diesem Problem *Kraus*, DB 2018, 701; für eine Unzulässigkeit einer solchen Aussortiertung durch technische Überwachung *Däubler*, Gläserne Belegschaften, S. 190 Rn. 260a.

1200 Vgl. hierzu bereits die *Belastungsstatistik*-Entscheidung des BAG (Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205), dargestellt und analysiert unter **E. § 1 III. 2. a) cc) (4)**.

1201 BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205 (1211) Rn. 30; etwas anderes gilt, wenn nur bestimmte Daten aus dem Bereich der täglichen Arbeit in Auswertungen einfließen, vgl. BAG, Beschl. v. 30.08.1995 – 1 ABR 4/95, NZA 1996, 218.

1202 *Lunk*, NZA 2009, 457 (461) m.w.N.

Vergleichswertes) dazu führen, dass ein gewisser Druck entsteht, höchstmögliche Score-Zahlen zu erreichen. Der Leistungsdruck besteht allerdings schon aus der Zielvereinbarung selbst, da die dort vereinbarten bzw. vorgegebenen Ziele erreicht werden sollen / müssen. Der Unterschied ist, dass sich der Druck aus dem direkten Vergleich mit anderen Arbeitnehmern durch Generierung spezifischer Punktezahlen durch Scoring erhöhen kann.

Beispiel: Der Arbeitnehmer erreicht die vereinbarten Ziele voll, andere vergleichbare Arbeitnehmer überschreiten diese erheblich. Im Vergleich erreicht ein Arbeitnehmer daher nicht (mehr) 100 %, sondern lediglich 60 %. Zu beachten ist aber, dass in einem gut funktionierenden HR-Management solche Unterschiede auch ohne ein Scoring-Verfahren aufgedeckt und die Zielvereinbarungen entsprechend angepasst werden sollten, mit der Folge, dass eine höhere Leistung erwartet wird und der Leistungsdruck sich daher nicht aus dem Scoring, sondern der Zielvereinbarung selbst ergibt.

Selbst wenn aber durch technische Maßnahmen (Überwachungs-)Daten erhoben werden, beispielsweise in Fällen, in denen aus Gründen der Prozesssteuerung sehr detaillierte Daten erhoben werden müssen, kann es zulässig sein, diese für die konkrete Beurteilung von Mitarbeitern zu aggregieren.[1203] Dies bedeutet, dass der Arbeitgeber für die Leistungsbeurteilung keine konkreten Einblicke in die einzelnen Prozessschritte erhält, sondern beispielsweise am Monatsende eine vergleichende Darstellung der Leistung der einzelnen Mitarbeitern, aggregiert über einen Zeitverlauf. Somit ist es dem Arbeitgeber unmöglich, ein Bewegungsprofil des Arbeitnehmers zu erstellen und ihn konkret zu überwachen. Darstellbar ist ein Gesamtbild der Arbeitsleistung auf Monatsbasis, das mit anderen Arbeitnehmern in den Vergleich gestellt und hieraus entsprechende Scores generiert werden können.

Bei einer entsprechenden Transparenz des Scoring-Verfahrens überwiegen die Arbeitgeber-Interessen an einer Effektivierung des Personalmanagements dem Recht auf Privatheit und informationelle Selbstbestimmung des Beschäftigten, zumal die Eingriffsintensität bei der Verwendung transparenter und mathematisch-korrekter Verfahren im Vergleich zur Mitarbeiterbeurteilung ohne Scoring allenfalls geringfügig höher ist. Letztlich kommt es aber darauf an, wer Zugriff auf diese Daten erhält, um eine endgültige Bewertung der Zulässigkeit vorzunehmen (siehe **E. § 3**). Dem

1203 *Schürmann*, Auswertung von Mitarbeiterdaten - (Any)/(No)thing possible?, in: Taeger, Smart world - smart law?, S. 508.

Grunde nach ist ein Scoring der Primärleistungspflicht folglich möglich, wie auch der Wortlaut des Art. 4 Nr. 4 DSGVO nahe legt.

(c) Scoring des betrieblichen Verhaltens (z.B. Kommunikationsverhalten)

Als weitere denkbare Scoring-Situation ist im Rahmen von Advanced People Analytics die Bewertung von nicht leistungsrelevanten Daten denkbar. Als Beispiel kann die Auswertung des betriebliche Kommunikationsverhaltens zum Zwecke der „Selbstoptimierung" (Softwarebeispiel: IBM Social Dashboard[1204] oder Microsoft MyAnalytics[1205]) genannt werden. Ebenfalls gibt es inzwischen Tools (z.B. Office 365 Workplace Analytics[1206]), die die Daten auch auf Unternehmensebene darstellen. So kann dort eingesehen werden, wer wie lange an einem Dokument gearbeitet hat oder welche Kontakte mit welchen Betreffzeilen miteinander kommuniziert haben.[1207] Da hier nicht notwendigerweise Aussagen zum Primärleistungsverhalten getroffen werden und somit kein Leistungsdruck erzeugt wird, sind die Interessen der Parteien in solchen Fällen anders zu bewerten.

In diesem Zusammenhang ist zunächst die Frage aufzuwerfen, ob das Scoring nicht direkt leistungsrelevanter Daten (beispielsweise zum Zwecke der Selbstoptimierung) überhaupt von § 26 Abs. 1 BDSG erfasst werden kann, also die Datenverarbeitung als „erforderlich für die Durchführung des Arbeitsverhältnisses" ist. Andernfalls muss ggf. auf eine andere Legitimationsgrundlage wie Art. 6 Abs. 1 lit. f DSGVO oder eine Einwilligung zurückgegriffen werden.

1204 Eine mögliche Darstellungsform zeigt der Screenshot unter **C. § 4 V.**

1205 Siehe die Produktbeschreibung auf der Website: https://products.office.com/de-de/business/myanalytics-personal-analytics (letzter Abruf am: 28.02.2020).

1206 Vgl. die Beschreibung auf der Website: https://products.office.com/de-de/business/workplace-analytics (letzter Abruf am: 28.02.2020).

1207 *DGB*, Darum ist Microsoft Office 365 ein Fall für den Betriebsrat, 24.07.2017, abrufbar unter: https://www.dgb.de/themen/++co++0342f31e-6c85-11e7-b8f9-525400e5a74a (letzter Abruf am: 28.02.2020); ferner *Kraus*, DB 2018, 701 (703); zu beachten ist allerdings, dass Microsoft damit wirbt, dass sie die Vorgaben der DSGVO einhalten und personenbezogene Daten nur dem einzelnen Arbeitnehmer zur Verfügung stellen, während die Unternehmensansicht lediglich aggregierte, anonyme Daten sind, vgl. https://docs.microsoft.com/de-DE/workplace-analytics/myanalytics/overview/privacy-guide (letzter Abruf am: 28.02.2020).

§ 26 Abs. 1 BDSG erfordert, dass der Arbeitgeber die Daten zur Erfüllung seiner vertraglichen oder gesetzlichen Pflichten oder Wahrnehmung seiner Rechte benötigt, wobei auch die Erforderlichkeit der Daten zur Wahrnehmung berechtigter Interessen des Arbeitgebers davon umfasst sind.[1208] Unter diesem Aspekt ist es auf den ersten Blick zweifelhaft, die Datenerfassung und -verarbeitung bezüglich des betrieblichen Verhaltens unter § 26 Abs. 1 BDSG zu subsumieren. Es könnte aber eine Wahrnehmung berechtigter Interessen vorliegen, wenn die Auswertung des betrieblichen Verhaltens und die Selbstoptimierung zum Zwecke der Effizienzsteigerung der Arbeitskraft erfolgen. Arbeitgeber haben ein berechtigtes Interesse daran, das Unternehmen möglichst wirtschaftlich zu führen und Arbeitnehmer in höchstem Maße gewinnbringend einzusetzen.[1209]

Die Verarbeitung müsste hierfür nicht nur „erforderlich" sein, d.h. kein milderes, gleich effektives Mittel zur Erreichung des Zwecks geben, sondern die Maßnahme ist auch auf ihre Geeignetheit zu überprüfen. Geeignet ist eine Maßnahme dann, wenn sie tauglich ist, den gewünschten Zweck zu fördern. In der *Belastungsstatistik*-Entscheidung hatten sich die Erfurter Richter mit diesem Begriff in einem ähnlichen Kontext auseinanderzusetzen.[1210] Dort sahen die Richter erhebliche Zweifel bei einer Belastungsstatistik, die in der konkreten Ausgestaltung nicht die Belastungssituation einzelner Ebenen erfasste und rein quantitative Erhebungen traf, ohne auf die Komplexität der einzelnen zugewiesenen Aufgabe einzugehen.[1211]

Die gleiche Gefahr besteht bei der Auswertung des betrieblichen Verhaltens, insbesondere des Kommunikationsverhaltens, wenn die eingesetzten Algorithmen nicht die individuelle Position und Situation der Arbeitnehmer berücksichtigen, sondern schlichtweg einen Vergleich zur gesamten Abteilung oder Unternehmen darstellen. Dann verliert der Score aufgrund des Kontextverlusts seinen Aussagewert.

Beispiel: Ein Abteilungsleiter, der eine Führungsverantwortung für 40 Arbeitnehmer in der Abteilung hat, bekommt einen schlechten Score, da er einen hohen Zeitanteil seines Arbeitstages in Meetings und mit dem Verfassen und Beantworten von E-Mails verbringt, während die restlichen

---

1208 Zum Zweck „Erforderlichkeit für die Durchführung des Beschäftigungsverhältnisses", siehe **E. § 1 I. 1. b) bb)**.

1209 BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205 (1212) Rn. 36 zu einer "Belastungsstatistik".

1210 Zum Inhalt der Entscheidung, siehe bereits **E. § 1 III. 2. a) cc) (4)**.

1211 Vgl. BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205 (1210) Rn. 26.

40 Arbeitnehmer im Verhältnis nur wenige E-Mails schreiben, sich einmal wöchentlich zu einem kurzen „Jour-Fixe" treffen und den Rest der Arbeitszeit mit ihrer Kernarbeit verbringen.

Dieses Beispiel zeigt eigentlich eine sehr effektiv funktionierende Abteilung, bei der ein einzelner Abteilungsleiter sich um die Organisation der Arbeit kümmert und die anstehenden Arbeiten im „Jour-Fixe" verteilt, sodass die restlichen Arbeitnehmer der Abteilung effizient arbeiten können. Der niedrige Score beruht dann darauf, dass ihm ein ganz anderer Aufgabenbereich zugewiesen ist als Abteilungsleiter, der im Algorithmus nicht ausreichend Berücksichtigung gefunden hat.

Ohne Aussagewert sind solche Scores nicht geeignet, den gewünschten Zweck („*Effizienzsteigerung des Unternehmens und Gewinnmaximierung*") zu fördern, sondern sogar eher hinderlich. Der Abteilungsleiter im o.g. Beispiel könnte aufgrund des Scores nun Anreize bekommen, seine Organisationstätigkeit zurückzufahren, um eine bessere Bewertung zu erhalten. Dies führt dazu, dass die sehr effizient arbeitenden 40 Abteilungsmitarbeiter nunmehr mehr Organisatorisches erledigen müssen und die Effizienz sinkt, da weniger produktive Arbeit geleistet werden kann.

Der Einsatz solcher Software setzt also voraus, dass im Vorhinein ausreichend Analysearbeit geleistet wird, um „korrekte" Vergleichsgruppen für das Scoring bilden zu können. Selbst in solchen Fällen kann jedoch die individuelle Situation von Arbeitnehmern nur gering berücksichtigt werden, sodass solche Vergleichsscorings kaum Aussagewert besitzen. Etwas anderes kann dann gelten, wenn nicht verschiedene Arbeitnehmer verglichen werden, sondern das Verhalten einzelner Arbeitnehmer im Zeitverlauf isoliert gescort wird.

Beispiel: Max Mustermann stellt fest, dass er kaum noch Arbeitszeit für seine Kerntätigkeit (die Software-Programmierung) zur Verfügung hat. Er kann jedoch nicht konkret ausmachen, was die Gründe hierfür sind; er merkt lediglich, dass er viel mehr Zeit mit dem Verfassen von E-Mails verbringt. Hier könnte eine solche Software zunächst aufdecken, welchen Anteil der Arbeitszeit das Beantworten von E-Mails im Zeitverlauf in Anspruch genommen hat. Werden weitere Kommunikationsparameter ausgewertet,[1212] könnte Max feststellen, dass nur ein Bruchteil seiner E-Mails gelesen, beantwortet oder weitergeleitet werden, er mithin seine Arbeitszeit effektivieren könnte, wenn er auf das Verfassen von E-Mails weitgehend verzichtet.

1212 Vgl. Beispiele in *Höller/Wedde*, Die Vermessung der Belegschaft, S. 26 f.

Solche Scorings könnten mit Schwellenwert-Trigger versehen werden, die den Arbeitnehmer per E-Mail informieren, wenn bestimmte Grenzen überschritten wurden und ihm in weiterer Folge Handlungsempfehlungen zugeleitet werden. Da der einzelne Arbeitnehmer seine individuelle Situation kennt, ist die Gefahr „fehlerhafter" Scorings gering. Eventuell entstehende Abweichungen zu früheren Werten kann er nachvollziehen und dadurch informiert entscheiden, ob Handlungsbedarf vorhanden ist.

Für den Fall, dass die Analyseergebnisse jedoch nur für den Arbeitnehmer selbst angezeigt werden, ist die Frage nach der Geeignetheit der Maßnahme aufzuwerfen, wenn Dashboards Arbeitnehmern aufgezwungen werden können:

Hintergrund hierfür ist, dass ein Arbeitnehmer möglicherweise die E-Mails nicht liest oder auch das Dashboard als Startseite sofort schließt, wenn er kein Interesse an einer solchen Auswertung hat.

Es stellt sich auch ein weiteres Problem: Eine solche Verarbeitung ist nicht erforderlich, da es ein milderes Mittel für die daran interessierten Arbeitnehmer gibt, das gleich effektiv ist. Nämlich: Die Einholung von Einwilligungen bei Nutzung eines solchen Dienstes als originärer Ausfluss der Selbstbestimmung. Da niemand sonst Zugriff auf die Daten des Scorings hat, ist von einer Freiwilligkeit auszugehen, da lediglich Vorteile für den Arbeitnehmer entstehen (§ 26 Abs. 2 S. 2 BDSG).

§ 26 Abs. 1 S. 1 BDSG scheidet daher unter den genannten Umständen als Legitimationsgrundlage aus.

Im Ergebnis sind die Anwendungsfelder für betriebliches Verhaltensscoring auf Basis von § 26 Abs. 1 S. 1 BDSG sehr eingeschränkt; bei der Auswertung von Kommunikationsverläufen bzw. des Kommunikationsverhaltens ist zudem die Rechtsentwicklung im Bereich der Anwendbarkeit des TKG auf Arbeitgeber bei erlaubter Privatnutzung im Auge zu behalten; nach hier vertretener Auffassung spricht bei entsprechender technischer Implementation nichts dagegen, die Kommunikationsparameter betrieblicher Kommunikation im Rahmen von People Analytics auszuwerten.[1213]

Dennoch ist Scoring des betrieblichen Verhaltens ist datenschutzrechtlich nicht grundsätzlich ausgeschlossen. Sollen die personenbezogenen Daten eines Arbeitnehmers nicht nur für ihn selbst erhoben und ausgewertet werden, ist die Legitimationsgrundlage ist § 26 Abs. 1 S. 1 BDSG, wenn die Verarbeitung auch zur Durchführung seines Beschäftigungsverhältnisses dient. Auf Art. 6 Abs. 1 lit. f DSGVO hingegen muss zurückgegriffen

1213 Vgl. **D. § 3 I. 2. b) bb)**.

werden, wenn die Verarbeitung der personenbezogenen Daten des Arbeitnehmers keinen Bezug mehr zu seinem Beschäftigungsverhältnis aufweist.

Beispiel: Die personenbezogenen Daten von Arbeitnehmern eines besonders effizient arbeitenden Teams werden erhoben, um Probleme in vergleichbaren Teams zu erkennen. Aufgrund der verschiedenen Aufgabenzuweisungen innerhalb des Teams ist es erforderlich, dass die jeweilige Zuweisung bekannt ist, um die Daten sinnvoll miteinander zu vergleichen können. Obwohl keine Namen genutzt werden, ist eine Identifizierbarkeit anhand der Daten gegeben. Hier dient die Verarbeitung der personenbezogenen Daten des einen Teams nicht zur Durchführung der Beschäftigungsverhältnisse dieser Arbeitnehmer, sondern zur Optimierung anderer Teams, sodass die Datenverarbeitung nicht auf § 26 Abs. 1 S. 1 BDSG gestützt werden kann, sondern auf Art. 6 Abs. 1 lit. f DSGVO basieren muss. Der Abwägungsmaßstab ist aber inhaltlich derselbe, sodass sich hieraus keine Unterschiede ergeben.

(d) Scoring von Gesundheitsdaten

Letztlich stellt sich in diesem Zusammenhang noch die Frage, ob auch ein Scoring von Gesundheitsdaten als sensitive Daten im Sinne von Art. 9 DSGVO zulässig sein kann, wenn dies im Rahmen des betrieblichen Gesundheitsmanagements oder zur Gefahrenprävention stattfindet. Auch hier sollte kurz vorweg klargestellt werden, dass das Scoring an sich noch kein Fall des Art. 22 DSGVO darstellt und daher grundsätzlich Gesundheitsdaten als Grundlage dienen können; eine solche Verarbeitung nicht bereits aufgrund Art. 22 Abs. 4 DSGVO verboten.

Wie bereits im Rahmen der Bewertung von Simple People Analytics-Maßnahmen dargestellt (**E. § 1 III. 1. b) bb) (2)**), unterliegen solche Daten gem. § 26 Abs. 3 S. 1 BDSG einem erhöhten Schutz. So ist es nicht mehr ausreichend, wenn der Arbeitgeber ein berechtigtes Interesse an der Verarbeitung der Daten im Rahmen des Beschäftigungsverhältnisses hat, sondern vielmehr entscheidend, dass die Verarbeitung der Daten zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist.

Für die rechtliche Bewertung gilt, dass an dieser Stelle nicht die Erhebung und Verarbeitung der Daten selbst im Vordergrund steht, sondern ein darauf beruhendes Profiling / Scoring, d.h. beispielsweise die Erstellung eines Gesundheitsprofils oder Gesundheitsscores des Arbeitnehmers.

Von einer rechtmäßigen Erhebung der Gesundheitsdaten für Zwecke der People Analytics unter den bereits im Rahmen von SPA genannten Voraussetzungen wird daher im weiteren Verlauf ausgegangen.

Da die hier untersuchte Grundlage der Verarbeitung nicht etwa eine Betriebsvereinbarung oder Einwilligung ist, muss geprüft werden, ob die Bewertung der Gesundheit für die Erfüllung gesetzlicher Pflichten insbesondere aus dem Arbeitsrecht erforderlich ist.

Ist die Verarbeitung nicht für die Durchführung des Beschäftigungsverhältnisses erforderlich, so beispielsweise im Rahmen der Gesundheitsvorsoge, so sind andere Rechtsgrundlagen der Verarbeitung nicht ausgeschlossen. Letzteres könnte auf § 22 Abs. 1 Nr. 1 lit. b BDSG gestützt werden,[1214] wobei dort erforderlich ist, dass die Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden. Zur Gesundheitsvorsorge gehört insbesondere auch die Arbeitsmedizin im Sinne einer arbeitsmedizinischen Fürsorge.[1215] In diesem Fall schreibt das Gesetz explizit vor, dass der Datenbestand unter Verantwortung des Arbeitsmediziners verarbeitet wird, d.h. diese Daten dürfen zwar – sofern die weiteren Voraussetzungen vorliegen – für arbeitsmedizinische Zwecke unter Umständen einem Profiling oder Scoring unterzogen werden, nicht hingegen für beschäftigungspolitische Zwecke durch die HR-Abteilung. Beschäftigten kann somit u.U. eine Gesundheitsapp auf dem Smartphone zur Verfügung gestellt werden, dabei muss aber darauf geachtet werden, dass der Arbeitgeber auf den Datenbestand keinen Zugriff hat, um den Anforderungen des § 22 Abs. 1 Nr. 1 lit. b BDSG zu entsprechen.

Für Advanced People Analytics bleiben daher nur noch solche sensitiven Daten, die für die Erfüllung gesetzlicher Pflichten, insbesondere aus dem Arbeitsrecht erforderlich sind. Die Einschränkung aus dem Wortlaut des § 26 Abs. 3 S. 1 BDSG ist freilich zu beachten, aus dem sich ergibt, dass die Daten *ausschließlich* für die Erfüllung der gesetzlichen Pflicht verarbeitet werden dürfen. Weitergehende Analytics sind nicht statthaft. Die Wertung des Art. 9 Abs. 1 DSGVO, wonach grundsätzlich ein Verarbeitungsverbot für solche Daten gilt, ist bei der Bewertung zu berücksichtigen, sodass ein Scoring / Profiling zwingend erforderlich sein müsste, um die gesetzlichen Pflichten zu erfüllen; das gesetzlich festgelegte Regel-Ausnahmeverhältnis darf nicht ins Gegenteil umgekehrt werden.

1214 So ausdrücklich die Gesetzesbegründung zu § 26 BDSG, BT-Drs. 18/11325, S. 98.

1215 BT-Drs. 18/11325, S. 95.

Während für Simple People Analytics eine Fortschreibung bisheriger gesundheitsrelevanter Daten für prospektive Sicherheitsbewertungen noch erforderlich sein kann, ist dies beim Profiling / Scoring von Gesundheitsdaten grundsätzlich zu verneinen. Es sind keine Gründe ersichtlich, weshalb über die prospektive Betrachtung im Rahmen von SPA hinausgehend, ein Scoring zwingend erforderlich sein sollte. Etwas anderes gilt natürlich, wenn ein Gesetz (in der Zukunft) bestimmte Profiling-/Scoring-Maßnahmen vorschreiben sollte. Dann ist allerdings Rechtsgrundlage nicht mehr § 26 Abs. 1 S. 1 BDSG, sondern Art. 6 Abs. 1 lit. c DSGVO.

(e) Zwischenergebnis

Schon im Bewerbungsverfahren unterliegt das Bewerten von „weichen" Kriterien der Bewerber hohen Maßstäben an die Datenerhebung; die Grenzen des Fragerechts des Arbeitgebers sind (auch bei weitergehenden Scoring-Maßnahmen) einzuhalten. Sind die Daten zulässigerweise erhoben, so ist auch eine daran anknüpfende Bewertung in Form eines Profilings, Scorings oder Rankings, das die Persönlichkeitsrechte der Arbeitnehmer wahrt, in aller Regel vom Zweck der Erforderlichkeit für die Begründung des Beschäftigungsverhältnisses nach § 26 Abs. 1 S. 1 BDSG erfasst, wie sich aus den beispielshaften Fällen zeigt. Vorsicht ist geboten, wenn Daten von bereits im Unternehmen beschäftigten Arbeitnehmern als Vergleichsgrundlage herangezogen werden sollen; für diese Datenerhebung ist nicht § 26 BDSG einschlägig, sondern Art. 6 Abs. 1 lit. f DSGVO. Möglich ist auch eine Verarbeitung auf Basis einer Betriebsvereinbarung sowie – mangels nachteiliger Folgen für den Arbeitnehmer bei strenger Zweckbindung der Daten – die Einholung einer Einwilligung.

Nach Begründung des Beschäftigungsverhältnisses scheidet ein Scoring der Hauptleistungspflicht aus, wenn das Leistungsverhalten des Arbeitnehmers lückenlos überwacht und hierdurch ein Überwachungs- und Anpassungsdruck erzeugt wird. Etwas anderes gilt dann, wenn die Daten, die im Rahmen von Mitarbeitergesprächen oder Zielvereinbarungen getroffen wurden, in ein Personalmanagementsystem eingepflegt werden, welches eine Gesamtbewertung in Form eines Scores generiert. Letztere Verarbeitung ist von § 26 Abs. 1 S. 1 BDSG gedeckt, da der Arbeitgeber ein berechtigtes Interesse daran hat, einen schnellen Überblick über die Leistung seiner Arbeitnehmer zu bekommen und hiergegen kein wesentliches Interesse des Arbeitnehmers am Unterbleiben eines solchen Scorings spricht,

sofern die zugrunde gelegten Daten korrekt sind und rationale Verfahren eingesetzt werden.

Bei der Bewertung des betrieblichen Verhaltens muss ebenfalls darauf geachtet werden, dass kein „Gefühl des Überwachtwerdens" erzeugt wird. Einsatzbeispiel könnte eine Auswertung des innerbetrieblichen Kommunikationsverhaltens für Zwecke der Selbstoptimierung des Arbeitnehmers sein, um die Effizienz der Arbeit zu steigern. Eine solche müsste allerdings mangels Geeignetheit bei Zwang auf einer Einwilligung nach § 26 Abs. 2 BDSG basieren. Lediglich Auswertungen zur Optimierung von Teams oder Abteilungen auf personenbezogener Basis zur Unterstützung von Entscheidungen von Vorgesetzten können unter gewissen Voraussetzungen auf § 26 Abs. 1 S. 1 BDSG gestützt werden.

Ein Scoring von sensitiven Daten (wie beispielsweise Gesundheitsdaten) ist in aller Regel unzulässig. Etwas anderes kann gelten, wenn die Datenverarbeitung und das Scoring im Rahmen der Gesundheitsvorsorge durch den innerbetrieblichen ärztlichen Dienst erfolgt. In Sonderfällen kann auch eine Verarbeitung auf Grundlage einer Einwilligung zulässig sein, beispielsweise dann, wenn Gesundheitsdaten von Profisportlern zur Team- und individuellen Leistungsoptimierung genutzt werden sollen. Legitimationsgrundlage ist dann § 22 Abs. 1 Nr. 1 lit. b BDSG. Zu beachten ist, dass der Arbeitgeber keinen Zugriff auf diese Daten erhalten darf und somit ein Einsatz für People Analytics im Bereich von HR-Maßnahmen ausscheidet.

(3) Legitimation durch eine Betriebsvereinbarung

Um Rechtsunsicherheiten bei der Anwendung des § 26 Abs. 1 BDSG oder Einholung einer Einwilligung zu umgehen, kann in bestimmten Fällen auch eine Betriebsvereinbarung abgeschlossen werden, um die Datenverarbeitung zu legitimieren. Hierdurch kann auch eine Verarbeitung von sensitiven Daten erfolgen, wie sich aus der Rechtsgrundlage des nach § 26 Abs. 4 S. 1 BDSG ergibt.

Art. 88 DSGVO bzw. § 26 Abs. 4 S. 1 BDSG spezifizieren als Legitimationsgrundlage nicht nur die Betriebsvereinbarung, sondern auch die Gesamtbetriebsvereinbarung, Konzernbetriebsvereinbarung sowie die zwischen Arbeitgeber und Sprecherausschuss zustande gekommenen Spre-

cherausschussrichtlinien nach § 28 SprAuG[1216] sowie etwaige Dienstvereinbarungen im öffentlichen Dienst (§ 73 BPersVG).[1217] Nur schuldrechtlich zwischen dem Arbeitgeber und dem Betriebsrat wirkende Regelungsabreden hingegen fallen mangels normativem Charakter nicht unter den Begriff der „Kollektivvereinbarung" und stellen somit keine tauglichen Rechtsnormen dar.[1218]

Zu beachten ist, dass die Betriebsvereinbarung nur für den in § 5 BetrVG genannten Personenkreis eine normative Wirkung entfalten und somit Legitimationswirkung besitzen kann; entsprechend scheiden Betriebsvereinbarungen über Scoring in Bewerbungssituationen aus.[1219]

In inhaltlicher Hinsicht dürfen die Vereinbarungen die Datenverarbeitung im Beschäftigtenkontext spezifizieren im Sinne einer Spezialregelung, aufgrund von Art. 88 Abs. 2 DSGVO jedoch nicht grundlegend vom Schutzstandard abweichen.[1220] Auch § 75 Abs. 2 BetrVG schreibt einen sehr ähnlichen Prüfungsmaßstab vor.[1221] Den Betriebspartnern sind aber gewisse (Einschätzungs-)Spielräume bei der Beurteilung der Eingriffsintensität einer einzuräumen (siehe bereits **E. § 1 III. 1. c) aa)**).

Über ein Scoring der Arbeitsleistung kann nach der *Belastungsstatistik*-Entscheidung des BAG[1222] grundsätzlich eine Betriebsvereinbarung abgeschlossen werden, die Auswertungen durch Überwachung der Primärleistungspflicht regelt. Zu beachten ist allerdings, dass die eingesetzte Datenverarbeitung insbesondere geeignet sein muss, die Arbeitsleistung für die Zwecke der Auswertungen auch korrekt zu erfassen und es nicht zu einer dauerhaften Überwachung der Primärleistungspflicht kommt. Zudem muss sie transparent gestaltet sein, sodass Beschäftigte einerseits im Vorfeld durch eine entsprechende Information nach Art. 13 f. DSGVO über die Vorgänge der Verarbeitung aufgeklärt werden und andererseits

1216 Vgl. *Dzida/Grau*, DB 2018, 189 (191): Sprecherausschussvereinbarungen sind ebenfalls als Kollektivvereinbarungen im Sinne von Art. 88 Abs. 1 DSGVO sowie § 26 Abs. 4 BDSG anzusehen.

1217 *Seifert*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 88 DSGVO Rn. 27.

1218 Vgl. *Seifert*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 88 DSGVO Rn. 28.

1219 Siehe bereits im Detail **E. § 1 III. 1. c) bb)**; ferner *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 252.

1220 Vgl. **D. § 1 V. 2** sowie **E. § 1 III. 1. c) aa)**.

1221 A.A. wohl *Wybitul*, ZD 2016, 203: Die Anforderungen des Art. 88 Abs. 2 DSGVO gehen über die Beschränkungen nach § 75 Abs. 2 BetrVG hinaus (mit unklarem Nachweis).

1222 BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205.

Kenntnis darüber erhalten können, welche personenbezogene Daten für das Scoring herangezogen werden und welche Folgen dies haben kann.

Eine pauschale Aussage zur Zulässigkeit solcher Regelungen verbietet sich, da dies jeweils anhand des konkreten Systems, dem gewünschten Auswertungsziel und der daran anknüpfenden Maßnahmen im Einzelfall zu bewerten ist. In **Kapitel F** stellt diese Arbeit verschiedene Einsatzszenarien und Regelungsmöglichkeiten für eine rechtskonforme Regelung der Datenverarbeitung auf Basis einer Betriebsvereinbarung dar.

Beim Scoring des betrieblichen Verhaltens gelten dieselben Maßstäbe. Hier ist allerdings zu berücksichtigen, dass nur bedingt Rückschlüsse auf das Leistungsverhalten gezogen werden können, was grundsätzlich den entstehenden Druck für die betroffenen Arbeitnehmer verringert. Dennoch ist darauf zu achten, dass durch die Überwachung des Verhaltens keine Totalüberwachung statuiert wird. Eine solche wäre datenschutzrechtlich unzulässig, da sie die betroffenen Arbeitnehmer in rechtswidriger Weise in ihren Grundrechten beeinträchtigen würde.[1223] Die Erzeugung von Bewegungsprofilen mittels RFID- oder GPS-Technik kann auch per Betriebsvereinbarung aufgrund der extrem hohen Eingriffsintensität in die Rechte der Arbeitnehmer nur in sehr begrenztem Maße legitimiert werden: In keinem Fall dürfen heimliche Überwachungsmaßnahmen etabliert werden; solche sind allenfalls zur Aufdeckung von Straftaten nach § 26 Abs. 1 S. 2 BDSG zulässig.[1224] Unter dem Gesichtspunkt des Überwachungsdrucks scheiden permanente, anlasslose Überwachungsmaßnahmen aus, da diese zu tief in die Persönlichkeitsrechte der Betroffenen eingreifen würden und somit nach § 75 Abs. 2 BetrVG unzulässig wären.

Stichprobenartige, offene Überwachungsmaßnahmen können allerdings in Betriebsvereinbarungen als „erforderlich" erachtet werden, um eine grundsätzliche Leistungs- und Verhaltenskontrolle zu statuieren.

Da in den genannten Bereichen auch betriebsverfassungsrechtliche Mitspracherechte, insbesondere aus § 87 Abs. 1 Nr. 6 BetrVG, bestehen, kommt der Betriebsvereinbarung insofern eine Doppelfunktion zu.[1225]

1223 *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 108; vgl. BAG, Beschl. v. 29.06.2004 – 1 ABR 21/03, NZA 2004, 1278 (1283 f.) = BAGE 111, 173 = AP BetrVG § 87 1972 Überwachung Nr. 41 (m. Anm. Ehmann) zum Abwägungsmaßstab bei einer Videoüberachung im Betrieb.

1224 *Däubler/Wedde*, in: Däubler et al., EU-Datenschutz-Grundverordnung und BDSG-neu, § 26 BDSG Rn. 131.

1225 *Wurzberger*, ZD 2017, 258 (260).

Bei der Auswertung der betrieblichen Kommunikation auf Basis einer Betriebsvereinbarung ist zudem die Rechtsprechung zur Anwendbarkeit des TKG bei erlaubter Privatnutzung im Auge zu behalten; Betriebsvereinbarungen können anders als im Beschäftigtendatenschutz nicht legitimierend für Eingriffe in das Fernmeldegeheimnis durch Arbeitgeber wirken.

Zu beachten ist ferner, dass in Betriebsvereinbarungen ausschließlich Sonderregelungen für die Zwecke des Beschäftigungsverhältnisses getroffen werden dürfen.[1226] Im unter (**d**) genannten Beispiel der „Gesundheitsapp" durch die Arbeitsmedizin schiede dementsprechend eine Betriebsvereinbarung aus.

Etwas anderes könnte gelten, wenn bestimmte Gesundheitsdaten für Zwecke des Arbeitsschutzes gescort werden sollen. Hierfür kann die Betriebsvereinbarung grundsätzlich eine taugliche Legitimationsgrundlage, insbesondere im Hinblick auf die sensitiven Daten, nach § 26 Abs. 4 S. 1 BDSG darstellen. Ausweislich der Gesetzesbegründung beruht die Befugnis zur Regelung der Verarbeitung von sensitiven Daten in Kollektivvereinbarungen auf Art. 9 Abs. 2 lit. b DSGVO.[1227] Nach dieser Norm ist die Verarbeitung besonderer Kategorien von personenbezogenen Daten zulässig, wenn die Verarbeitung erforderlich ist, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht […] erwachsenen Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach […] einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten […] zulässig ist. Erforderlich ist, dass geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorgesehen werden. Nach deutschem Recht regelt dies § 22 Abs. 2 BDSG, der somit auch auf die Verarbeitung auf Grundlage einer Kollektivvereinbarung anwendbar ist.

Nach § 26 Abs. 3 BDSG fehlt für ein Scoring von Gesundheitsdaten für diese Zwecke bzw. im Rahmen von Advanced People Analytics eine gesetzliche Basis (siehe (**d**)). Den Betriebspartnern steht es in diesem Kontext aber grundsätzlich offen, eine erweiterte Regelung für die Verarbeitung von sensitiven Daten zu treffen, wenn sie in der konkreten Betriebs-/Unternehmenssituation den Pflichten zum Arbeitsschutz durch ein Scoring besser bzw. effektiver nachgekommen werden kann. Voraussetzung: Die Rechte der Betroffenen müssen hinreichend berücksichtigt und geschützt werden.

1226 *Wybitul*, ZD 2016, 203 (207).
1227 BT-Drs. 18/11325, S. 98.

Letztlich können durch eine Betriebsvereinbarung auch nach Erwägungsgrund 155 der DSGVO spezifische Möglichkeiten der Einwilligung von Arbeitnehmern in besonderen Verarbeitungssituationen geregelt werden, indem beispielsweise der Begriff der Freiwilligkeit konkreter geregelt wird. So könnte beispielsweise festgelegt werden, dass für die Einwilligung des Arbeitnehmers in bestimmten Verarbeitungssituationen eine Freiwilligkeit vermutet wird. Eine unwiderlegliche Vermutung der Freiwilligkeit wäre hingegen wohl nicht mit Art. 88 Abs. 2 DSGVO vereinbar, da es den Grundsatz aushebeln würde. Möglich sind ferner auch abweichende Regelungen zur Form der Einwilligung des Arbeitnehmers. Während das deutsche Recht in § 26 Abs. 2 S. 3 BDSG vorschreibt, dass die Einwilligung grundsätzlich schriftlich oder elektronisch[1228] zu erfolgen hat, können in einer Betriebsvereinbarung auch mündliche Einwilligungen für bestimmte Verarbeitungen entsprechend Art. 4 Nr. 11 DSGVO als ausreichend bestimmt werden oder strengere Voraussetzungen wie die Schriftform für besonders intensive Verarbeitungssituationen statuiert werden.

3. Zwischenergebnis

Simple People Analytics werfen datenschutzrechtlich kaum Probleme auf. Es ist davon auszugehen, dass diese als klassische Personalmanagement-Maßnahmen in aller Regel „erforderlich" im Sinne von § 26 Abs. 1 S. 1 BDSG sind, da die Arbeitgebergeberinteressen an einem effektiven Personaleinsatz sowie -planung überwiegen. Das Themenfeld um Advanced People Analytics hingegen, das derzeit umgangssprachlich schlicht als „People Analytics" bezeichnet wird und mit einer Bewertung persönlicher Merkmale (*Profiling*) einhergeht, ist deutlich komplexer zu beurteilen. Einerseits ist bereits die begriffliche Definition unscharf,[1229] sodass sich pauschale Aussagen zur Zulässigkeit oder Unzulässigkeit von People Analytics verbieten.[1230] Das Feld von People Analytics reicht von einfachen computergestützten Skill-Abgleichen im Rahmen des Bewerbungsprozesses bis hin zur Erstellung detaillierter Persönlichkeitsprofile der Arbeitnehmer durch lückenlose Überwachung mittels Log-Dateien, Wearables und Sen-

1228 Die grundsätzliche Zulässigkeit der elektronischen Form wurde mit dem zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU) eingefügt, vgl. BT-Drs. 19/11181, S. 19.

1229 Zu dieser Problematik bereits **C. § 1**.

1230 So aber BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 118.3.

soren.[1231] Während ersteres unter dem Gesichtspunkt der Erforderlichkeit für die Entscheidung über die Begründung des Beschäftigungsverhältnisses gerechtfertigt sein kann (**E. § 1 III. 2. c) dd) (2) (a)**), scheidet letzteres auf jeden Fall aufgrund des gravierenden Eingriffs in die Persönlichkeitsrechte der Arbeitnehmer aus (**E. § 1 III. 2. c) dd) (2) (b)** und (**c**)).

Dazwischen besteht eine rechtliche „Grauzone",[1232] die in der Rechtsprechung noch nicht ausgeurteilt und auch in der Literatur allenfalls oberflächlich behandelt wurde, obwohl die betriebswirtschaftliche Bedeutung im Rahmen der Arbeit 4.0 immer größer wird. Für die Bewertung der Fälle, die in diesem Zwischenfeld liegen, müssen die Systeme genau analysiert und festgestellt werden, welche Daten für welchen Zweck erhoben werden, wie hoch die Arbeitgeberinteressen an der Verarbeitung solcher Daten sind und welche Arbeitnehmerinteressen entgegenstehen könnten. In vielen Fällen zulässig ist ein Profiling oder Scoring von Beschäftigtendaten zum Zwecke der Analytics, sofern es sich nicht um sensitive Daten im Sinne von Art. 9 DSGVO handelt. Obwohl die spezifische Regelung zum Scoring nach § 31 BDSG unionsrechtswidrig ist, sind die darin enthaltenen Grundsätze bereits in der DSGVO selbst enthalten und bieten gute Anhaltspunkte für Arbeitgeber, welche Mindestanforderungen an eine Bewertung von Arbeitnehmern durch Algorithmen zu stellen sind, um diese rechtskonform umzusetzen.

Auch der Einsatz künstlicher Intelligenz im Rahmen von Scoring- und Profilingverfahren scheidet nicht per se aus, sofern die Verfahren eine gewisse Basisrationalität wahren und somit hinreichend transparent ausgestaltet werden (**E. § 1 III. 2. c) cc)**).

Das Instrument der Betriebsvereinbarung kann die Datenverarbeitung in diesem spezifischen Kontext weitgehend rechtssicher legitimieren, sofern die Betriebspartner die Grundsätze der DSGVO und die berechtigten Interessen der Arbeitnehmer wahren. In Betriebsvereinbarungen können im Weiteren die Anforderungen an Einwilligungen von Arbeitnehmern für konkrete Verarbeitungsvorgänge spezifiziert werden, um Rechtssicherheit zu schaffen.

Außerhalb dieses Kontextes ist das Institut der Einwilligung im Rahmen für *People Analytics* im Beschäftigungsumfeld nur bedingt zur Legitimation von Verarbeitungen geeignet und unterliegt hohen Rechtsunsicherheiten. Ein mögliches Beispiel stellt das Scoring zum Selbstzweck dar (**E. § 1 III. 2. c) dd) (2) (c)**).

1231 Vgl. *Dzida/Groh*, ArbRB 2018, 179 (180).
1232 Ähnlich *Dzida*, NZA 2017, 541 (543).

IV. Mitbestimmungsrechte des Betriebsrats

Da die Betriebsvereinbarung datenschutzrechtlich „das Mittel der Wahl ist“[1233] und nach § 26 Abs. 6 BDSG die Beteiligungsrechte der Interessensvertretungen durch das Datenschutzrecht unberührt bleiben, stehen dem Betriebsrat weitgehende Mitbestimmungsrechte zu. Dies gilt insbesondere dann, wenn technische Überwachungssysteme eingesetzt werden oder die Erkenntnisse aus den Analytics unmittelbar in die Entscheidung bei Personalmaßnahmen einfließen sollen. Im Folgenden werden die einschlägigen Mitbestimmungsrechte des Betriebsrats aufgezeigt. Die in der folgenden Darstellung werden die Mitbestimmungsrechte für Simple People Analytics und Advanced People Analytics getrennt dargestellt.

Gerade in Bereichen, in denen ohnehin zwingende Mitbestimmungsrechte des Betriebsrats bestehen, empfiehlt es sich in jedem Fall, beim Entwerfen einer Betriebsvereinbarung entsprechende Regelungen zur Legitimation der Datenverarbeitung zu treffen, um Rechtsunsicherheiten bei der Auslegung des unbestimmten Rechtsbegriffs der Erforderlichkeit weitgehend zu vermeiden.[1234]

1. Simple People Analytics

Nach hiesiger Definition der Simple People Analytics handelt es sich um Maßnahmen, die aus bereits bestehenden Daten Fortschreibungen generieren, um prospektiv Personalplanung und -steuerung betreiben zu können. In diesem Zusammenhang werden keine neuen Daten durch technische Maßnahmen aktiv erhoben.

Simple People Analytics werden meist durch Personalmanagement-Software durchgeführt. Beim Einsatz solcher Software werden in aller Regel die Zugriffe durch die Personalverantwortlichen registriert und gespeichert (z.B. zum Zwecke der Missbrauchskontrolle). Da § 87 Abs. 1 Nr. 6 BetrVG bereits ausgelöst wird, wenn die Maßnahme geeignet ist, die Leistung von Arbeitnehmern zu erfassen (hier der HR-Mitarbeiter, deren Zugriffe auf das System protokolliert werden), hat der Betriebsrat ein zwin-

1233 So wohl auch *Körner*, NZA 2019, 1389 (1390).

1234 So wohl auch *Wybitul*, NZA 2017, 1488 (1494); *Klösel/Mahnhold*, NZA 2017, 1428 (1433).

gendes Mitbestimmungsrecht beim Einsatz solcher Software, auch wenn hierdurch die bewerteten Arbeitnehmer nicht überwacht werden.[1235]

Sollen die hierdurch gewonnen Vorhersagedaten als Grundlage herangezogen werden, um Lohnfestlegungen für das kommende Jahr zu treffen, so besteht auch ein Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 10 BetrVG, wenn es sich um konkret leistungsbezogene Entgelte handelt, wäre Nr. 11 einschlägig. Allerdings werden leistungsbezogene Entgelte in aller Regel retrospektiv bezahlt und sind daher nicht im Kernbereich der Simple People Analytics angesiedelt.

Da bei SPA – im Unterschied zu APA – nur ein simpler Abgleich des Bewerberprofils mit der Stellenanforderung und inhaltlich keine Bewertung von Bewerbermerkmalen stattfindet, handelt es sich bei dem Abgleich noch nicht um eine Auswahlrichtline nach § 95 BetrVG; Bewerber die nicht den Anforderungen entsprechen, werden vorab „aussortiert" und kommen daher gar nicht erst für die Stelle in Betracht, auch wenn beispielsweise nur eine Person sich bewirbt. Eine Auswahl zwischen Bewerbern findet daher nicht statt, da diese Maßnahme der Auswahl vorgelagert ist.[1236]

Nach § 92 BetrVG muss der Arbeitgeber den Betriebsrat über die Personalplanung und den gegenwärtigen und künftigen Personalbedarf […] umfassend unterrichten und mit ihm darüber beraten. Für die Berechnung und Beratung dieser Gegenstände werden SPA-Maßnahmen eingesetzt. Ebenso wird der Tatbestand erfüllt, wenn SPA im Betrieb eingeführt werden sollen, da auch dies eine Maßnahme der Personalplanung ist, über die frühzeitig zu informieren ist.[1237]

Letztlich handelt es sich bei der Einführung von People Analytics um die Planung einer technischen Anlage i.S.v. § 90 Abs. 1 Nr. 2 BetrVG, wenn diese über neue Softwarekomponenten erfolgen soll.[1238] Hiernach ist vor Einführung der Betriebsrat rechtzeitig zu unterrichten und mit ihm darüber zu beraten.

Mitbestimmungsrechte statuieren §§ 90 und 92 BetrVG allerdings keine, sondern lediglich Informations- und Beratungsrechte.

1235 Vgl. hierzu **D. § 2 II. 1. b) bb)**.
1236 Siehe grundlegend **D. § 2 II. 2. b)**.
1237 Siehe auch **D. § 2 II. 4**.
1238 Siehe die Ausführungen zu § 90 BetrVG unter **D. § 2 II. 5.**

2. Advanced People Analytics

Bei Advanced People Analytics werden nicht nur bestehende Daten mit einfachen statistischen Methoden fortgeschrieben, sondern Ziel dieser ist es, mit einer Vielzahl von neu zu erhebenden oder zweckändernd verarbeiteten Daten aussagekräftige Kennzahlen für ein evidenzbasiertes Personalmanagement zu erzeugen. Es erfolgt also auch eine inhaltliche Bewertung der Daten durch Profiling- oder Scoring-Maßnahmen. Automatisierte Entscheidungen erfolgen in diesem Stadium noch nicht, es steht zunächst die Datenerhebung und insbesondere -verarbeitung im Vordergrund.

Auf der Erhebungsebene wurden in diesem Rahmen insbesondere IT-Nutzungs- und Sensordaten (etwa von Wearables) untersucht. Da diese Maßnahmen aktiv Beschäftigtendaten aufzeichnen, hat der Betriebsrat nicht nur ein Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG in Bezug auf die Einführung eines APA-Systems, sondern bereits bei der Erhebung solcher Daten beim Arbeitnehmer, d.h. bei der Einführung von Wearables oder IT-Systemen, die eine solche Auswertung ermöglichen. Dies ist der Kernmitbestimmungstatbestand für Advanced People Analytics, da genau dieser dazu dient, die Persönlichkeitsrechte von Arbeitnehmern (die durch solche Maßnahmen besonders tangiert werden) zu schützen.[1239]

Schreibt der Arbeitgeber den Arbeitnehmern vor, „smart clothes" in besonders gefährlichen Bereichen zu tragen, um hierdurch die Arbeitssicherheit zu erhöhen, oder bestimmte Software zur Kommunikation mit Teamkollegen zu nutzen, handelt es sich um eine Regelung, die nicht das mitbestimmungsfreie Arbeitsverhalten selbst betrifft, sondern das Ordnungsverhalten im Betrieb, welches nach § 87 Abs. 1 Nr. 1 BetrVG der Mitbestimmung unterliegt.[1240] Weiterhin sind auch etwaige „Gesundheitswettbewerbe" z.B. durch die Ausgabe von Fitness-Trackern im Betrieb davon erfasst, wenn Arbeitgeber dadurch erreichen möchten, dass sich Arbeitnehmer im Betrieb aktiver verhalten, z.B. öfters vom PC-Arbeitsplatz aufstehen und ein paar Schritte gehen.[1241] Auch hierdurch bezweckt der Arbeitgeber, das Verhalten der Arbeitnehmer in Bezug auf die betriebliche Ordnung zu beeinflussen.[1242]

1239 Vgl. **D. § 2 II. 1. b**).

1240 BAG, Beschl. v. 17.01.2012 – 1 ABR 45/10, NZA 2012, 687 (689) Rn. 23 zur Anordnung einer Dienstkleidungspflicht.

1241 Vgl. BAG, Beschl. v. 24.03.1981 – 1 ABR 32/78, NJW 1982, 404 = AP BetrVG 1972 § 87 Arbeitssicherheit Nr. 2 zu einem „Sicherheitswettbewerb" im Betrieb.

1242 Siehe hierzu grundlegend **D. § 2 II. 1. a**).

Erst recht werden wie bei Simple People Analytics auch die Mitbestimmungstatbestände der § 87 Abs. 1 Nr. 10 und 11 BetrVG ausgelöst, wenn die Daten genutzt werden sollen, die Entlohnung der Arbeitnehmer zu bestimmen oder leistungsbezogene Entgelte, die auf Scores basieren, festzulegen. Das Mitstimmungsrecht erstreckt sich auf die Bezugsgrößen einschließlich des Geldfaktors.[1243]

Werden im laufenden Arbeitsverhältnis oder im Bewerbungsprozess standardisierte Fragebögen eingesetzt (auch in digitaler Form von Eingabemasken), so muss der Betriebsrat nach § 94 BetrVG der Einführung zustimmen. Dieses Mitbestimmungsrecht besteht auch hinsichtlich des Inhalts der Fragebögen sowie die Umstände der Verwendung (somit auch Zweckbestimmung und Rahmenbedingungen der Datenverarbeitung). Solch standardisierte Formulare sind beispielsweise notwendig, um ein Bewerberscoring durchzuführen, damit die erhobenen Daten vergleichbar sind und etwaigen Fehlern beim CV-Parsing[1244] oder automatisierten Auswerten sonstiger eingereichter Unterlagen (z.B. mittels OCR-Scans) vorzubeugen.

§ 94 BetrVG greift auch ein, wenn das Verhalten oder die Leistung von Arbeitnehmern mit Hilfe von Scoring oder Profiling bewertet werden soll, da hierfür eine Bewertungsmatrix erforderlich ist (so auch beim Bewerberscoring, sodass hier das Mitbestimmungsrecht „doppelt" greift).

Beispiel: Der Arbeitgeber möchte ein System implementieren, welches die Arbeitnehmer im Betrieb in verschiedene Leistungskategorien klassifiziert. Für die verschiedenen Tätigkeiten werden einzelne Bewertungsmatrizen erstellt, die ein Scoring der Arbeitnehmer in den jeweiligen Tätigkeiten in Bezug zu den Anforderungen ermöglichen. Jeder Arbeitnehmer erhält einen Score. Durch die Erstellung des Scores lassen sich die Arbeitnehmer bei vergleichbaren Anforderungen in den Bewertungsmatrizen auch tätigkeitsübergreifend miteinander vergleichen und somit eine „Performer-Liste" für den gesamten Betrieb etablieren (z.B. zur Darstellung in Dashboards, hierzu **E. § 3 II**).

Weitgehende Informations- und Beratungspflichten statuiert § 92 BetrVG, die bereits in der Planungsphase eines Analytics-Systems ansetzen, sofern die hierdurch gewonnen Daten als Grundlage für Personalentscheidungen dienen sollen.

1243 ErfK/*Kania*, § 87 BetrVG Rn. 117.

1244 Parsing ist ein Vorgang, bei welchem mit Hilfe eines Computeralgorithmus Daten aus einem nicht für die elektronische Verarbeitung optimierten Dokuments gezogen werden.

Letztlich könnte die Einführung von Advanced People Analytics auch eine Betriebsänderung nach § 111 S. 3 Nr. 5 BetrVG darstellen, insbesondere wenn ein Unternehmen gleichzeitig von „klassischem" Personalmanagement auf evidenzbasiertes Management umstellt. Insbesondere bei einem Unternehmen ohne eine technisierte Personalabteilung kann es zu weitgehenden Änderungen durch Einführung grundlegend neuer Arbeitsmethoden kommen. Dies ist jedoch im Einzelfall zu prüfen.[1245] Jedenfalls aber stellt es die Planung einer technischen Anlage nach § 90 Abs. 1 Nr. 2 BetrVG dar.

V. Zusammenfassung

Die Anwendungsfelder für People Analytics in Betrieben und Unternehmen sind mannigfaltig. Unterschieden werden muss zwischen simplen und fortgeschrittenen People Analytics.

Bei den simplen Analytics werden lediglich vorhandene Daten durch einfache mathematische und statistische Verfahren fortgeschrieben. Solche werden bereits seit Jahren in vorhandenen Personalmanagementsystemen eingesetzt, um beispielsweise Fluktuationsquoten und sonstige Veränderungen im Personal mit Hilfe einer retrospektiven Betrachtung fortzuschreiben und Anhaltspunkte für zukünftige Veränderungen zu geben.

Solche Maßnahmen sind datenschutzrechtlich als relativ unkritisch einzustufen, da lediglich bereits rechtmäßig für die Zwecke der Durchführung des Beschäftigungsverhältnisses erhobene Daten (§ 26 Abs. 1 S. 1 Var. 2 BDSG) genutzt werden und keine *grundlegend* neuen personenbezogenen Daten generiert werden. Insbesondere findet hier keine inhaltliche Bewertung einzelner Personen statt, die mit tieferen Eingriffen in die Rechte der Arbeitnehmer verbunden ist. Oftmals lassen sich solche Analysen auch anonym durchführen, sodass der Datenschutz nur marginal (für den Anonymisierungsvorgang) berührt ist. Ist eine Anonymisierung tunlich, dass muss eine solche als milderes, gleich effektives Mittel auch vorgenommen werden.

Dennoch hat der Betriebsrat– allein aufgrund der Nutzung von Software – Mitbestimmungsrechte, die dazu führen, dass eine Betriebsvereinbarung abgeschlossen werden sollte, um diese Verfahren inhaltlich rechtsicher zu regeln. Eine solche kann nach Art. 88 DSGVO, § 26 Abs. 4 BDSG auch Datenverarbeitungen im Beschäftigtenkontext legitimieren, sodass

1245 Hierzu **D. § 2 II. 6. b**).

auch auf datenschutzrechtlicher Ebene Rechtssicherheit geschaffen werden kann.

Deutlich spannender und absolut im Trend sind fortgeschrittene (Advanced) People Analytics, die nicht nur bereits vorhandene Daten fortschreiben, sondern einerseits durch die Erhebung weiterer „Live-Daten" aus digitalen Systemen Echtzeitauswertungen ermöglichen und andererseits inhaltliche Bewertungen vornehmen. Hierfür kommen Profiling- und Scoring-Techniken zum Einsatz, die in vielen Fällen auch mit künstlicher Intelligenz kombiniert werden.

Solche Techniken sind unter datenschutzrechtlichen Gesichtspunkten weitaus kritischer zu betrachten, da sie eingriffsintensiver sind. Dennoch sind diese neuen Verfahren, sofern sie datenschutzkonform ausgestaltet werden und die Rechte der betroffenen Arbeitnehmer wahren, durchaus zulässig. Als Legitimationsgrundlage dient in der Regel § 26 Abs. 1 S. 1 BDSG, sofern die Durchführung des konkreten Beschäftigungsverhältnisses im Mittelpunkt steht. Sollen Daten von Arbeitnehmern für andere betriebliche Zwecke genutzt werden, muss auf Art. 6 Abs. 1 lit. f DSGVO zurückgegriffen werden.

In Fällen, in denen Arbeitnehmer keine Nachteile zu befürchten haben, kann auch auf eine Einwilligung nach § 26 Abs. 2 BDSG zurückgegriffen werden, da eine Freiwilligkeit dann vermutet wird. Dieser Anwendungsbereich beschränkt sich aber auf eng begrenzte Ausnahmefälle und birgt das Risiko in sich, dass der Arbeitnehmer von seinem Recht, die Einwilligung jederzeit zu widerrufen (Art. 7 Abs. 3 S. 1 DSGVO), Gebrauch macht.

Aus diesem Grund ist in der überwiegenden Anzahl der Fälle die Betriebsvereinbarung das vorzugswürdige Mittel. Diese kann nicht nur aufgrund der bestehenden Unterkomplexität der Datenschutzgrundverordnung und des BDSG zum Beschäftigtendatenschutz Rechtssicherheit schaffen, sondern auch aufgrund der in der Regel bestehenden Mitspracherechte des Betriebsrates eine einfache Möglichkeit der Regelung dieses Themenbereiches gewähren. Verhandelt werden muss mit dem Betriebsrat über den Einsatz solcher Technologien und die Reichweite von Auswertungen (insbesondere aufgrund § 87 Abs. 1 Nr. 6 BetrVG) ohnehin. Wird eine Einigung erzielt, lassen sich hierdurch auch die Datenverarbeitung legitimieren und differenzierte Regelungen schaffen, die das Datenschutzniveau auf Betriebsebene sogar steigern, da die besondere Unternehmens- und Betriebssituation berücksichtigt wird.

Eine Ausnahme stellen Bewerbungssituationen dar, da der Betriebsrat nur für Arbeitnehmer (§ 5 BetrVG) zuständig ist; in diesem Bereich müssen zwar mitunter Betriebsvereinbarungen über Auswahlrichtlinien

geschlossen werden, datenschutzrechtlich legitimierend wirken sie mangels normativer Wirkung für diesen Personenkreis nicht. Arbeitgeber sind daher gehalten, die Anforderungen des § 26 Abs. 1 S. 1 Var. 1 BDSG genau einzuhalten.

§ 2 *Automatisierte Entscheidungen auf Basis von People Analytics*

Ziel von People Analytics ist nicht nur, weitgehende Informationen über die Personalstruktur und Arbeitnehmer zu erhalten, sondern auch Betriebsabläufe im Personalmanagement zu effektivieren. Hierzu kann auch zählen, dass bestimmte (standardisierte) oder besonders arbeitsintensive Aufgaben nicht mehr durch Menschen, sondern vollständig automatisiert durch ein modernes Personalmanagementsystem erledigt werden. Bereits jetzt gibt es Software auf dem Markt, die je nach Kategorisierung der Mitarbeiter bestimmte Logiken auslöst. So beispielsweise eine automatisierte Gehaltserhöhung zum Jahresende bei „High Performern", um diese an das Unternehmen zu binden.[1246] Auch im Bereich des Bewerbermanagements werden zuweilen (insbesondere im angloamerikanischen Raum) Software-Lösungen vorgeschlagen, die eine automatische Vor- bzw. sogar Endauswahl[1247] der Bewerber vornehmen, ohne dass ein menschlicher Entscheider zwischengeschaltet wird.

Im Anwendungsbereich der Datenschutzgrundverordnung sind automatisierte Einzelfallentscheidungen, die gegenüber den Betroffenen eine rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen, grundsätzlich verboten (Art. 22 Abs. 1 DSGVO).[1248]

Zu prüfen ist im Folgenden, welche Maßnahmen im Rahmen von People Analytics von diesem Verbot erfasst sind und in welchen Situationen sich Arbeitgeber auf die in Art. 22 Abs. 2 DSGVO normierten Ausnahmetatbestände berufen können.

I. Bewerbermanagement

Das Bewerbermanagement dürfte der wichtigste Anwendungsbereich automatisierter Einzelfallentscheidungen sein, insbesondere wenn aufgrund

1246 *Sommer*, CuA 2017, 8 (10).
1247 Vgl. *Peck*, The Atlantic 2013 (Dezember 2013).
1248 Die Grundlagen wurden bereits im Abschnitt **D. § 1 V. 3** erläutert.

hoher Bewerberflut es für menschliche Entscheider faktisch unmöglich ist, alle Bewerbungen zu sichten und somit eine gerechte Auswahl vorzunehmen. So erhalten Großunternehmen mit mind. 500 Mitarbeiter im Schnitt 2.000 Bewerbungen pro Jahr, bei Unternehmen mit einer Mitarbeiteranzahl von 100 bis 499 sind es 374, während es bei klein- und mittelständischen Unternehmen mit 50-99 Arbeitnehmern 182 sind. Die Personalabteilung besteht dabei im Schnitt aus 13 Mitarbeitern bei Großunternehmen, 3 bei Unternehmen mit bis zu 499 Mitarbeitern und 1,9 bei Unternehmen mit 50 – 99 Angestellten.[1249] Hierbei ist zu bedenken, dass die HR-Verantwortlichen auch laufende Aufgaben wie Personalmanagement, -entwicklung und -abrechnung vorzunehmen haben. Bei beliebten Arbeitgebern wie Audi oder Google sehen die Zahlen noch deutlich drastischer aus: Bei Audi in Ingolstadt geht im Schnitt alle 52 Sekunden eine neue Bewerbung ein, das sind mehr als 100.000 pro Jahr; bei Google sind es 75.000 pro *Woche* (!).[1250] Automatisierte Lösungen zum Bewerbermanagement sind für solche Unternehmen unumgänglich.

Für den Einsatz der zur Bewältigung erforderlichen Software sind mehrere Szenarien für automatisierte Entscheidungen denkbar: Das Aussortieren von bereits formal ungeeigneten Kandidaten, ein Ranking aller eingehenden Bewerbungen und eine Bestenauslese[1251] sowie ein vollständig automatisiertes Einstellungsmanagement, völlig ohne menschliche Interaktion, wobei letzteres in Deutschland nicht nur aus datenschutzrechtlichen Gründen zum aktuellen Zeitpunkt noch reine Science-Fiction darstellen dürfte.[1252] Die anderen beiden untersuchten Szenarien werden aber teilweise schon in der Praxis angewandt und sind in vielen größeren Softwarelösungen bereits implementiert.[1253]

1249 So eine gemeinsame Studie von *Bitkom Research GmbH/Personio GmbH*, Woran scheitern Einstellungen?

1250 *Kontio*, Wie Bewerber die Robo-Recruiter überlisten können, 04.09.2018, abrufbar unter: https://www.handelsblatt.com/unternehmen/beruf-und-buero/the_shift/jobsuche-wie-bewerber-die-robo-recruiter-ueberlisten-koennen/22991974.html?ticket=ST-3589804-FXMKTFgbNgF1zeM14jmT-ap2 (letzter Abruf am: 06.03.2020).

1251 Hierzu grundlegend *Blum/Kainer*, PERSONALquarterly 2019, 22 sowie noch zum altem Datenschutzrecht *Groß/Gressel*, NZA 2016, 990 (992 f.).

1252 So aber bereits teilweise in den USA angewandt, vgl. *Peck*, The Atlantic 2013 (Dezember 2013).

1253 Siehe hierzu beispielsweise *Kontio*, Wie Bewerber die Robo-Recruiter überlisten können, 04.09.2018, abrufbar unter: https://www.handelsblatt.com/unternehmen/beruf-und-buero/the_shift/jobsuche-wie-bewerber-die-robo-recruiter-ueberlisten-koennen/22991974.html?ticket=ST-3589804-FXMKTFgbNgF1

1. Vorauswahl und automatische Absage an ungeeignete Bewerber

Wenn man bedenkt, dass bei 97 % der Fälle die Bewerber noch nicht einmal die Kriterien der Stellenanzeigen erfüllen und mit gleicher Quote zu hohe Gehaltsvorstellungen angegeben werden,[1254] lässt sich durch eine automatische Vorauswahl solch formal ungeeigneter Bewerber bereits eine Vielzahl der Kandidaten aussortieren. Hierdurch könnten sich die Verantwortlichen im Unternehmen mehr Zeit für die in Frage kommenden Bewerber nehmen und folglich eine bessere Auswahl treffen.

Aus datenschutzrechtlicher sowie nachgelagert betriebsverfassungsrechtlicher Sicht ist die Frage aufzuwerfen, ob ein solches Vorselektionssystem in der Praxis umsetzbar ist. Für die rechtliche Bewertung steht insbesondere das Verbot automatisierter Einzelfallentscheidungen aus Art. 22 DSGVO im Fokus, während nachgelagert eventuelle Mitspracherechte des Betriebsrats nach § 99 BetrVG voll automatisierten Absagevorgängen entgegenstehen könnten.

a) Datenschutzrechtlicher Rahmen

Für eine Anwendbarkeit des Art. 22 DSGVO bedarf es einer vollautomatischen Entscheidung durch das Bewerbermanagementsystem. Nicht vom Verbot erfasst ist es, wenn der Algorithmus lediglich Vorschläge für eine letztlich vom Menschen zu treffende Entscheidung erstellt, indem beispielsweise alle Bewerber nach der Passgenauigkeit auf das Stellenprofil sortiert werden, letztlich aber ein Mensch die Entscheidung „Absage" nach inhaltlicher Prüfung trifft. Voraussetzung ist allerdings, dass der menschliche Entscheider nicht nur den Vorschlag des Computers übernimmt und sich (wie sich aus dem Einschub „einschließlich Profiling" ergibt) auf die Bewertung des Systems verlässt, sondern selbst unter Berücksichtigung der Datengrundlage, d.h. den vom Bewerber eingereichten Daten, eine wertende Entscheidung vornimmt.[1255] Nur dann kann das Schutzziel des Art. 22 DSGVO erreicht werden, keine vom Computer inhaltlich verant-

---

zeM14jmT-ap2 (letzter Abruf am: 06.03.2020); ein Softwarebeispiel stellt die Bewerbermanagement-Software von *Persis* dar, vgl. https://www.persis.de/bewerbermanagement/ (letzter Abruf am: 06.03.2020); ähnliche Funktionen dürfte Prescreen anbieten, vgl. https://prescreen.io/de/bewerberverwaltung/ (letzter Abruf am: 06.03.2020).

1254 *Bitkom Research GmbH/Personio GmbH*, Woran scheitern Einstellungen?, S. 8.

1255 Siehe bereits **D. § 1 V. 3. c) aa)**.

worteten Entscheidungen zuzulassen, bei denen der Mensch zum Objekt der Datenverarbeitung wird, sofern sich Verarbeiter nicht auf einen Ausnahmetatbestand stützen können.[1256]

Obwohl die Ablehnung eines Arbeitsvertragsschlusses noch keine rechtliche Wirkung im Sinne des Art. 22 Abs. 1 DSGVO erzeugt, stellt dies bei objektiver Betrachtung eine erhebliche Beeinträchtigung für den Bewerber dar,[1257] sodass derartige Anwendungen vom Verbot des Art. 22 Abs. 1 DSGVO erfasst sind und im Folgenden zu prüfen ist, ob ein Ausnahmetatbestand des Abs. 2 einschlägig ist.

Während die Einwilligung in eine automatisierte Entscheidung im Bewerbungsprozess aus denselben Gründen ausscheidet wie eine „normale" Datenverarbeitung auf dieser Basis[1258] und ebenso wenig eine Erlaubnisnorm nach Art. 22 Abs. 2 lit. b DSGVO besteht, kommt es darauf an, ob die automatisierte Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist. Obwohl von der Erforderlichkeit für den „Abschluss des Vertrages" gesprochen wird, können auch ablehnende Entscheidungen von Art. 22 Abs. 2 lit. a DSGVO gerechtfertigt werden.[1259]

Inwieweit eine automatisierte Entscheidung im Rahmen der Bewerbervorauswahl erforderlich ist, hängt davon ab, bis zu welchem Maße dem Arbeitgeber eine Sichtung der Bewerbungsunterlagen durch menschliche Entscheider zumutbar ist.[1260] Sicherlich ist es im genannten Bespiel von Audi unzumutbar, dass die Personalverantwortlichen jede Minute eine Bewerbung sichten und hierüber entscheiden; umso mehr gilt dies für Google. Auch bei Großunternehmen mit im Schnitt 2.000 Bewerbungen handelt es sich immer noch (bei im Schnitt 230 Arbeitstagen pro Jahr) um knapp 8,7 Bewerbungen, die täglich (von 13 Personalverantwortlichen) zu bearbeiten wären. Auch in solchen Fällen ist die Zumutbarkeitsgrenze

1256 *Klar*, BB 2019, 2243 (2249).

1257 Wie hier *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 22 DSGVO Rn. 36.

1258 Zum Kriterium der Freiwilligkeit: **D. § 1 III. 2. a) bb) (2)**; vgl. aber *Götz*, Big Data im Personalmanagement, S. 177 zu einer "optionalen Teilnahme an automatisierten Bewertungssystemen. *Götz* übergeht leider das Problem, dass Bewerber dennoch unfreiwillig an der Maßnahme teilnehmen werden, da sie Benachteiligungen befürchten, wenn sie die Option nicht auswählen.

1259 *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 22 DSGVO Rn. 29; *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 22 DSGVO Rn. 40.

1260 Zum Begriff der Erforderlichkeit im Detail: **D. § 1 V. 3. d) aa)**.

überschritten, wenn man bedenkt, dass die Personalakquise nur ein Bruchteil der Personalarbeit im Unternehmen darstellt. Selbst die Bearbeitung von 1,6 Bewerbungen (bei drei Personalverantwortlichen) bei mittleren Unternehmen oder 0,8 Bewerbungen (bei 1,9 Personalverantwortlichen) bei kleinen Unternehmen pro Tag dürfte die Zumutbarkeitsgrenze sprengen. Dies wäre im Schnitt über alle Unternehmensgrößen alle zwei Tage eine Bewerbung, die pro HR-Mitarbeiter zu bearbeiten ist, wobei nicht berücksichtigt wird, dass diese Zahlen nur Mittelwerte darstellen, nicht alle Abteilungsmitarbeiter auch für das Bewerbermanagement zuständig sind und bei (neuen) Stellenausschreibungen deutliche Spitzen auftreten, während z.B. bei Initiativbewerbungen im Gegensatz in aller Regel nur die einzelne Bewerbung geprüft werden muss.

Im Allgemeinen ist daher eine Bewerbervorauswahl als erforderliche Maßnahme für den Abschluss eines Arbeitsvertrags vom Verbot der automatisierten Entscheidung nach Art. 22 Abs. 2 lit. a DSGVO ausgenommen. Dies gilt nach den bisherigen Ausführungen allerdings nur soweit als die Datenauswertung und -entscheidung im Einzelfall durch einen menschlichen Entscheider für den Arbeitgeber unzumutbar ist. Ist nur eine Stelle ausgeschrieben und bewerben sich hierfür zwischen 10 und 15 Bewerber bei einem Personalverantwortlichen in einem kleineren Unternehmen, so steht die Bearbeitung dieser Bewerbungen kurzfristig im Vordergrund – eine automatisierte Vorauswahl ist nicht erforderlich. Letztendlich hängt es vom Einzelfall ab, ob computergestützte Vorauswahlen geboten sind oder nicht.

Um den Anforderungen des Verhältnismäßigkeitsgrundsatzes nachzukommen, muss die Anwendung des Systems gestuft erfolgen, d.h. datenschutzrechtlich weniger einschneidende Maßnahmen müssen vorrangig angewandt werden, während eine Entscheidung mittels Profiling als eine ins Persönlichkeitsrecht intensiver eingreifende Maßnahme erst in einem zweiten Schritt erfolgen darf.

Zunächst muss daher bei einer angenommenen Bewerberflut eine automatische Vorselektion anhand rein formaler Kriterien erfolgen. Erst wenn hiernach weiterhin eine derart große Anzahl an Stellenbewerbern übrigbleibt, dass auch diese nicht durch menschliche Entscheider bewältigbar ist, kommt eine weitere Selektion mittels Profiling- oder Scoring-Maßnahmen in Betracht.

Der Arbeitgeber muss im Rahmen dessen die betroffenen Bewerber genau über das Vorliegen und die Reichweite einer automatisierte Entscheidungsfindung sowie über die involvierte Logik und angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person, informie-

ren (Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g DSGVO). Ein Auskunftsrecht mit demselben Inhalt besteht aus Art. 15 Abs. 1 lit. h DSGVO.

Nach Art. 22 Abs. 3 DSGVO hat die betroffene Person zudem das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts sowie auf Anfechtung der Entscheidung.

Zwar schreibt Art. 35 DSGVO für den Fall der Aussortierung bei mangelnder formaler Qualifikation nicht explizit eine Datenschutzfolgenabschätzung vor, da hierfür ein Profiling erforderlich wäre (vgl. insofern auch Erwägungsgrund 91 S. 2: „*Eine Datenschutz-Folgenabschätzung sollte auch durchgeführt werden, wenn die personenbezogenen Daten für das Treffen von Entscheidungen auf bestimmte natürliche Personen im Anschluss an eine systematische und eingehende Bewertung persönlicher Aspekte natürlicher Personen auf der Grundlage eines Profilings dieser Daten oder im Anschluss an die Verarbeitung besonderer Kategorien von personenbezogenen Daten […] [erfolgt].*“).

Dennoch ist davon auszugehen – auch wenn nicht vom Regelbeispiel des Art. 35 Abs. 3 lit. a DSGVO erfasst[1261] –, dass Art. 35 Abs. 1 DSGVO einschlägig ist. Hiernach ist eine Datenschutz-Folgenabschätzung erforderlich, wenn diese Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat:

Bei der Bewerbung für ein Arbeitsverhältnis steht in aller Regel die Haupteinnahmequelle des Bewerbers im Vordergrund (Umstände sowie hohes Risiko) und bei solchen Systemen handelt es sich um neuartige Technologien im Personalbereich, die erst durch die zunehmende Verarbeitungsgeschwindigkeit ermöglicht wurden (Verwendung neuer Technologien). Fehler, die zu einer Nicht-Berücksichtigung führen, können gravierende Folgen für den einzelnen Betroffenen haben, wodurch ein hohes Risiko besteht. Es ist daher geboten, die möglichen Folgen und Risiken des Einsatzes eines solchen Systems exakt zu eruieren und insbesondere die Fehleranfälligkeit (z.B. beim Parsen von CVs oder sonstigen Unterlagen) zu bewerten, bevor dieses zum Einsatz kommt.

1261 Siehe bereits **D. § 1 V. 4.**

b) Betriebsverfassungsrechtlicher Kontext

Aus betriebsverfassungsrechtlicher Hinsicht stellt sich die Frage der Umsetzbarkeit aufgrund der Mitbestimmungsrechte bei personellen Maßnahmen aus § 99 BetrVG. Gem. § 99 Abs. 1 BetrVG hat in Unternehmen mit mehr als 20 wahlberechtigten Arbeitnehmern der Arbeitgeber den Betriebsrat *vor jeder Einstellung […] zu unterrichten, ihm die erforderlichen Bewerbungsunterlagen vorzulegen und Auskunft über die Person der Beteiligten zu geben*. Im Anschluss muss er die Zustimmung des Betriebsrats zu der geplanten Maßnahme einholen.

Der Arbeitgeber hat die Bewerbungsunterlagen *aller*[1262] Bewerber an den Betriebsrat zu übergeben, wozu das Bewerbungsschreiben mit allen Anlagen und die vom Arbeitgeber zum Einstellungsverfahren angefertigten eigenen Dokumente gehören.[1263]

Die Unterrichtung muss vor der jeweiligen Maßnahme stattfinden, wobei das Gesetz keinen konkreten Zeitpunkt angibt. Zweckmäßig ist es, den Betriebsrat so früh wie möglich zu informieren. Spätestens (wie sich aus § 99 Abs. 3 BetrVG ergibt) muss die Unterrichtung jedoch eine Woche vor der geplanten Einstellung stattfinden.[1264] Die Informationspflicht wird allerdings erst dann ausgelöst, wenn der Arbeitgeber sich darüber schlüssig geworden ist, welchen der Stellenbewerber er einstellen möchte.[1265]

Sinn und Zweck der Vorschrift ist nicht der Schutz des betroffenen Bewerbers, sondern der der übrigen Arbeitnehmer im Betrieb, andernfalls würde ein Zustimmungserfordernis zu einer Einstellung kaum Sinn ergeben.[1266]

Die Auskunftspflicht des Arbeitgebers gegenüber dem Betriebsrat erstreckt sich auf jene Bewerber, die er nicht berücksichtigen will.[1267] Argument ist, dass das Einstellungsverfahren mit der Auswahl durch den

1262 BT-Drs. IV/1786, S. 51.
1263 BAG, Beschl. v. 03.122.1985 – 1 ABR 72/83, AP BetrVG 1972 § 99 Nr. 29 unter II. 2. der Gründe; Beschl. v. 28.06.2005 – 1 ABR 26/04, NZA 2006, 111 (113) Rn. 23 m.w.N.
1264 ErfK/*Kania*, § 99 BetrVG Rn. 22.
1265 BAG, Beschl. v. 18.07.1978 – 1 ABR 8/75, AP BetrVG 1972 § 99 Nr. 7 unter II. 1. a) der Gründe.
1266 Vgl. Richardi/*Thüsing*, § 99 BetrVG Rn. 29.
1267 So bereits BAG, Beschl. v. 19.05.1981 – 1 ABR 109/78, AP BetrVG 1972 § 118 Nr. 18; Beschl. v. 03.122.1985 – 1 ABR 72/83, AP BetrVG 1972 § 99 Nr. 29; Beschl. v. 28.06.2005 – 1 ABR 26/04, NZA 2006, 111 (114) Rn. 25; ferner BeckOK ArbR/*Mauer*, § 99 BetrVG Rn. 13 m.w.N.

Arbeitgeber noch nicht erledigt ist und der Betriebsrat – im Falle der Verweigerung der Zustimmung – auch die Möglichkeit im Rahmen von § 99 BetrVG hat, *„Anregungen zu geben und Gesichtspunkte vorzubringen, die aus seiner Sicht für die Berücksichtigung eines anderen als des vom Arbeitgeber ausgewählten Stellenbewerbers sprechen.“*[1268] Diese weite Auffassung des BAG wird in der Literatur insbesondere hinsichtlich der offensichtlich ausscheidenden (z.B. wegen fehlenden Qualifikationsvoraussetzungen[1269]) Bewerber kritisiert.[1270] So wird überwiegend vertreten, dass diese Personen bereits nicht zum Kreis der Beteiligten gehören.[1271]

Die „Maßnahme“ stellt die Einstellung des schlussendlich durch den Arbeitgeber ausgewählten Arbeitnehmers selbst dar. Fraglich ist, inwiefern ein Arbeitgeber einem offensichtlich ungeeigneten oder chancenlosen Stellenbewerber bereits vor der Information und Zustimmung des Betriebsrats zum letztendlich gewählten Bewerber eine Absage erteilen darf. Im oben zitierten Urteil aus dem Jahre 1978[1272] stellte das Bundesarbeitsgericht klar, dass die Auswahl unter den Stellenbewerbern Sache des Arbeitgebers ist und erst wenn der Arbeitgeber sich für einen oder mehrere entschieden hat, er beim Betriebsrat um dessen Zustimmung zu der vorgesehenen Einstellung nachsuchen und ihm die dazu erforderlichen Auskünfte geben kann.

Obgleich der Betriebsrat über offensichtlich nicht in Betracht kommende Bewerber informiert werden muss, hat dieser lediglich ein Vetorecht betreffend die Einstellung des vom Arbeitgeber gewählten Kandidaten, da er nach § 99 Abs. 1 BetrVG nur die Zustimmung zur personellen Einzelmaßnahme verweigern kann. Er kann hingegen nicht die Einstellung eines bestimmten Bewerbers verlangen.[1273] Aus diesem Grund kann es dem Arbeitgeber auch nicht verwehrt sein, entsprechenden Stellenbewerbern eine Absage zu erteilen, wenn der Arbeitgeber diese ohnehin nicht berücksichtigen würde. Hieran ändern auch die o.g. Ausführungen zur Möglichkeit des Betriebsrats nichts, Anregungen zur Einstellung eines anderen Bewerbers zu äußern, der nach Auffassung des Betriebsrats besser geeignet

1268 BAG, Beschl. v. 19.05.1981 – 1 ABR 109/78, AP BetrVG 1972 § 118 Nr. 18 unter I. der Gründe.
1269 BAG, Beschl. v. 21.10.2014 – 1 ABR 10/13, NZA 2015, 311 (313) Rn. 29.
1270 *Gragert*, ArbRAktuell 2015, 135.
1271 So bspw. Richardi/*Thüsing*, § 99 BetrVG Rn. 156 m.w.N.; ähnlich MHdB-ArbR/*Lunk*, § 340 Die Mitbestimmung bei der Einstellung, Rn. 50.
1272 BAG, Beschl. v. 18.07.1978 – 1 ABR 8/75, AP BetrVG 1972 § 99 Nr. 7.
1273 Richardi/*Thüsing*, § 99 BetrVG Rn. 204 m.N.; MHdB-ArbR/*Lunk*, § 340 Die Mitbestimmung bei der Einstellung, Rn. 60.

ist. Zwar wird hierdurch die Effektivität der „Anregung" geschmälert, dennoch betrifft das Zustimmungsverfahren nach § 99 BetrVG nur die konkret ausgewählte Person durch den Arbeitgeber.

Betriebsverfassungsrechtlich wird daher eine automatisierte Vorauswahl bzw. ein automatisiertes Vorausscheiden von offensichtlich ungeeigneten Bewerbern nicht durch die Mitspracherechte aus § 99 Abs. 1 BetrVG verhindert. In jedem Falle ist der Betriebsrat aber über diese Teilnehmer des Bewerbungsverfahrens sowie die Gründe für die Aussortierung nach aktueller Rechtsprechung des BAG zu informieren, damit dieser seine Entscheidung über die Zustimmung oder Ablehnung mit einer breiteren Informationsbasis treffen kann sowie dem Arbeitgeber Gegenvorschläge unterbreiten kann.

Da der Betriebsrat aber ebenso wie eine Personalabteilung bei einer Bewerberflut (und nur in diesem Fall kommt diese Problematik überhaupt in Betracht) mit der Sichtung aller Bewerbungsunterlagen maßlos überfordert sein wird, werden in der Praxis häufig andere Absprachen betriebsintern getroffen.[1274]

Aus praktischen Gründen empfiehlt es sich, eine Absprache über die (beim Einsatz von Scoring) im zweiten Schritt anwendbaren Auswahlrichtlinien gem. § 95 BetrVG (dazu nachfolgend **2. b**) in diesem Abschnitt) zu treffen. Diese sollte bereits bei Verfassung der Betriebsvereinbarung, spätestens aber vor Einführung eines solchen Systems vorliegen. Durch eine solche können eventuelle Streitigkeiten im Rahmen des Zustimmungsverfahrens nach § 99 BetrVG, die dadurch entstehen könnten, dass sich der Betriebsrat durch die automatische Vorselektion übergangen fühlt, vermieden werden.

Zu beachten ist, dass der Betriebsrat zudem bereits in der Planungs- und Umsetzungsphase ein Mitbestimmungsrecht nach § 94 Abs. 1 BetrVG hat, wenn im Rahmen einer Bewerbungsplattform o.ä. standardisierte Fragebögen (auch in digitaler Form) zum Einsatz kommen.[1275]

c) Ergebnis

Sowohl aus datenschutzrechtlicher als auch betriebsverfassungsrechtlicher Sicht ist eine computergestützte Selektion der geeigneten Bewerber grund-

---

1274 Vgl. MHdB-ArbR/*Lunk*, § 340 Die Mitbestimmung bei der Einstellung, Rn. 50.

1275 Zur Reichweite des Mitbestimmungsrechts aus § 94 Abs. 1 BetrVG, **D. § 2 II. 2. a**).

sätzlich möglich. Voraussetzung ist, dass (a) die automatische Entscheidungsfindung gem. Art. 22 Abs. 2 lit. a DSGVO erforderlich ist und (b) der Betriebsrat auch über die aussortierten Bewerber umfassend informiert wird. Erforderlich ist eine Vorselektion dann, wenn das Unternehmen eine derart hohe Anzahl an Bewerbungen bekommt, dass es diesem nicht mehr zumutbar ist, alle Bewerbungen manuell zu prüfen und daher – um eine Berücksichtigung aller Bewerber zu ermöglichen – eine computergestützte Auswahl stattfindet.

Die Information des Betriebsrats kann praktischerweise über einen entsprechenden Zugriff auf das Auswahlsystem ermöglicht werden, wobei berücksichtigt werden muss, dass ein Bewerber der Weiterleitung seiner Bewerbungsunterlagen an den Betriebsrat widersprechen kann[1276] und im System für diesen Fall ein Sperrvermerk eingetragen werden müsste, dass der Betriebsrat auf diese Daten keinen Zugriff erhält. Durch einen solchen elektronischen Zugriff umginge man auch den in der rechtswissenschaftlichen Literatur bestehenden Streit hinsichtlich der Reichweite des Informationsrechts des Betriebsrats. Ohnehin besteht für die Mitglieder des Betriebsrats nach § 99 Abs. 1 S. 3 BetrVG eine Schweigepflicht betreffend die hierdurch erlangten Kenntnisse über die Bewerber.

Empfehlenswert, aber nicht zwingend erforderlich, ist eine betriebsinterne Absprache über das Vorgehen bei offensichtlich ungeeigneten Bewerbern; in diesem Rahmen hat der Betriebsrat zwar kein Mitspracherecht bzgl. der Absage, sodass solche auch schon vor Abschluss des Verfahrens automatisch versandt werden dürfen. Dennoch entwertet dies die Möglichkeiten des Betriebsrats, einen anderen, nach seiner Sicht geeigneteren Bewerber vorzuschlagen. Das könnte im Rahmen der Zustimmung zu Personalmaßnahmen nach § 99 Abs. 1 BetrVG zu unnötigen Verzögerungen und Ungereimtheiten führen, wenn beispielsweise der Betriebsrat seine Zustimmung zu einem gut geeigneten Bewerber nur deshalb verneint, weil er sich übergangen fühlt und zunächst ein Zustimmungsersetzungsverfahren nach § 99 Abs. 4 BetrVG geführt werden muss, auch wenn Maßnahme ggf. vorläufig nach § 100 BetrVG dennoch unmittelbar durchführbar ist.

1276 Richardi/*Thüsing*, § 99 BetrVG Rn. 171 m.w.N.

2. Ranking und automatische Bestenvorauswahl

Bleiben nach einem ersten (formalen) Selektionsvorgang so viele Bewerber übrig, dass eine Bearbeitung aller Bewerber durch HR-Verantwortliche immer noch unzumutbar ist und daher ausscheidet, können in einem weiteren Schritt weitere Maßnahmen erforderlich sein, die Bewerbermenge auf ein human bearbeitbares Maß zu senken. Hierfür kann ein Scoring und Ranking, verbunden mit einer Bestenvorauswahl dienen.

Alle nach Phase 1 übriggebliebenen Bewerber werden danach in einem weiteren computerbasierten Verfahren auf ihre Passgenauigkeit für die vorhergesehene Stelle bewertet und benotet. Auf Basis dieses Scores wird dann eine Bestenauswahl vorgenommen, dergestalt, dass die Bewerberanzahl so weit reduziert wird, dass eine manuelle Bearbeitung der übriggebliebenen Stellenbewerber möglich ist.

a) Datenschutzrechtlicher Rahmen

Aus datenschutzrechtlicher Hinsicht besteht nun ein beachtlicher Unterscheid zur formalen Vorselektion. Nun findet ein Profiling / Scoring im Sinne des Art. 4 Nr. 4 DSGVO statt, welches bedeutend stärker in die Persönlichkeitsrechte der betroffenen Bewerber eingreift als die reine Selektion nach formalen Kriterien. Nun werden die perspektivische Arbeitsleistung und das Verhalten durch einen Algorithmus bewertet und daraus eine Vorhersage in Form eines Wahrscheinlichkeitswerts (*Scores*) gebildet, anhand dessen dem HR-Verantwortlichen eine vorsortierte Liste angezeigt wird. Bewerber, die bei dieser Vorsortierung einen unteren Rang erreichen, könnten automatisch aussortiert oder – was einer automatischen Aussortierung gleichkommt[1277] – vom Personalverantwortlichen aufgrund des schlechten Scores nicht mehr beachtet werden.

aa) Anforderungen an das Bewerberscoring

Wie bereits auf den Seiten 321 ff. ausführlich dargestellt, ist ein Bewerberscoring grundsätzlich zulässig, sofern es auf Daten basiert, die zulässigerweise erhoben wurden. Es ist zu beachten, dass die Anzahl der „weichen"

1277 Anm.: Mangels inhaltlicher Entscheidung eines Menschen, hierzu **D. § 1 V. 3. c) aa)**.

Fakten, also Daten zur Persönlichkeit des Bewerbers, stark von der zu besetzenden Stelle abhängig ist. Während in unteren Hierarchieebenen (z.B. beim Arbeitnehmer in der Logistik oder Fertigung am Förderband) es zunächst kaum auf Führungskompetenzen ankommen dürfte, sieht dies beim Gruppen- oder Abteilungsleiter, der eine Personalverantwortung hat, bereits anders aus. Deutlich weitgehender dürfte das Fragerecht des Arbeitgebers bei Managern sein, die auch als leitende Angestellte im Sinne des § 5 Abs. 3 BetrVG zu qualifizieren sind.

Keinesfalls darf ein Totalabbild der Persönlichkeit als Grundlage für die automatisierte Entscheidung herangezogen werden. Bei allem, was kein solches Totalabbild darstellt, ist eine Einzelfallabwägung, basierend auf den Anforderungen der konkret zu besetzenden Stelle erforderlich.

Im Rahmen des Scorings muss darauf geachtet werden, dass in den Algorithmus nur solche Daten einfließen, die tatsächlich für die Generierung des Scores notwendig sind. Zudem muss der Score grundsätzlich zu korrekten Ergebnissen führen, wobei ausreichend ist, dass eine gewisse „Basisrationalität" besteht.[1278] Über die grundlegende Funktion des Scoring-Verfahrens hat der Arbeitgeber die Bewerber auch gem. Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g DSGVO aufzuklären, wobei er jedoch nicht die konkrete Scoring-Formel herausgeben muss (siehe zum Ganzen bereits S. 306 ff.).

bb) Anforderungen an die automatische Auswahlentscheidung

Im Anschluss an das Scoring und Ranking der Bewerber erfolgt eine automatische Bestenvorauswahl. Diese findet nicht nur dann statt, wenn der Computer nur bspw. die 10, 50 oder 100 besten Kandidaten anzeigt, sondern auch dann, wenn die Liste alle Bewerber enthält, die Personalverantwortlichen jedoch nur noch einen Bruchteil aller Bewerber aus den Top-Rängen selbst sichten. Auch in letzterem Fall entscheidet nämlich faktisch der vom Computer generierte Score über die Berücksichtigung im Bewerbungsverfahren und die Entscheidung bezüglich der anderen Bewerber wird nicht mehr menschlich verantwortet.[1279]

Es macht also aus datenschutzrechtlicher Hinsicht keinen Unterschied, ob direkt die Absagen an die nicht-berücksichtigten Stelleninteressenten versandt werden oder ein Mensch zum Ende des Bewerbungsprozesses

1278 *Gerberding/Wagner*, ZRP 2019, 116 (119).
1279 Hierzu bereits **D. § 1 V. 3. c) aa)**.

noch den entsprechenden Button klickt und den Vorschlag des Computers ohne weitere Prüfung übernimmt.

Daher muss für ein solches Verfahren der in Art. 22 Abs. 2 lit. a DSGVO statuierte Erforderlichkeitsgrundsatz gewahrt bleiben (siehe insofern bereits die Ausführungen unter **1. a**) dieses Abschnitts). Auf dieser Grundlage dürfen das Scoring und Ranking als eine Entscheidung vorbereitende Maßnahme auf alle Bewerber angewandt werden (hierzu bereits S. 321 ff.). Soweit es den Personalverantwortlichen aber zumutbar und möglich ist, die Bewerbungen nochmals zu sichten und auf Basis der Datengrundlage und nicht ausschließlich des Scores und Rankings zu entscheiden, muss dies auch vorgenommen werden, da dann eine vollautomatisierte Einzelfallentscheidung nicht erforderlich ist.

Pauschale Grenzen können jedoch nicht genannt werden. Letztendlich hängt es vom Einzelfall (insbesondere Größe der Personalabteilung sowie sonstige Arbeitsbelastung der Personalverantwortlichen) ab, welche Untergrenzen an Bewerbungen für die Automatisierung gelten.

b) Betriebsverfassungsrechtlicher Kontext

Zu den in Ziff. 1 dieses Abschnitts genannten Rechte des Betriebsrats kommen beim Einsatz von Scoringverfahren noch Mitbestimmungsrechte bei der Festlegung allgemeiner Beurteilungsgrundsätze und Auswahlrichtlinien nach den §§ 94 und 95 BetrVG hinzu. Diese Mitbestimmungsrechte entstehen nicht erst im konkreten Bewerbungsverfahren, sondern bereits in der Planungsphase vor Einführung eines solchen Systems. Für das Scoring müssen vorab bestimmte Grundsätze und Kriterien festgelegt werden, nach denen die Bewerber bewertet werden sollen. Diese stellen allgemeine Beurteilungsgrundsätze nach § 94 Abs. 2 sowie, falls auf dieser Basis dann auch eine Auswahl stattfindet, Auswahlrichtlinien nach § 95 BetrVG dar.[1280]

Zu beachten ist, dass der Arbeitgeber dem Betriebsrat nicht nur die Bewerbungsunterlagen aller Bewerber mitteilen muss, sondern auch den vom System generierten Score und Rang in der Liste.[1281] Nur so kann

---

1280 Zum Ganzen siehe **D. § 2 II. 2. b**) und **D. § 2 II. 3**.

1281 Der Arbeitgeber ist verpflichtet, alle Unterlagen anlässlich der Bewerbung, also auch solche Unterlagen, die der Arbeitgeber anlässlich der Bewerbung über die Person erstellt hat, dem Betriebsrat zu übermitteln, vgl. Richardi/*Thüsing*, § 99 BetrVG Rn. 166 m.w.N. aus der Rechtsprechung.

der Betriebsrat nachvollziehen, weshalb ein Arbeitgeber nur bestimmte Stelleninteressenten berücksichtigt und andere außer Betracht bleiben. Ebenfalls sollten bereits im Vorfeld entsprechende Absprachen mit dem Betriebsrat getroffen werden.

c) Ergebnis

Ein Ranking mit automatischer Bestenvorauswahl ist aus datenschutzrechtlicher Hinsicht grundsätzlich zulässig, sofern die Anzahl der eingehenden Bewerbungen ein solches Vorgehen erforderlich macht. Dies ist insbesondere dann der Fall, wenn nach einer ersten Selektion anhand formaler Kriterien (wie z.B. Nichterfüllung von Qualifikationsvoraussetzungen) als milderes Mittel weiterhin so viele Bewerbungen im Pool bleiben, dass es den menschlichen Entscheidern unzumutbar ist, die übrigen Bewerbungen in angemessener Zeit zu sichten und eine ordnungsgemäße Auswahl zu treffen.

In diesem Fall müssen dem Betriebsrat alle Unterlagen, somit auch der konkrete Score und Rang für die jeweiligen Bewerber, übermittelt werden, wobei dies bei rein digitalen Bewerbungen auch durch einen (eingeschränkten[1282]) Zugriff auf das Bewerbermanagementsystem erfolgen kann.[1283]

3. Vollständig automatisiertes Einstellungsmanagement

Wie sich aus den bisherigen Ausführungen unter Ziff. 1 und 2 ergibt, ist sowohl aus datenschutz- als auch betriebsverfassungsrechtlicher Hinsicht (Zustimmungserfordernis gem. § 99 BetrVG) ein vollständig automatisiertes Einstellungsmanagement unzulässig. In keinem Falle kann es erforderlich im Sinne von Art. 22 Abs. 2 lit. a DSGVO sein, dass eine Einstellung vollautomatisch abläuft, ohne dass ein menschlicher Entscheider eine zu-

---

1282 Der Bewerber hat die Möglichkeit, einer Weiterleitung seiner Unterlagen an den Betriebsrat zu widersprechen, vgl. Richardi/*Thüsing*, § 99 BetrVG Rn. 171 m.w.N.

1283 Grundsätzlich muss ein Arbeitgeber dem Betriebsrat die Unterlagen vorlegen, also physikalisch zur Verfügung stellen. Solange die Unterlagen aber ausschließlich digital vorlegen, muss der Arbeitgeber diese nicht extra zur Vorlage anfertigen (ErfK/*Kania*, § 99 BetrVG Rn. 21). Die Ermöglichung des Zugriffs erfüllt daher die Anforderungen des § 99 BetrVG.

mutbare Anzahl Bewerbungen noch selbst prüft. Während die Einstellung des konkret ausgewählten Bewerbers aufgrund der ausschließlich positiven Wirkung nicht vom Verbot des Art. 22 Abs. 1 DSGVO erfasst ist[1284], muss den anderen Bewerbern aber auch eine Absage erteilt werden. Zumindest hierfür muss ein menschlicher Entscheider eingeschaltet werden, der ein Minimum an Bewerbern noch manuell prüft.

Zulässig ist es im Rahmen des Entscheidungsprozesses jedoch, die in Frage kommenden Bewerber vollautomatisch zu einem Bewerbungsgespräch einzuladen und entsprechende Termine automatisch durch das System mit den Entscheidungsträgern abstimmen zu lassen, sofern die Vorauswahl bereits getroffen wurde und dadurch gegenüber den restlichen Bewerbern keine Entscheidung im Sinne des Art. 22 Abs. 1 DSGVO getroffen wird, die rechtliche Wirkung oder ähnliche Wirkungen entfalten würde. Die Einladung selbst stellt keine Entscheidung mit rechtlicher Wirkung oder ähnlicher Beeinträchtigung dar, sodass dieser Automatismus nicht vom Verbot der automatisierten Einzelfallentscheidung erfasst ist.

II. Laufendes Beschäftigungsverhältnis

Automatisierte Einzelfallentscheidungen sind nicht nur im Rahmen des Bewerbungsprozesses denkbar, sondern auch im laufenden Beschäftigungsverhältnis. So könnten auf Basis generierter Scores oder Leistungsbewertungen am Ende des Jahres automatisch Gehaltserhöhungen an High-Performer ausbezahlt oder bestimmte Arbeitnehmer für Weiterbildungen automatisch angemeldet werden. Aus praktischer Hinsicht könnte das so weit führen, dass Versetzungen oder Kündigungen durch das System bei längerfristigen Minderleistungen „ausgesprochen" werden. All diese Maßnahmen müssen aus datenschutzrechtlicher Hinsicht am Maßstab des Art. 22 DSGVO gemessen werden. Im Folgenden sollen diese Anwendungsszenarien aus datenschutzrechtlicher sowie betriebsverfassungsrechtlicher Sicht auf ihre Zulässigkeit untersucht werden.

a) Gehaltsveränderungen / Festlegung variabler Lohnbestandteile

Wie bereits kurz dargestellt, könnten automatisierte Prozesse dazu genutzt werden, den variablen Lohn von Arbeitnehmern aufgrund digitalisierter

1284 Siehe hierzu **D. § 1 V. 3. c) bb)**.

Zielvereinbarungen, Scores oder Umsatzzahlen zum jeweiligen Stichtag automatisiert festzulegen oder eventuelle Gehaltsveränderungen (z.B. eine automatische Erhöhung bei High-Performern) am Jahresende vollständig automatisch festgesetzt werden.

aa) Datenschutzrechtlicher Rahmen

Aus datenschutzrechtlicher Sicht muss zwischen dem Prozess der Erhebung und Verarbeitung der notwendigen Daten für die Entscheidung (§ 26 Abs. 1 S. 1 BDSG) sowie der Automation des Entscheidungsprozesses selbst (Art. 22 DSGVO) unterschieden werden.

(1) Festlegung und Auszahlung variabler Vergütungen

Sollen variable Gehaltsbestandteile aufgrund von Umsatzzahlen ausbezahlt werden, so handelt es sich noch nicht um ein Profiling im Sinne des Art. 4 Nr. 4 DSGVO, da keine persönlichen Aspekte, die sich auf eine natürliche Person beziehen, bewertet werden. Die Verwendung dieser Zahlen ist aus datenschutzrechtlicher Hinsicht völlig unproblematisch, da es sich nicht um personenbezogene Daten handelt. Erst durch die Verknüpfung mit dem jeweiligen Datensatz des zu bezahlenden Arbeitnehmers erhalten diese Daten eine datenschutzrechtliche Relevanz, da sie dann personenbezogen werden, insbesondere, wenn sie als Grundlage zur Bestimmung des variablen Vergütungsanteils einer natürlichen Person dienen.

Dennoch unterliegt diese Maßnahme nicht dem Verbot des Art. 22 Abs. 1 DSGVO, da bereits keine *Entscheidung* mit rechtlicher Wirkung oder ähnlicher Beeinträchtigung vorliegt: In diesem Fall wird lediglich ausgeführt, was zuvor vertraglich vereinbart wurde.[1285] Der Betroffene benötigt für diesen Prozess auch nicht den Schutz des Art. 22 Abs. 3 DSGVO, da er bei einer Falschberechnung durch den Computer (wenn z.B. falsche Umsatzzahlen als Grundlage herangezogen werden), bereits aus dem Arbeitsvertrag ein Recht auf Auszahlung des korrekten variablen Vergütungsbestandteils hat.

Etwas anderes kann gelten, wenn auf Basis von Zielvereinbarungen und Scores die Festlegung des variablen Bestandteils erfolgt. In aller Regel

1285 *Klar*, BB 2019, 2243 (2249); *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 19.

besteht zwar auch hier eine Abmachung, wie hoch der zu zahlende Anteil bei einer gewissen Bewertung ist, die Bewertung selbst, die Basis der Entscheidung ist, obliegt aber dem Arbeitgeber bzw. beim Scoring dem Computeralgorithmus. Maßgeblich ist, dass der Score vollautomatisch erstellt wird und die Entscheidung über die Auszahlung beinhaltet. Bei letzterem handelt es sich daher um eine von Art. 22 Abs. 1 DSGVO erfasste Entscheidung, da ohne Dazwischenschalten eines Menschen automatisch die variable Vergütung ausbezahlt wird. In solchen Fällen muss ein Recht auf Darlegung des eigenen Standpunkts und Anfechtung der Entscheidung nach Art. 22 Abs. 3 DSGVO gewährt werden.

Dies gilt nicht nur für eine vollautomatische Entscheidung, sondern auch für eine menschliche Entscheidung, die allein darauf fußt, dass der Score als Grundlage für die Auszahlung des variablen Vergütungsbestandsteils verwendet wird, denn dann wird der menschliche Entscheider nur noch formal eingeschaltet und prüft nicht mehr das Ergebnis der Entscheidung auf Basis der Datengrundlage.[1286] Der betroffene Arbeitnehmer stünde schutzlos dar, wenn er den Score, der als Grundlage der Entscheidung diente, nicht anfechten könnte und kein Recht auf Darlegung des eigenen Standpunkts bekäme.

Da die Nicht-Ausbezahlung der vollen variablen Vergütung in aller Regel eine erhebliche Beeinträchtigung darstellt (Art. 22 Abs. 1 DSGVO), unterliegt diese Maßnahme dem grundsätzlichen Verbot der automatisierten Einzelfallentscheidung. Fraglich ist, ob die Ausnahme der Erforderlichkeit nach Art. 22 Abs. 2 lit. a DSGVO einschlägig ist. Hierfür wäre es erforderlich, dass ein derart großer Datensatz als Grundlage dient, dass es für einen menschlichen Entscheider unzumutbar ist, diesen manuell abzuarbeiten. Dies wird in der Regel nicht der Fall sein.

Selbst dann dürfte aber eine vollautomatisierte Entscheidung, dergestalt, dass kein Mensch zumindest den Computervorschlag noch genehmigt, unzulässig sein. Jedenfalls den fachverantwortlichen Bereichs-/Gruppen-/Abteilungsleitern ist es zumutbar, die computergenerierten Scores zumindest noch auf ihre Plausibilität zu überprüfen. Zu weitgehend wäre es aber, diesen abzuverlangen, dass bei sehr komplexen Beurteilungsalgorithmen (falls solche notwendig sind, um eine faire Beurteilung zu gewährleisten), der Entscheider die gesamte Datengrundlage nochmals überprüfen muss; insofern ist eine automatisierte Entscheidung notwendig und unter der Ausnahme des Art. 22 Abs. 2 lit. a unter den in **D. § 1 V. 3. d) aa)** entwickelten Maßstäben zu rechtfertigen.

1286 Siehe hierzu **D. § 1 V. 3. c) aa)**.

(2) Berechnung und Auszahlungen von Gehaltserhöhungen

Etwas anderes gilt, wenn am Jahresende Gehaltserhöhungen automatisch festgelegt und ausbezahlt werden sollen. Eine Gehaltserhöhung stellt ein (ggf. konkludentes) Angebot des Arbeitgebers an den Arbeitnehmer dar, das durch vorbehaltslose Weiterarbeit und Entgegennahme des erhöhten Entgelts durch den Arbeitnehmer konkludent gem. § 151 BGB angenommen wird.[1287] Um von Art. 22 DSGVO erfasst zu sein, müsste eine (nachteilige) rechtliche Wirkung vorliegen. Eine rechtliche Wirkung liegt dann vor, wenn sich der rechtliche Status der betroffenen Person in irgendeiner Weise (nachteilig) verändert.[1288] Zwar ist zweifelhaft, ob durch die Abgabe eines konkludenten Angebots durch den Arbeitgeber sich der rechtliche Status des Arbeitnehmers verändert[1289], jedenfalls handelt es sich hierbei nicht um eine nachteilige rechtliche Wirkung, sodass die Maßnahme „automatisierte Gehaltserhöhung" in aller Regel nicht vom Verbot des Art. 22 Abs. 1 DSGVO erfasst ist. Eine Ausnahme bilden diejenigen Fälle, in denen der Algorithmus (in unzulässiger Weise) diskriminiert oder willkürlich entscheidet, sodass gegen den arbeitsrechtlichen Gleichbehandlungsgrundsatz[1290] oder Diskriminierungsverbote[1291] verstoßen wird.

Für die letztere Maßnahme benötigt es daher keiner besonderen datenschutzrechtlichen Rechtfertigung nach Art. 22 Abs. 2 DSGVO.

1287 Vgl. LAG München, Urt. v. 19.01.2017 – 3 Sa 668/16, BeckRS 2017, 152341 Rn. 45.

1288 *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 22 DSGVO Rn. 32, wobei hier keine nachteilige rechtliche Wirkung gefordert wird.

1289 Dies ist wohl anzunehmen, da aufgrund der Bindung des Antragenden an das Angebot (§ 145 BGB) der Antragsempfänger eine Rechtsposition dergestalt bekommt, dass er das Angebot innerhalb der Annahmefrist zu den angebotenen Konditionen annehmen kann und der Antragende dies nicht mehr einseitig zurückziehen kann. Unklar in diesem Zusammenhang: *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 22 DSGVO Rn. 34, der das Beispiel des Angebots zwar nennt, aber nicht auf die Person des Abgebenden eingeht; wohl dafür *Schulz*, in: Gola, Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 22: Grundsätzlich ist jede Rechtsfolge erfasst, die eine Rechsposition begründet. *Schulz* schränkt das Recht aber auch auf nachteilige Rechtsfolgen ein, sodass die Begründung einer Rechtsposition des Betroffenen auch nach seiner Auffassung nicht darunterfallen dürfte.

1290 Zur Einordnung des arbereitsrechtlichen Gleichbehandlungsgrundsatzes unter die Kriterien des Art. 22 DSGVO, vgl. bereits oben **D. § 1 V. 3. c) bb)**.

1291 Ehmann/Selmayr/*Hladjk*, Art. 22 DSGVO Rn. 9.

bb) Betriebsverfassungsrechtlicher Kontext

Im betriebsverfassungsrechtlichen Kontext sind vor allem im Vorfeld solcher Maßnahmen weitgehende Mitbestimmungsrechte des Betriebsrats gegeben. Hierzu zählen insbesondere § 87 Abs. 1 Nr. 10 und 11 BetrVG.[1292] Während Nr. 10 die Lohngerechtigkeit dadurch sicherstellen soll, dass der Betriebsrat bei der betrieblichen Lohngestaltung, insbesondere bei der Aufstellung von Entlohnungsgrundsätzen und Einführung und Anwendung von neuen Entlohnungsmethoden ein Mitspracherecht hat, dient Nr. 11 demselben Zweck, allerdings spezifisch bei leistungsbezogenen Entgelten. § 87 Abs. 1 Nr. 11 BetrVG ist weiter als Nr. 10, da ersterer auch ein Mitbestimmungsrecht hinsichtlich der Lohnhöhe statuiert. Dies folgt daraus, dass die Festlegung der Geldfaktoren immer unter Anwendung eines Beurteilungsspielraums erfolgen müssen und enormen Druck auf die Arbeitnehmer erzeugen können.

Ein weiteres, in diesem Zusammenhang zu beachtendes Mitbestimmungsrecht statuiert § 94 Abs. 2 BetrVG: Die Mitbestimmung hinsichtlich der Aufstellung allgemeiner Beurteilungsgrundsätze.[1293] Diese Beurteilungsgrundsätze benötigt es, um eine Grundlage für Scoring und Profiling zu schaffen und einen „Leistungsbezugsrahmen" festzulegen. Auch diese müssen in Zusammenarbeit mit dem Betriebsrat vorab festgelegt werden. Das Mitbestimmungsrecht erstreckt sich ferner auf die Frage, ob die Bewertung vollautomatisch erfolgt oder eine Person dazwischengeschaltet wird.[1294]

Sollen technische Einrichtungen zur Überwachung der Leistung eingesetzt werden und diese Daten zur Festlegung der variablen Vergütung genutzt werden, so muss bereits vor der Einführung der technischen Einrichtungen der Betriebsrat nach § 87 Abs. 1 Nr. 6 BetrVG beteiligt werden.[1295]

cc) Ergebnis

Es kann festgehalten werden, dass nicht jegliche Entscheidungen im Personalbereich von Art. 22 Abs. 1 DSGVO erfasst sind; insbesondere Gehaltser-

1292 Siehe die Grundlagen unter **D. § 2 II. 1. c**).
1293 Vgl. **D. § 2 II. 2. b**).
1294 Richardi/*Thüsing*, § 94 BetrVG Rn. 62.
1295 Zum Mitbestimmungsrecht bei technischen (Überwachungs-)Einrichtungen, siehe bereits ausführlich **D. § 2 II. 1. b**).

höhungen sind – die Diskriminierungs- und Willkürfreiheit vorausgesetzt – nicht vom Verbot erfasst. Umsatzabhängige variable Vergütungen, die automatisiert ausbezahlt werden, unterliegen mangels einer automatisierten Einzelfallentscheidung ebenfalls nicht dem Verbot. Erfasst sind hingegen Leistungsbeurteilungen durch den Computer, sofern diese zu einer erheblichen Beeinträchtigung in Form einer (verminderten) variablen Vergütung führen können, wenn ein Algorithmus die Entscheidung über die Auszahlung entweder vollautomatisch durchführt oder ein menschlicher Entscheider den computergenerierten Score schlicht übernimmt.

Während die vollautomatische Durchführung nicht unter dem Aspekt der Erforderlichkeit gerechtfertigt werden kann, ist die Lage bei der Übernahme durch einen Menschen, verbunden mit einer Plausibilitätsprüfung, anders zu bewerten. In letzterem Fall kann es (dies ist im Einzelfall zu prüfen) durchaus aufgrund einer komplexen Datenausgangslage erforderlich sein, dass der gebildete Score weitgehend übernommen wird. Der betroffene Arbeitnehmer hat zu seinem Schutz ein Recht auf Anfechtung der Entscheidung und Darlegung des eigenen Standpunkts im Einzelfall nach Art. 22 Abs. 3 DSGVO.

b) Anmeldung für Weiterbildungen (Personalförderung)

Advanced People Analytics können auch dazu genutzt werden, um ein (Weiterbildungs-)Profil zu generieren, das die fachlichen/persönlichen Stärken und Schwächen des Arbeitnehmers aufzeigt (zu den Voraussetzungen einer solchen Profilbildung **E. § 1 II** sowie **E. § 1 III. 2. c**)).

Auf Basis dieses Profils könnten Arbeitnehmer dann automatisch im Rahmen der Personalförderung durch das HR-Management-System zu Fortbildungen angemeldet werden. In einer sehr fortschrittlichen Variante könnte ein solches System den digitalen Kalender des jeweiligen Arbeitnehmers analysieren und Fortbildungen so terminieren, dass keine wichtigen Termine verpasst werden. Dies könnte so weit führen, dass das System den Termin der Fortbildung automatisch in den Kalender einträgt und den Arbeitnehmer per E-Mail informiert.

Im Kern der Betrachtung stehen hier berufliche Fortbildungen im Sinne des § 1 Abs. 1 und 4 BBiG.[1296] Diese kann der Arbeitgeber einseitig per Direktionsrecht anordnen und den Arbeitnehmer zur Teilnahme verpflich-

1296 Einen Überblick gibt *Poeche*, Stichwort "Fortbildung", in: Küttner, Personalbuch 2020, Rn. 2 ff.

ten.[1297] Voraussetzung ist, dass „diese Schulungen bzw. Fortbildungsmaßnahmen der Ausübung der vertraglich geschuldeten Tätigkeit förderlich sind, d.h. so weit die im Rahmen der Schulung vermittelten Kenntnisse typischerweise im vereinbarten Tätigkeitsbereich einzusetzen sind."[1298]

Denkbar ist auch, dass für Fortbildungsmaßnahmen Verträge abgeschlossen werden, insbesondere wenn es sich um kostspielige Fortbildungen (z.B. Vorbereitungskurs zum Steuerberaterexamen oder eine Pilotenausbildung) handelt und eine Bindung des Arbeitnehmers an den Arbeitgeber gewollt ist.[1299] Da aber bereits aus praktischer Hinsicht eine automatisierte Einzelfallentscheidung aufgrund der besonderen Auswirkungen auf das Arbeitsverhältnis und der Notwendigkeit weiterer Verhandlungen ausscheidet, wird diese Möglichkeit in dieser Arbeit nicht weiter untersucht.

aa) Datenschutzrechtlicher Rahmen

Bei den Schulungsmaßnahmen, die durch Direktionsrecht angeordnet werden, besteht eine Verpflichtung des Arbeitnehmers an diesen teilzunehmen. Diese Entscheidung entfaltet also eine rechtliche Wirkung[1300], die nicht lediglich vorteilhaft für den Arbeitnehmer ist (Nicht-Folgeleistung ist eine Pflichtverletzung), sodass grundsätzlich das Verbot des Art. 22 Abs. 1 DSGVO eingreift, mit der Folge, dass der Ausnahmetatbestand der Erforderlichkeit nach Abs. 2 lit. a vorliegen müsste.

Eine Erforderlichkeit erscheint nach den unter **D. § 1 V. 3. d) aa)** herausgearbeiteten Grundsätzen höchst zweifelhaft: Auch in solchen Konstellationen ist zwischen dem Profiling des Arbeitnehmers als ersten Schritt der Fortbildungsplanung, der im Anschluss folgenden automatischen Anmeldung als zweiten Schritt und der Eintragung im Kalender und Mitteilung an den Arbeitnehmer als dritten Schritt zu unterscheiden. Erstere Maßnahme stellt noch keine automatisierte Einzelfallentscheidung dar, sondern ist als Advanced People Analytics-Maßnahme und somit einfachen Verarbeitungsvorgang (siehe oben **E. § 1 III. 2**) einzuordnen. Dasselbe gilt für

1297 *Klinkhammer/Peters*, ArbRAktuell 2015, 369 (370); *Poeche*, Stichwort "Fortbildung", in: Küttner, Personalbuch 2020, Rn. 16.

1298 LAG Rheinland-Pfalz, Urt. v. 23.11.2016 – 2 Ca 1147/16, BeckRS 2017, 123929 Rn. 36 m.w.N.

1299 Vgl. auch die Empfehlung von *Klinkhammer/Peters*, ArbRAktuell 2015, 369 (370).

1300 Zum Merkmal der „rechtlichen Wirkung" siehe **D. § 1 V. 3. c) bb) (1)**.

letzteres: Die Eintragung im Kalender; diese ist mangels Entscheidung mit rechtlicher Wirkung oder ähnlicher Beeinträchtigung ebenfalls nicht von Art. 22 Abs. 1 DSGVO erfasst.

Im Kern der Betrachtung steht daher die Erforderlichkeit einer automatischen Datierung für und Anmeldung von Fortbildungsmaßnahmen für Arbeitnehmer. Dies dürfte in aller Regel zu verneinen sein, da die Situation im Vergleich zu den bisher untersuchten (z.B. die Bewerberflut in **E. § 2 I**) eine völlig unterschiedliche ist.[1301] In diesem Fall müssen nicht wenige HR-Verantwortliche eine (vergleichsweise) extrem hohe Anzahl an Entscheidungen nahezu gleichzeitig treffen, sondern je nach Fortbildung sind immer nur wenige Arbeitnehmer betroffen und die inhaltliche Entscheidung über die Notwendigkeit und das Datum kann durchaus auch vom jeweiligen Gruppen- oder Abteilungsleiter getroffen werden. Eine gangbare Alternative ist es, dass das System Vorschläge generiert und die Ausgangslage des Vorschlags für den Entscheidungsträger transparent dargestellt wird, sodass dieser auf Basis der Datengrundlage dem Vorschlag folgen kann. So können in aller Regel auch persönliche Erfahrungen des Vorgesetzten mit dem jeweiligen Arbeitnehmer in die Entscheidung miteinfließen, sodass es sich bei der Übernahme des Vorschlags dennoch nicht um eine „blinde Übernahme" handelt und somit keine automatisierte Einzelfallentscheidung i.S.d. Art. 22 DSGVO vorliegt.

Alternativ können bei optionalen Schulungen, die nicht per Direktionsrecht angeordnet werden, den Arbeitnehmern Vorschläge unterbreitet werden (z.B. in einem persönlichen Dashboard oder per E-Mail), bei denen dieser dann entsprechend seinem persönlichen Zeitplan ein passendes Datum auswählen (sofern mehrere zur Verfügung stehen) und sich hierfür per Mausklick anmelden kann. Die Daten werden im Anschluss automatisch in das Fortbildungssystem übernommen und entsprechende Kurse gebucht. In diesem Fall handelt es sich nicht um eine automatisierte Einzelfallentscheidung, da der Computer letztlich (ähnlich wie bei einer Bestellung auf Amazon o.ä.) nur ausführt, was der Arbeitnehmer (und der Arbeitgeber, indem der dem Arbeitgeber die Möglichkeit zur „freien" Buchung eines Kurses überlässt) entschieden hat.

1301 So i.E. auch *Hinz*, 11. Arbeitsrecht, in: Kaulartz/Ammann/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, Rn. 25.

bb) Betriebsverfassungsrechtlicher Kontext

Sämtliche Maßnahmen der Berufsbildung i.S.d. § 1 Abs. 1 BBiG, wozu auch Fortbildungen, betriebliche Lehrgänge, Seminare etc. gehören, unterliegen den Beteiligungsrechten des Betriebsrats nach §§ 96 - 98 BetrVG.[1302] Das Beteiligungsrecht bezieht sich vor allem auf betriebliche Maßnahmen, d.h. solche, bei denen der Arbeitgeber Träger bzw. Veranstalter der Bildungsmaßnahme ist, unabhängig von der örtlichen Durchführung.[1303] Dies ist immer dann der Fall, wenn der Arbeitgeber – rechtlich gesehen – einen beherrschenden Einfluss auf Inhalt und Organisation hat.[1304] Handelt es sich um eine überbetriebliche Bildungsmaßnahme, z.B. auf Basis eines Kooperationsvertrags zwischen mehreren Arbeitgebern, so kann der Betriebsrat dort mitbestimmen, wo der Arbeitgeber noch eigene Festlegungen für die spätere Maßnahme treffen kann (z.B. wenn der Arbeitgeber den Inhalt bestimmen/beeinflussen kann oder den Zeitpunkt der Veranstaltung).[1305]

Bei vollständig außerbetrieblichen Maßnahmen scheitert ein Mitbestimmungsrecht des Betriebsrats an der mangelnden Gestaltungsmacht des Arbeitgebers.[1306] Hinsichtlich des Berufsbildungsbedarfs und der Fragen der Berufsbildung der Arbeitnehmer des Betriebs hat der Betriebsrat jedoch ein Beratungsrecht nach § 96 Abs. 1 S. 2 BetrVG – auch bei vollständig externen Maßnahmen.[1307]

All diese Beteiligungsrechte hindern den Arbeitgeber aber nicht daran, bestimmte Maßnahmen für bestimmte Arbeitnehmer automatisiert anzubieten.

Lediglich unter den Voraussetzungen des § 98 Abs. 3 BetrVG kann der Betriebsrat Vorschläge für die Teilnahme von Arbeitnehmern oder Gruppen von Arbeitnehmern an Berufsbildungsmaßnahmen machen. Dies ist der Fall, wenn der Arbeitgeber die Maßnahmen entweder selbst durchführt, Arbeitnehmer für außerbetriebliche Maßnahmen freistellt oder die Kosten ganz oder teilweise trägt. Dieses Vorschlagsrecht geht so weit, dass bei einer Uneinigkeit über die Vorschläge nach § 98 Abs. 4 BetrVG die

1302 BeckOK ArbR/*Mauer*, § 96 BetrVG Rn. 2 f.
1303 ErfK/*Kania*, § 96 BetrVG Rn. 8.
1304 BAG, Beschl. v. 04.12.1990 – 1 ABR 10/90, AP BetrVG 1972 § 97 Nr. 1.
1305 BAG, Beschl. v. 18.04.2000 – 1 ABR 28/99, AP BetrVG 1972 § 98 Nr. 9 unter B. I. 2. c) cc) der Gründe.
1306 BAG, Beschl. v. 18.04.2000 – 1 ABR 28/99, AP BetrVG 1972 § 98 Nr. 9 unter B. I. 2. a) bb) der Gründe m.w.N.
1307 ErfK/*Kania*, § 96 BetrVG Rn. 8 m.w.N.

Einigungsstelle angerufen werden kann. Das Recht ist also nicht nur ein Vorschlagsrecht, sondern ein Mitbestimmungsrecht in Form eines Initiativrechts.[1308] Die fachlichen Zulässigkeitsvoraussetzungen für die jeweilige Bildungsmaßnahme obliegen aber ausschließlich dem Arbeitgeber.[1309] Der Betriebsrat muss also eigene Vorschläge machen, um z.B. bei Kapazitätsengpässen über die Auswahl der Arbeitnehmer nach dem vom Arbeitgeber festgelegten Zulässigkeitskriterien mitbestimmen zu können.[1310]

In letzterem Fall entscheidet bei Streitigkeiten die Einigungsstelle nicht nur über die Vorschläge des Betriebsrats, sondern auch über jene, die vom Arbeitgeber ausgewählt wurden, gemeinsam und wählt die Arbeitnehmer anhand der festgelegten Kriterien aus, bis die Kapazitätsgrenze der Bildungsmaßnahme erreicht ist; ein generelles Mitbestimmungsrecht hinsichtlich der Auswahl des Arbeitgebers besteht daher nicht.[1311]

Aus betriebsverfassungsrechtlicher Sicht ist es aber daher notwendig, geplante Bildungsmaßnahmen zunächst mit dem Betriebsrat abzusprechen, bevor solche dem Arbeitnehmer verbindlich angeboten werden und dieser sich einen Platz über das Fortbildungssystem buchen kann. Empfehlenswert ist, die Vorschlagsliste des Arbeitgebers, die durch ein Scoring / Profiling der Arbeitnehmer produziert wurde, dem Betriebsrat zu übermitteln, sodass dieser überprüfen kann, ob jene Arbeitnehmer, die der Betriebsrat vorschlagen würde, bereits auf der Liste sind. Vor der Anmeldung für die Schulung ist sodann zu überprüfen, ob der Betriebsrat eigene Vorschläge macht und ob diese im Rahmen der Kapazitäten der Bildungsmaßnahme liegen und den fachlichen Zulässigkeitsvoraussetzungen des Arbeitgebers entsprechen. Hier kann ein Scoring der Vorschläge des Betriebsrats helfen, im Streitfall eine einvernehmliche Lösung zu finden, ohne dass es zu einer Anrufung der Einigungsstelle nach § 98 Abs. 4 BetrVG kommen muss.

cc) Ergebnis

Ein vollständig automatisiertes Bildungsmanagement durch ein intelligentes Personalmanagementsystem scheidet sowohl aus datenschutzrecht-

1308 Richardi/*Thüsing*, § 98 BetrVG Rn. 60.
1309 BAG, Beschl. v. 08.12.1987 – 1 ABR 32/86, AP BetrVG 1972 § 98 Nr. 4; ferner Richardi/*Thüsing*, § 98 BetrVG Rn. 61 m.w.N.
1310 Vgl. BAG, Beschl. v. 20.04.2010 – 1 ABR 78/08, NZA 2010, 902 (903 f.) Rn. 16.
1311 BAG, Beschl. v. 08.12.1987 – 1 ABR 32/86, NZA 1988, 401 f.

lichen als auch betriebsverfassungsrechtlichen Gründen aus. Für einen Teil der Bildungsmaßnahmen ist dies bereits aus praktischer Hinsicht undenkbar, da weitere Vereinbarungen zwischen Arbeitgeber und Arbeitnehmer, z.B. im Hinblick auf die Kostentragung oder eventuelle Bindungen des Arbeitnehmers (insbesondere bei höherpreisigen und längerfristigen Bildungsmaßnahmen[1312]) getroffen werden müssen. Der Großteil der Bildungsmaßnahmen wird in der Praxis (wohl) per Direktionsrecht angeordnet oder dem Arbeitnehmer die Teilnahme freigestellt. Lediglich bei ersteren läge eine automatisierte Einzelfallentscheidung vor, deren Zulässigkeit aber an der Erforderlichkeit der Maßnahme gem. Art. 22 Abs. 1 lit. a DSGVO scheitert. Zudem hat der Betriebsrat bei Bildungsmaßnahmen ein Vorschlagsrecht nach § 98 Abs. 3 BetrVG. Dies gilt auch bei externen Schulungsmaßnahmen, sofern Arbeitnehmer dafür freigestellt werden oder er die Kosten ganz oder teilweise trägt. Dies dürfte die überwiegende Anzahl der Fortbildungen im Rahmen des Arbeitsverhältnisses betreffen. Da in aller Regel die Maßnahmen nur eine bedingte Kapazität haben, ist damit zu rechnen, dass es zu Engpässen kommen kann und daher die Betriebsparteien sich über die Teilnahme aller, also nicht nur der Vorschläge des Betriebsrats, sondern auch der vom Arbeitgeber vorgesehenen Fortbildungsteilnehmer, einigen müssen.

Eine automatisierte Einzelfallentscheidung (bspw. in Form einer Anmeldung für die Schulung) führt daher auch aus betriebsverfassungsrechtlichen Gründen zu Problemen.

Möglich bleibt es aber dennoch, die Arbeitnehmer in diesem Rahmen zu scoren bzw. profilen[1313] und eine Vorschlagsliste generieren zu lassen. Ebenso unproblematisch, da keine Entscheidung mit rechtlicher Wirkung oder ähnlicher Beeinträchtigung vorliegt, ist nach erfolgter Anmeldung eine automatische Eintragung in den Kalender des jeweiligen Arbeitnehmers und eine Information per E-Mail oder das automatisierte Versenden einer Termineinladung zur Schulung per E-Mail, die der Arbeitnehmer dann bestätigen kann.

1312 *Poeche*, Stichwort "Rückzahlungsklausel", in: Küttner, Personalbuch 2020, Rn. 1 ff.

1313 Hierbei handelt es sich um eine Advanced People Analytics-Maßnahme, die den unter **E. § 1 III. 2** beschriebenen Voraussetzungen unterliegt.

c) Versetzungen und Kündigungen

Ein weiteres mögliches Einsatzszenario für automatisierte Einzelfallentscheidungen stellen Versetzungen und Kündigungen dar. Dies kommt etwa in Betracht, wenn Kapazitätsengpässe in einer anderen Niederlassung bestehen oder über ein Scoring der Arbeitsleistung über einen größeren Zeitraum festgestellt wird, dass ein Arbeitnehmer ein sog. Low-Performer ist und deshalb gekündigt werden soll. Insbesondere bei Kündigungen sind nicht nur datenschutzrechtliche und betriebsverfassungsrechtliche, sondern auch kündigungsschutzrechtliche Fragen zu klären, weshalb diese Maßnahmen im Folgenden gesondert geprüft werden.

aa) Versetzungen

Unter einer Versetzung versteht man (im betriebsverfassungsrechtlichen Sinne, vgl. § 95 Abs. 3 BetrVG) die Zuweisung eines anderen Arbeitsbereichs, die voraussichtlich die Dauer von einem Monat überschreitet oder die mit einer erheblichen Änderung der Umstände verbunden ist, unter denen die Arbeit zu leisten ist.[1314] Lediglich wenn die Arbeitnehmer nach der Eigenart des Arbeitsverhältnisses nicht ständig an einem bestimmten Arbeitsplatz beschäftigt werden, handelt es sich nicht um eine Versetzung.

Ein anderer Arbeitsbereich dem Arbeitnehmer wird zugewiesen, wenn diesem ein neuer Tätigkeitsbereich übertragen wird, sodass der Gegenstand der geforderten Arbeitsleistung nun ein anderer wird und sich das Gesamtbild der Tätigkeit verändert. Von einer Veränderung ist auch auszugehen, wenn sich die Umstände, unter denen die Arbeit zu erbringen ist, wesentlich verändern. Nicht ausreichend hierfür ist, wenn sich lediglich die Arbeitszeit ändert.[1315]

Es muss nicht zwingend ein Wechsel des Arbeitsplatzes stattfinden. So kann es bereits als Versetzung gewertet werden, wenn z.B. im Rahmen

---

1314 *Nota bene:* Individualarbeitsrechtlich gibt es keine einheitliche Definition für eine Versetzung; insbesondere gibt es dort keine starren zeitlichen Fristen, vgl. *Poeche*, Stichwort "Versetzung", in: Küttner, Personalbuch 2020, Rn. 2 ff. In aller Regel kommt es jedoch zu einem Gleichlauf mit dem betriebsverfassungsrechtlichen Begriff.

1315 Zum Begriff des Arbeitsbereichs bereits BAG, Beschl. v. 23.11.1993 – 1 ABR 38/93, AP BetrVG 1972 § 95 Nr. 33 unter B. I. 1. der Gründe; Beschl. v. 19.02.1991 – 1 ABR 21/90, AP BetrVG 1972 § 95 Nr. 25 unter B. II. der Gründe.

einer Matrixorganisation neue Vorgesetzte hinzukommen, die eigene disziplinarische Befugnisse haben.[1316]

In aller Regel liegt eine Versetzung vor, wenn ein Arbeitsplatz an einem anderen Ort zugewiesen wird, auch wenn die zu erbringende Arbeitsleistung inhaltlich unverändert bleibt. Dasselbe gilt, wenn der Arbeitnehmer in eine andere organisatorische Einheit eingegliedert wird.[1317]

Ebenso um eine Versetzung handelt es sich, wenn dem Arbeitnehmer eine Tätigkeit im Home-Office zugewiesen wird. Fehlt es an einer Zuweisung und wird ihm lediglich die Option eröffnet, während sein bisheriger Arbeitsplatz bestehen bleibt, liegt keine Versetzung vor.[1318]

(1) Datenschutzrechtlicher Rahmen

Individualarbeitsrechtlich handelt es sich bei der Versetzung um eine einseitige Änderung des Arbeitsortes per Direktionsrecht gem. § 106 GewO[1319], wobei dieses arbeitsvertraglich durch Versetzungsklauseln eingeschränkt oder erweitert werden kann.[1320] Wird eine solche Versetzung mittels Direktionsrecht per automatisierter Einzelfallentscheidung vorgenommen, unterliegt diese grundsätzlich dem Verbot aus Art. 22 Abs. 1 DSGVO und muss daher erforderlich im Sinne des Buchst. a des Absatzes 2 sein, da keine anderen Ausnahmetatbestände einschlägig sind.[1321]

Nach den bisher entwickelten Maßstäben müsste hierfür eine derart große Menge an Daten auszuwerten sein, dass ein bzw. mehrere Entscheider damit „überfordert" sind, m.a.W. es nicht mehr zumutbar ist, die Entscheidung selbst zu treffen.

Da Versetzungen nur vereinzelt und nicht als „Massenphänomen" stattfinden, ist eine automatisierte Einzelfallentscheidung nicht erforderlich und somit unzulässig.

1316 ErfK/*Kania*, § 99 BetrVG Rn. 14 m.w.N.

1317 Vgl. BAG, Beschl. v. 18.02.1986 – 1 ABR 27/84, AP BetrVG 1972 § 99 Nr. 33; Beschl. v. 18.10.1988 – 1 ABR 26/87, AP BetrVG 1972 § 99 Nr. 56.

1318 ErfK/*Kania*, § 99 BetrVG Rn. 15.

1319 Versetzungen, die nicht vom Direktionsrecht erfasst sind, bedürfen einer Änderungskündigung und werden somit von den Ausführungen unter bb) erfasst.

1320 Im Überblick *Poeche*, Stichwort "Versetzung", in: Küttner, Personalbuch 2020, Rn. 2 ff. m.w.N.

1321 Zur Erforderlichkeit im Sinne von Art. 22 Abs. 2 lit. a DSGVO siehe bereits ausführlich **D. § 1 V. 3. d**) **aa**).

Hingegen ist es aber zulässig, dass Versetzungsempfehlungen durch Personalsoftware vorbereitet werden und auf Grundlage eines Scorings erfolgen. Mangels rechtlicher Wirkung oder ähnlicher erheblicher Beeinträchtigung für den Betroffenen kann auch automatisiert eine Unterrichtung des Betriebsrats über den bzw. die zu versetzenden Mitarbeiter erfolgen. Dennoch bleibt es den Verantwortlichen – anders als beispielsweise im Fall des Bewerbungsverfahrens – zumutbar, die Datengrundlage zu sichten und diese zu überprüfen und auf dieser Basis die Letztentscheidung (nach positiver Rückmeldung durch den Betriebsrat) zu treffen.

(2) Betriebsverfassungsrechtlicher Kontext

Das Betriebsverfassungsrecht regelt mit § 99 Abs. 1 BetrVG die Mitbestimmungsrechte des Betriebsrats bei Versetzungen. Der Betriebsrat muss hierüber informiert werden und der geplanten Maßnahme zustimmen. Die Gründe für eine Zustimmungsverweigerung sind in § 99 Abs. 2 BetrVG abschließend aufgezählt,[1322] können jedoch durch freiwillige Betriebsvereinbarungen erweitert werden.[1323] Hierfür hat der Betriebsrat nach § 99 Abs. 3 BetrVG eine Woche Zeit. Verweigert er die Zustimmung, so muss der Arbeitgeber beim Arbeitsgericht beantragen, die Zustimmung zu ersetzen (§ 99 Abs. 4 BetrVG), in dringenden Fällen kann er die Maßnahme nach § 100 BetrVG vorläufig durchführen.

Aus betriebsverfassungsrechtlicher Sicht wäre es daher grundsätzlich möglich, dass arbeitgeberseitig die Entscheidung automatisiert gefällt und der Betriebsrat im Anschluss hiervon unterrichtet wird, bevor die Maßnahme vollzogen wird.

(3) Ergebnis

Vollständig automatisiert lassen sich Versetzungen in der Praxis mangels Erforderlichkeit nicht umsetzen. Möglich ist es aber, den Entscheidungsvorgang so weit zu automatisieren, dass auch der Betriebsrat über die geplante Maßnahme automatisch unterrichtet wird und diesem die Ergebnisse des Scoring-Verfahrens (sowie die Datengrundlage) mitgeteilt werden,

1322 Richardi/*Thüsing*, § 99 BetrVG Rn. 208.
1323 BAG, Beschl. v. 23.08.2016 – 1 ABR 22/14, NZA 2017, 194 (198 f.) Rn. 39 ff.

sodass dieser nach § 99 Abs. 1 BetrVG die Zustimmung erteilen kann.[1324] Für die endgültige Entscheidung muss aber ein menschlicher Entscheider nochmals die Datengrundlage überprüfen und auf dieser Basis den Vorschlag des Algorithmus bestätigen.

bb) Kündigungen

Dieselben Überlegungen bei der Versetzung gelten auch für die Kündigung, wobei zusätzlich die Vorgaben des Kündigungsschutzgesetzes einzuhalten sind. Zudem erfolgt die Beteiligung des Betriebsrats nach § 102 BetrVG. Eine ohne Anhörung des Betriebsrats ausgesprochene Kündigung ist unwirksam (§ 102 Abs. 1 S. 2 BetrVG).

Lediglich im Falle einer Massenentlassung könnte es zu ähnlichen Fällen wie im Bewerbungsverfahren kommen, also dass über so viele Personen auf einer breiten Basis entschieden werden muss, dass es den Verantwortlichen nicht mehr zumutbar ist, die gesamte Datenbasis noch manuell zu überblicken. Maßgeblich ist wiederum die jeweilige Betriebsgröße[1325] und die Anzahl der Entlassungen. Kündigungsschutzrechtlich handelt es sich nach § 17 Abs. 1 KSchG um eine meldepflichtige Massenentlassung, wenn in Betrieben mit 21 - 59 Arbeitnehmern innerhalb von 30 Kalendertagen mehr als 5 Arbeitnehmer entlassen werden. In diesem Fall wird man noch nicht von einer Erforderlichkeit nach Art. 22 Abs. 2 lit. a DSGVO ausgehen dürfen. Kritisch sieht dies auch in den Fällen von § 17 Abs. 1 Nr. 2 und 3, die eine Anzeigepflicht ab 6 bzw. 25 und 30 Arbeitnehmern innerhalb von 30 Tagen vorsehen.

Es sind aber Fälle denkbar, in denen eine derart große Anzahl an Arbeitnehmern entlassen werden muss, dass es in einem zumutbaren Zeitraum nicht möglich ist, die angesetzten Kriterien für die Entlassung im Detail zu überprüfen, sondern lediglich eine Plausibilitätsprüfung des Ergebnisses in Betracht kommt. In solchen (Ausnahme-)Fällen wäre eine automatisierte Einzelfallentscheidung nach Art. 22 Abs. 2 lit. a DSGVO zulässig, wobei unter Wahrung des Verhältnismäßigkeitsgrundsatzes weiterhin erforder-

---

1324 Die Zustimmung gilt nach § 99 Abs. 3 a.E. auch als erteilt, wenn der Betriebsrat sich nicht binnen einer Woche nach Unterrichtung äußert.

1325 Es gilt der Betriebsbegriff des BetrVG (§§ 1 und 4 BetrVG), vgl. APS/*Moll*, § 17 KSchG Rn. 3 Beim Vorhandensein mehrerer Betriebe ist zudem der europäische Betriebsbegriff der Massenentlassungsrichtlinie (kurz: MERL) heranzuziehen, vgl. hierzu *Kreitner/Seidel/Voelzke*, Stichwort "Massenentlassung", in: Küttner, Personalbuch 2020, Rn. 4 ff.

lich bleibt, dass so viele Daten wie möglich, zumindest aber die Plausibilität durch einen menschlichen Entscheider geprüft wird.

Bei jeder Massenentlassung müssen der Agentur für Arbeit nach § 17 Abs. 2 und 3 die Gründe für die geplanten Entlassungen, die Zahl und die Berufsgruppen der zu entlassenden Arbeitnehmer, die Zahl und die Berufsgruppen der in der Regel beschäftigten Arbeitnehmer, den Zeitraum, in dem die Entlassungen vorgenommen werden sollen sowie die vorgesehenen Kriterien für die Auswahl der zu entlassenen Arbeitnehmer mitgeteilt werden. Dem Betriebsrat müssen zusätzlich noch die für die Berechnung etwaiger Abfindungen vorgesehenen Kriterien mitgeteilt werden.

(1) Betriebsverfassungsrechtlicher Rahmen bei der Massenentlassung

Nach § 111 Nr. 1 BetrVG liegt eine Betriebsänderung vor, wenn ein Betrieb oder wesentliche Betriebsteile eingeschränkt oder stillgelegt werden.[1326] Anders als die Meldepflicht in § 17 Abs. 1 KSchG gilt § 111 BetrVG bei einer Unternehmensgröße (nicht: Betriebsgröße) von mehr als 20 wahlberechtigen Arbeitnehmer.[1327] Die ständige Rechtsprechung des Bundesarbeitsgerichts greift für die Feststellung einer Betriebsänderung nach § 111 S. 3 Nr. 1 BetrVG grundsätzlich auf die Grenzen des § 17 Abs. 1 KSchG zurück.[1328] Besondere Regelungen sind in § 112a BetrVG enthalten, wenn die geplante Betriebsänderung allein in der Entlassung von Arbeitnehmern besteht. Hiernach wird die *Erzwingbarkeit* von Sozialplänen eingeschränkt, wenn es sich um Maßnahmen des Personalabbaus handelt.[1329] Der Arbeitgeber muss jedoch weiterhin versuchen, einen Interessensausgleich herbeizuführen.[1330]

Gegenstand des Sozialplans ist der Ausgleich oder die Milderung der wirtschaftlichen Nachteile, die den Arbeitnehmern infolge der geplanten Betriebsänderung entstehen, wie sich aus der Legaldefinition in § 112

1326 Allgemein zur Betriebsänderung sowie spezifisch zu § 111 Nr. 4 und 5 bereits unter **D. § 2 II. 6.**

1327 *Fitting*, § 111 Rn. 18 f.

1328 Vgl. statt aller BAG, Urt. v. 09.11.2010 – 1 AZR 708/09, NZA 2011, 466 (467) Rn. 15 m.w.N.; Beschl. v. 28.03.2006 – 1 ABR 5/05, NZA 2006, 932 (933) Rn. 18 m.w.N.

1329 Richardi/*Annuß*, § 112a BetrVG Rn. 2.

1330 BeckOK ArbR/*Besgen*, § 112a BetrVG Rn. 2; Richardi/*Annuß*, § 112a BetrVG Rn. 2.

Abs. 1 S. 2 BetrVG ergibt. Dieser hat die Wirkung einer Betriebsvereinbarung und ist zwischen Arbeitgeber und Betriebsrat zu verhandeln.

Der Interessenausgleich regelt hingegen die organisatorische Umsetzung der Betriebsänderung und die damit verbundenen personellen Maßnahmen. Hierin sollen die Interessen des Arbeitgebers an einer wirtschaftlichen Führung des Betriebs mit denen der Arbeitnehmer am Erhalt ihrer Arbeitsplätze und -bedingungen ausgeglichen werden. Anders als der Sozialplan wirkt dieser nicht normativ.[1331]

Während der Interessensausgleich also um das Ob und Wie der Maßnahmen geht, regelt der Sozialplan nur noch den Ausgleich der sozialen Folgen. Bevor eine Selektion der zu entlassenden Mitarbeiter durch einen Algorithmus stattfinden kann, muss mit dem Betriebsrat im Rahmen eines Interessensausgleichs über Auswahlrichtlinien verhandelt werden, wobei die vier „Grunddaten" Betriebszugehörigkeit, Lebensalter, Unterhaltspflichten und Schwerbehinderung in einem erheblichen und ausgewogenen Maß berücksichtigt werden müssen. Hierzu kann ein Punktesystem dienen.[1332]

Hierfür könnten zusätzliche Daten aus dem Personalmanagementsystem, z.B. die mittels *Advanced People Analytics* gewonnen wurden, mit in die Auswahlrichtlinien einfließen. Diese könnten neben den zwingend zu berücksichtigenden Kriterien weitere Anhaltspunkte für eine sozial gerechte Auswahl liefern. Verarbeitungsgrundlage ist wiederum § 26 Abs. 1 S. 1 BDSG.

Im Anschluss an den Interessensausgleich können die dort vereinbarten Auswahlrichtlinien in das System eingearbeitet und eine Liste der zu entlassenden Mitarbeiter generiert werden, z.B. über ein Scoring-System, das alle Kriterien berücksichtigt und eine entsprechende Bewertung pro Mitarbeiter erstellt. Anstatt ausschließlich die vier „Grunddaten" zu berücksichtigen und eine entsprechende Punktezahl daraus zu berechnen, kann mittels eines Scoring-Systems eine deutlich differenziertere (und in der Regel gerechtere) Auswahl getroffen werden, die weitere Faktoren (z.B. Teamfähigkeit, wenn vorwiegend in Teams gearbeitet wird etc.) berücksichtigt. Je nach Anzahl der zu entlassenden Mitarbeiter kann es dem Arbeitgeber unzumutbar sein, alle Bewertungskriterien des Auswahlalgorithmus zu überprüfen, sondern lediglich noch eine Plausibilitätsprüfung

1331 *Schmidt*, Stichwort "Interessensausgleich", in: Küttner, Personalbuch 2020, Rn. 1 m.w.N.

1332 *Schmidt*, Stichwort "Interessensausgleich", in: Küttner, Personalbuch 2020, Rn. 5.

durchführbar sein. Bei letzterem handelte es sich dann um eine automatisierte Einzelfallentscheidung nach Art. 22 Abs. 1 DSGVO, die nach Abs. 2 lit. a DSGVO aufgrund von Erforderlichkeit gerechtfertigt sein kann. Dies ist im Einzelfall zu prüfen.

Die Ausbezahlung etwaiger im Sozialplan festgelegten Abfindungen kann hingegen ohne weiteres vollautomatisiert erfolgen, denn hier findet keine automatisierte Entscheidung mehr statt. Der Computer führt lediglich die zuvor mit dem Betriebsrat vereinbarten Regelungen aus und entscheidet nicht selbst.[1333] Beschäftigte sind bei Berechnungsfehlern dadurch geschützt, dass der Sozialplan eine normative Wirkung hat und sie somit einen unmittelbaren Rechtsanspruch aus dem Sozialplan herleiten können.

(2) Kündigungsschutzrechtliche Vorgaben

Neben den Beteiligungsvorschriften der §§ 17 ff. KSchG ist auch der individualrechtliche Kündigungsschutz der §§ 1 ff. KSchG anwendbar,[1334] sodass bei einer betriebsbedingten Kündigung – wie bei der Massenentlassung – auch eine Sozialauswahl nach § 1 Abs. 3 KSchG getroffen werden muss.[1335] Es gelten grundsätzlich dieselben vier Kernkriterien wie bei Auswahlrichtlinien im Interessensausgleich (siehe oben); anders als beim Interessensausgleich ist die Aufzählung der Kriterien jedoch abschließend, wobei dem Arbeitgeber ein Wertungsspielraum zusteht[1336]. Nach § 1 Abs. 3 S. 2 KSchG müssen jedoch solche Arbeitnehmer nicht in die Sozialauswahl miteinbezogen werden, deren Weiterbeschäftigung, insbesondere wegen ihrer Kenntnisse, Fähigkeiten und Leistungen oder zur Sicherung einer ausgewogenen Personalstruktur des Betriebs, im berechtigten betrieblichen Interesse liegt.

Die Kenntnisse beziehen sich auf das Wissen des Arbeitnehmers, die Fähigkeiten auf die sog. Soft-Skills, die nicht zwingend die Hauptleistung betreffen müssen und die Leistungen auf qualitative oder quantitative

1333 Zum Kriterium der „Entscheidung" siehe **D. § 1 V. 3. c**).

1334 BAG, Urt. v. 06.12.1973 – 2 AZR 10/73, NJW 1974, 1263; APS/*Moll*, Vor § 17 KSchG Rn. 17 m.w.N.; *Kreitner/Seidel/Voelzke*, Stichwort "Massenentlassung", in: Küttner, Personalbuch 2020, Rn. 11.

1335 *Kreitner/Seidel/Voelzke*, Stichwort "Massenentlassung", in: Küttner, Personalbuch 2020, Rn. 11.

1336 *Eisemann/Seidel/Voelzke*, Stichwort "Kündigung, betriebsbedingte", in: Küttner, Personalbuch 2020, Rn. 34 m.w.N.

Güte der geschuldeten Leistung im Vergleich zu anderen Arbeitnehmern, sofern sie sich objektivieren lassen.[1337]

Ebenfalls sind Arbeitnehmer mit einem Sonderkündigungsschutz wie beispielsweise Schwerbehinderte (§§ 85 ff. SGB IX), Schwangere und junge Mütter (§§ 99 MuSchG, 18 BEEG) sowie betriebsverfassungsrechtliche Funktionsträger[1338] von der Sozialauswahl ausgeschlossen.[1339]

Die Anwendung von *Advanced People Analytics* bzw. der Daten aus dem Personalmanagementsystem erlaubt es dem Arbeitgeber schnell und unkompliziert zu den Daten der Sozialauswahl zu kommen, wobei die Auswahl in zwei Schritten zu erfolgen hat:

In einem ersten Schritt werden all jene Arbeitnehmer ausgeschlossen, die nicht an der Sozialauswahl teilnehmen. Hierbei kann mittels APA ermittelt werden, wer die Top-Performer im jeweiligen Betrieb, somit unverzichtbar und von der Sozialauswahl ausgeschlossen sind. Die Daten aus den APA ermöglichen dem Arbeitgeber den Nachweis der betrieblichen Erforderlichkeit jener Arbeitnehmer.

Im zweiten Schritt werden die verbleibenden Arbeitnehmer anhand der in § 1 Abs. 3 S. 1 KSchG festgelegten Kriterien einer Sozialauswahl unterzogen, wobei auch das System dabei behilflich sein kann, die Wertung der einzelnen Kriterien zu bestimmen und eine sozial gerechte Liste der zu kündigenden Arbeitnehmer zu generieren. Die Ausarbeitung der Auswahlrichtlinie hat gem. § 112 Abs. 1 BetrVG ohnehin im Rahmen eines Interessensausgleichs zu erfolgen, sodass eine vollständige Automatisierung des Vorgangs ausscheidet.

(3) Ergebnis

Während automatisierte Einzelfallentscheidungen nach Art. 22 Abs. 1 DSGVO in aller Regel bei Kündigung ausgeschlossen sind, ist ein Anwendungsfall zumindest denkbar: Die Entlassung einer Vielzahl von Arbeitnehmern, insbesondere die Massenentlassung nach §§ 17 ff. KSchG. In diesem Fall kann – insbesondere bei sehr großen Betrieben – die Datengrundlage, als Basis für die Sozialauswahl und den Interessensausgleich genutzt werden soll, so groß sein, dass es den Verantwortlichen nicht zumutbar ist,

1337 APS/*Vossen*, § 1 KSchG Rn. 670 ff.
1338 Aufzählung aus *Eisemann/Seidel/Voelzke*, Stichwort "Kündigung, betriebsbedingte", in: Küttner, Personalbuch 2020, Rn. 26.
1339 BAG, Urt. v. 17.11.2005 – 6 AZR 118/05, NZA 2006, 370 (371) Rn. 17.

eine Entscheidung unter Nachprüfung der gesamten Datengrundlage zu treffen. Wird ein System eingesetzt, dass entsprechende Listen generiert, kann es bei hoher Komplexität der Auswahlkriterien und einer Vielzahl von Fällen dazu kommen, dass nur noch eine Plausibilitätsprüfung möglich ist. In einem solchen Fall liegt eine automatisierte Einzelfallentscheidung vor, die jedoch von der Ausnahme des Art. 22 Abs. 1 lit. a DSGVO erfasst und somit rechtmäßig ist.

Neben dem Sonderfall der Massenentlassung können Advanced People Analytics bei jeder betriebsbedingten Kündigung behilflich sein, entsprechende Kriterien für die Sozialauswahl festzulegen und Listen zu generieren, die dann aber noch von einem menschlichen Entscheider nachzuprüfen sind. Dennoch lässt sich durch die Feststellung z.B. der High-Performer im Unternehmen leichter die soziale Auswahl treffen und insbesondere im gerichtlichen Prozess ein Ausschluss dieser Arbeitnehmer von dieser auch nachweisen.

Keine Fall des Art. 22 Abs. 1 DSGVO stellt es mangels Entscheidung dar, wenn das System nur noch die bereits von den menschlichen Verantwortungsträgern getroffenen Entscheidungen ausführt. Klassischer Anwendungsfall hierfür wäre die Festlegung und Ausbezahlung der Abfindungshöhe nach dem Sozialplan für die einzelnen Arbeitnehmer.

III. Zusammenfassung

Im Bewerbermanagement können automatisierte Einzelfallentscheidungen im Sinne des Art. 22 Abs. 1 DSGVO bei hohen Bewerberzahlen zulässig sein. Grund hierfür ist, dass aufgrund mangelnder Kapazitäten in der HR-Abteilung bei Bewerberfluten es schlichtweg aus praktischen Gründen ausscheidet, alle Bewerbungen einzeln zu sichten. Im Sinne eines fairen Bewerbungsverfahrens, bei dem alle Bewerbungen berücksichtigt werden, kann es erforderlich sein, automatisierte Einzelfallentscheidungen einzusetzen. Ein solches Vorgehen wäre unter den o.g. Voraussetzungen auf die Ausnahme des Art. 22 Abs. 2 lit. a DSGVO zu stützen.

Etwas anderes gilt im laufenden Arbeitsverhältnis: Dort ist die Häufigkeit von für verschiedene Arbeitnehmer gleichzeitig zu treffenden Einzelfallentscheidungen deutlich geringer, sodass in aller Regel die Erforderlichkeit einer automatisierten Einzelfallentscheidung verneint werden muss. Möglich bleibt ein Automatismus, der beispielsweise automatische Vorschläge für Fortbildungsveranstaltungen an bestimmte Arbeitnehmer sendet. Mangels rechtlicher Wirkung ist dieses Szenario nicht vom Verbot

des Art. 22 Abs. 1 DSGVO erfasst und somit ohne weitere Rechtfertigung zulässig.

Allenfalls im Rahmen von Massenentlassungen könnten in laufenden Beschäftigungsverhältnissen bzw. zur Beendigung solcher automatisierte Entscheidungen zulässig sein und zwar dann, wenn die Anzahl der zu entlassenden Arbeitnehmer und zu berücksichtigenden Kriterien so hoch ist, dass eine durch den Algorithmus (bspw. auf Basis eines Scorings) generierte Vorschlagsliste nicht mehr in jedem Einzelfall durch einen menschlichen Entscheider überprüft werden kann. Dies dürfte aber einen eng begrenzten Ausnahmefall darstellen.

§ 3 Dashboards

Die Generierung von People Analytics-Daten erfolgt in vielfältiger Weise im Hintergrund, wobei hierfür verschiedene Log-Dateien von Systemen, unzählige Datenbanken (SQL, OLAP etc.) sowie ggf. verschiedene sonstige Softwaresysteme als Datengrundlage herangezogen werden. Die Ergebnisse der People Analytics werden wiederum in der integrierten Datenbank des People Analytics-Systems gespeichert oder – falls diese im Rahmen eines Personalmanagement-Systems erfolgen – im HRM-System selbst. Hierbei handelt es sich zumeist aber um Rohdaten, die in Form einer Datenbank gespeichert und zunächst „umgewandelt“[1340] werden müssen, um für den Menschen zugänglich zu sein.

Beispiel: Das IT-System speichert für die E-Mail-Auswertung das aktive Fenster des Computers und den Empfänger der E-Mail, die gerade getippt wird, alle 10 Sekunden, um eine Zeitauswertung des Arbeitstags zu ermöglichen. Im Protokoll speichert der Computer alle 10 Sekunden eine Zeile ab, beispielsweise in der Form „2020-03-26 08:03:10 E-Mail: true, Rcpt: max@mustercompany.de“.

Die Anzeige hunderter Datenbankzeilen oder Log-Dateien ist für den Mensch, der auf dieser Basis entscheiden will, kaum hilfreich. Hier benötigt es eine Abfrage (z.B. in der Abfragesprache SQL bei Datenbanken), die diese Daten aggregiert und selektiert, sodass diese in einer Form ange-

1340 Genauer: Mittels spezifischen Datenbank-Abfragen, wie SQL-Befehle, aggregiert und selektiert werden.

zeigt werden können, die auch hilfreich für den Menschen ist.[1341] Dies geschieht häufig in Form eines Dashboards.

Hiermit könnte dem Arbeitnehmer beispielsweise angezeigt werden, dass er am Tag 3 Stunden mit dem Schreiben von E-Mails verbracht hat und der E-Mail-Verkehr mit max@mustercompany.de insgesamt 45 Minuten in Anspruch genommen hat. Mit Hilfe eines Kuchendiagramms der täglichen Arbeitszeit ließe sich das beispielsweise gut darstellen.

Bei solchen Dashboards stellt sich jedoch insbesondere aus datenschutzrechtlicher Sicht die Frage, welche Kategorien von Daten an welche Empfänger (nur der Arbeitnehmer selbst [nachfolgend **I.**], die Abteilungs- oder Unternehmensleitung [**II.**]) übermittelt werden und inwiefern diese aggregiert, bzw. anonymisiert werden (müssen) (nachfolgend **III.**).

I. Persönliches Dashboard für den Arbeitnehmer

Die datenschutzrechtlich am wenigsten einschneidende Maßnahme ist jene, bei der ausschließlich der Arbeitnehmer Zugriff auf seine über die IT-Systeme gesammelten Daten bekommt und Dritte (also z.B. des Team-, Abteilungs- oder Unternehmensleiters) keine Einsicht erhalten können. Derjenige, über den die Daten gesammelt werden, behält grundsätzlich die Datenmacht, auch wenn der Arbeitgeber der Verarbeiter ist. Sichergestellt werden kann dies beispielsweise durch eine Verschlüsselung, bei welcher nur der Arbeitnehmer das Entschlüsselungskennwort hat.[1342] Dennoch handelt es sich bei diesen Daten – auch aus Sicht des Arbeitgebers als Verarbeiter – um personenbezogene Daten, auch wenn er keine Möglichkeit zum direkten Zugriff hat.[1343] Dies ergibt sich bereits aus Erwägungsgrund 26 der DSGVO.[1344]

1341 Von der Wichtigkeit einer entsprechenden Aufbereitung spricht *Jentzsch*, HR Performance 2013, 60 (61).

1342 Vgl. hierzu auch zum sog. Hashing von Daten *Voitel*, DuD 2017, 686; zu den verschiedensten Formen der Verschlüsselung kompakt im Überblick Paal/Pauly/*Martini*, Art. 32 DSGVO Rn. 34a.

1343 Siehe bereits **D. § 1 I. 4. c).**

1344 Vgl. HdbIT-DSR/*Conrad et al.*, § 22 Cloud Computing, Rn. 262 f.

1. Datenschutzrechtliche Verarbeitungsgrundlage

a) Einwilligung

Für ein Dashboard, auf welches nur der Arbeitnehmer Zugriff hat, kommt zuvorderst die Einwilligung nach Art. 6 Abs. 1 lit. a, 7 DSGVO i.V.m. § 26 Abs. 2 BDSG in Betracht. Voraussetzung ist, dass diese eindeutig, freiwillig, in informierter Weise für einen oder mehrere bestimmte Zwecke abgegeben wurde.[1345] Diese kann im Beschäftigungsverhältnis auch regelmäßig in elektronischer Form erteilt werden, wie § 26 Abs. 2 S. 3 BDSG klarstellt.

Umgesetzt werden kann dies in der Praxis in formeller Hinsicht dadurch, dass der Arbeitnehmer beim ersten Start des Dashboards und somit vor der damit verbundenen Sammlung und Verknüpfung diverser IT-Systemdaten mit seinem Benutzerprofil, in einem Anmelde- oder Registrierungsbildschirm seine Einwilligung per Mausklick abgibt. Dies ist bei elektronischen Diensten absoluter Praxisstandard, der auch im Rahmen des Arbeitsverhältnisses angewandt werden kann.

Die Besonderheit ist, dass die ansonsten im Arbeitsverhältnis eher zweifelhafte Freiwilligkeit in dieser Situation unproblematisch ist, da der Arbeitgeber auf die verschlüsselten Daten, die im Rahmen des Dashboards für den Arbeitnehmer gesammelt werden, keinen inhaltlichen Zugriff erhält, sofern eine ausreichend sichere Verschlüsselungsmethode nach dem Stand der Technik (vgl. Art. 32 Abs. 1 lit. a DSGVO) eingesetzt wird.[1346]

Für symmetrische Verschlüsselungsverfahren wird derzeit AES-128/192/256 empfohlen, wobei die Kennziffer die Bit-Länge angibt. Je höher die Bit-Länge, desto sicherer ist die Verschlüsselung. Bei asymmetrischen Versschlüsselungsverfahren wird mindestens ECIES-250, DLIES-2000, RSA 2000, curve25519, curve448 oder ECC-Brainpool empfohlen, wobei bei ECIES eine Mindestbitlänge von 384 Bit vorliegen sollte und bei RSA/DLIES 3072 Bit.

1345 Zu den materiellen Voraussetzungen der Einwilligung, siehe **D. § 1 III. 2. a) bb)**.

1346 Von den Branchenverbänden werden immer wieder aktualisierte Handreichungen zum „Stand der Technik“ herausgegeben, so z.B. aktuell *TeleTrusT - Bundesverband IT-Sicherheit e.V.*, IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum "Stand der Technik" technischer und organisatorischer Maßnahmen, <www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/2020-01_TeleTrusT_Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DEU.pdf>.

Wird mit Hashing-Verfahren gearbeitet, so sollte SHA-256/384/512 bzw. SHA3-256/384/512 verwendet werden; SHA1 und MD5 entsprechen hingegen nicht mehr dem Stand der Technik.[1347]

Selbstverständlich bedarf es bei den Verschlüsselungstechniken immer wieder Aktualisierungen, insbesondere wenn die Rechenkapazität steigt und die Algorithmen somit schneller geknackt werden können oder sich ein Algorithmus im Nachhinein als unsicher darstellt, weil eine Schwachstelle gefunden wird. Arbeitgeber müssen daher als Verantwortliche im Sinne der DSGVO den technischen Fortschritt immer beobachten und ggf. unverzüglich handeln.

Voraussetzung ist, dass ausschließlich der Arbeitnehmer das erforderliche Kennwort zur Entschlüsselung hat. Andernfalls ist die Freiwilligkeit zweifelhaft, da ein etwaiger Druck seitens des Arbeitgebers bestehen könnte, die Einwilligung zur Datenverarbeitung abzugeben, wenn dieser hierdurch ebenfalls Zugriff auf die Arbeitnehmerdaten bekommen könnte.

b) Erforderlichkeit gem. § 26 Abs. 1 S. 1 BDSG / Berechtigtes Interesse gem. Art. 6 Abs. 1 lit. f DSGVO

Im Einzelfall kann sich darüber hinaus die Frage stellen, ob eine Datenverarbeitung für das persönliche Dashboard erforderlich im Sinne von § 26 Abs. 1 S. 1 BDSG sein kann, m.a.W. dem Arbeitnehmer die Nutzung des Dashboards „aufgezwungen" werden kann. Dies kann beispielsweise dadurch geschehen, dass das Dashboard automatisch als Startseite des Browsers aufgerufen wird oder dem Arbeitnehmer täglich eine E-Mail mit einer zusammenfassenden Darstellung durch das System zugesandt wird.

Wenn der Arbeitgeber unabhängig vom Einverständnis des Arbeitnehmers möchte, dass dies in Form einer täglichen Zusammenfassung dem jeweiligen Arbeitnehmer angezeigt wird, würde die Einwilligung als Legitimationsgrundlage kein taugliches Mittel darstellen, da diese jederzeit widerrufbar ist. Der Arbeitgeber kann zwar nicht sicherstellen, dass seine Beschäftigten die Daten wirklich zur Selbstoptimierung[1348] nutzen, dennoch

---

1347 *TeleTrusT - Bundesverband IT-Sicherheit e.V.*, IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum "Stand der Technik" technischer und organisatorischer Maßnahmen, <www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/2020-01_TeleTrusT_Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DEU.pdf>, S. 25.

1348 Vgl. **C. § 4 V.**

ist die Wahrscheinlichkeit einer Kenntnisnahme und Auseinandersetzung mit den Daten wahrscheinlicher.

Da bereits die Geeignetheit unerwünschten Scorings zur Erreichung des angestrebten Ziels für zweifelhaft ist,[1349] muss dies erst recht für die Nutzung der durch das Scoring gewonnen Daten für den Arbeitnehmer gelten. Auch hier besteht die Problematik, dass die Anzeige der Daten in aller Regel nicht zur gewünschten Selbstoptimierung führt, wenn ein Arbeitnehmer solche Auswertungen – aus welchem Grund auch immer – ablehnt. Jedenfalls besteht jedoch auch hier ein milderes Mittel: Die Einholung einer Einwilligung beim Arbeitnehmer.

c) Betriebsvereinbarung

Unter den bereits getroffenen Erwägungen stellt sich die Frage, ob eine Verarbeitung auf Basis einer Betriebsvereinbarung legitimiert werden könnte oder ob der Umstand, dass die Einwilligung schnell und per Mausklick abgegeben werden kann, der Möglichkeit der Verarbeitung auf Grundlage einer Betriebsvereinbarung entgegensteht.

Auch in einer Betriebsvereinbarung müssen sich die Betriebspartner an die Datenschutzgrundsätze und somit insbesondere an die Datenminimierung bzw. Erforderlichkeit der Datenverarbeitung halten. Sie haben jedoch das Recht, per Betriebsvereinbarung eigene Legitimationstatbestände zu schaffen, die sich am Grundsatz der Erforderlichkeit orientieren bzw. die Rahmenbedingungen der Einwilligung spezifizieren.[1350]

Aufgrund der mangelnden Geeignetheit und objektiven Erforderlichkeit der Datenverarbeitung bei einem Dashboard, bei welchem ausschließlich der Beschäftigte darauf Zugriff hat, kann diese auch durch eine Betriebsvereinbarung nicht legitimiert werden. Die zweifelhafte Eignung der Datenverarbeitung zur Erreichung des erstrebten Zwecks kann hierdurch ebenfalls nicht verbessert werden; auch hier steht die Einwilligung als milderes Mittel, das das Selbstbestimmungsrecht des Betroffenen besser wahrt und gleich effektiv ist, einer Erforderlichkeit entgegen.

Möglich bleibt es aber, die Bedingungen für die Einwilligung zu konkretisieren, wobei die Grundsätze aus Art. 7 DSGVO gewahrt bleiben müssen. Es wäre also nicht möglich, die Einwilligung oder die Widerruf-

1349 Vgl. die Ausführungen unter **E. § 1 III. 2. c) dd) (2) (c)**.
1350 Hierzu siehe bereits **D. § 1 V. 2**.

lichkeit dieser (Art. 7 Abs. 3 S. 1 DSGVO) per Betriebsvereinbarung vollständig auszuschließen.[1351]

Aufgrund mangelnder Rechenkapazitäten bei einem Tochterunternehmen eines Konzerns könnte eine (Konzern-)Betriebsvereinbarung jedoch die Datenübermittlung an eine Konzernzentrale legitimieren, insbesondere, wenn es sich (wie häufig) um zentralisierte IT-Strukturen handelt. Die DSGVO kennt selbst kein ausdrückliches Konzernprivileg. Lediglich in Erwägungsgrund 48 ist festgeschrieben, dass für die Übermittlung innerhalb der Unternehmensgruppe für interne Verwaltungszwecke ein berechtigtes Interesse bestehen kann. Art. 88 Abs. 2 DSGVO fordert bei einer Konzernübermittlung entsprechende Konkretisierungen in einer Betriebsvereinbarung.[1352] Diesbezüglich können in einer Konzernbetriebsvereinbarung spezifischere Vorschriften geschaffen werden.[1353]

2. Betriebsverfassungsrechtlicher Kontext

Bei der Einführung von Dashboards hat der Betriebsrat ein Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG, da es sich um eine technische Einrichtung handelt, die geeignet ist, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.[1354] Nach § 75 Abs. 2 BetrVG hat der Betriebsrat sicherzustellen, dass der Arbeitgeber die Persönlichkeitsrechte der betroffenen Arbeitnehmer wahrt. Hierzu gehört auch sicherzustellen, dass der Arbeitgeber keinen heimlichen Zugriff auf das System erhält. Dem Betriebsrat daher auch ein Schutzauftrag hinsichtlich der Integrität und Sicherheit eines solchen Datenverarbeitungssystems.

Zur frühzeitigen und effektiven Ausübung seiner Rechte stehen dem Betriebsrat bereits in der Planungsphase nach § 90 Abs. 1 Nr. 2 BetrVG umfassende Unterrichtungs- und Beratungsrechte zu. Es müssen ihm auch die erforderlichen Unterlagen zur Beurteilung vorgelegt werden.

1351 Vgl. EuArbRK/*Franzen*, Art. 88 DSGVO Rn. 11; EuArbRK/*Franzen*, Art. 7 DSGVO Rn. 6; ferner *Körner*, NZA 2019, 1389 (1392).

1352 Dazu unten im Überblick **F. § 2 III**.

1353 Die Diskussion über die Reichweite solcher Vereinbarungen befindet sich jedoch noch in Kinderschuhen, vgl. *Körner*, NZA 2019, 1389 (1395); *Wurzberger*, ZD 2017, 258 (259 f.).

1354 Trotz des Wortlauts „bestimmt" (vgl. § 87 Abs. 1 Nr. 6 BetrVG) reicht die Geeignetheit zur Überwachung nach st. Rspr. des BAG, vgl. hierzu bereits **D. § 2 II. 1. b**).

Durch Dashboards könnte der Arbeitgeber auch den Zweck verfolgen, dass das betriebliche Ordnungsverhalten beeinflusst wird.[1355] Es ist nicht erforderlich, dass der Arbeitgeber verbindliche Verhaltensrichtlinien aufstellt, um das Mitbestimmungsrecht aus § 87 Abs. 1 S. 1 BetrVG auszulösen; ausreichend ist bereits eine Beeinflussung durch arbeitgeberseitige Maßnahmen wie beispielsweise die Zurverfügungstellung eines Dashboards.

3. Anwendungsbeispiel: Office 365 & Microsoft Delve MyAnalytics

Um die abstrakten Ausführungen etwas zu veranschaulichen, wird im Folgenden kurz das Beispiel des Dashboards von Microsoft Office 365 bzw. Delve MyAnalytics beschrieben. Hierbei handelt es sich um ein Werkzeug, das mit der Anwendungssoftware „Office 365", die wohl in den meisten Unternehmen verwendet werden dürfte, mitgeliefert wird. Über die Nutzung von vernetzten Cloud- und Online-Diensten wird es dem sog. Office Graph, einem selbstlernenden Algorithmus aus dem KI-Bereich, ermöglicht, die Arbeit von Personen, ihren Beziehungen und Interkationen untereinander zu analysieren. Durch diese Analysen können nicht nur die Beziehungen und Interaktionen der Nutzer untereinander (siehe hierzu nachfolgend **§ 4**), sondern auch das Nutzungsverhalten von Programmen und Dokumenten aufgezeigt werden sowie Prognosen darüber getroffen werden, wer besonders „produktiv" ist und in welchen Bereichen verbessert werden kann oder welche Dokumente für welche Arbeitnehmer von Interesse sein könnten. MyAnalytics stellt dem Arbeitnehmer dar, wie und wofür die Arbeitszeit genutzt wurde, also wie viel Zeit in Meetings und dem Verfassen von E-Mails verbracht werden, wieviel Zeit des Tages wirkliche „Focustime" ist und wieviel ein Arbeitnehmer nach Feierabend arbeitet. Ebenfalls gibt MyAnalytics Vorschläge, wenn ineffiziente Meetings besucht werden (z.B. solche die viele Teilnehmer haben, länger als 60 Minuten dauern und in regelmäßigen Abständen wiederkehren)[1356] und gibt

1355 Siehe hierzu **D. § 2 II. 1. a**).

1356 Vgl. *Knapp*, Delve Analytics - Ich weiß wer du bist, weißt du's?, 12.11.2015, abrufbar unter: https://www.brandmysharepoint.de/delve-analytics-ich-weiss-wer-du-bist-weisst-dus/ (letzter Abruf am: 31.03.2020).

Rückmeldungen, welche Mails relevant sind und mit wem häufig und intensiv zusammengearbeitet wird.[1357]

Microsoft verfolgt zwar nicht standardmäßig den hier für notwendig erachteten Ansatz der Einwilligung bei Self-Analytics,[1358] lässt sich jedoch so durch den Administrator konfigurieren, dass sich Benutzer selbst aktiv dafür anmelden müssen. Ebenfalls wird auf der Datenschutz-Informationswebsite von Microsoft klargestellt, dass MyAnalytics nicht für die Bewertung, Überwachung, automatische Entscheidungsfindung, Profilerstellung oder Überwachung von Mitarbeitern vorgesehen ist, sondern lediglich einzelnen Personen der Einblick in ihre eigenen Statistiken gewährt wird. Auch ein Zugriff auf Informationen von anderen Kollegen wird unterbunden. Die Daten werden dazu im Exchange-Online-Postfach[1359] des jeweiligen Mitarbeiters gespeichert, sodass diese vor Zugriffen von Dritten geschützt sind.

Den Arbeitnehmern steht zudem frei, welche Daten sie in die Analytics miteinbeziehen wollen, also ob lediglich Postfachdaten (E-Mail, Kalender, Chat- oder Anrufaktivitäten) oder auch Windows 10-Aktivitätsveraufsdaten (welche Anwendungen und Apps werden auf welchen Geräten verwendet) oder inkrementelle Daten (z.B. grober Anteil gelesener E-Mails[1360]) verwendet werden sollen.[1361]

Ohne nun die technischen Details dieser Softwarelösung zu analysieren, darf grundsätzlich davon ausgegangen werden, dass unter den bisher genannten Gesichtspunkten diese Form der Analytics eine grundsätzlich datenschutzkonforme Umsetzung darstellen. Voraussetzung ist selbstver-

---

1357 Eine kurze Analyse der Analyticsmöglichkeiten von Office 365 gibt *Hanke*, Datenschutzprobleme und Gestaltungsmöglichkeiten in der Praxis, 2018, abrufbar unter: https://www.arbeitnehmerkammer.de/fileadmin/user_upload/Veranstaltungen/Veranstaltungsdokumentation/Downloads/Datenschutzrecht_20180221_Hanke.pdf (letzter Abruf am: 31.03.2020).

1358 Dies widerspricht zwar dem Grundsatz „Privacy by Default" (Art. 25 DSGVO), dieser Grundsatz trifft jedoch grundsätzlich den Verantwortlichen, der das Produkt einsetzen möchte, also vornehmlich den Arbeitgeber.

1359 Das ist der E-Mail-Server von Microsoft; die Daten unterliegen hier einem besonderen Schutz vor Zugriffen Dritter.

1360 Es werden keine Leseraten für E-Mails, die an weniger als 5 Empfänger versandt wurden, angezeigt. Ebenso kein prozentualer Anteil, sondern lediglich, ob die Leserate über oder unter einem bestimmten Schwellenwert liegt, der von der Anzahl der E-Mail-Empfänger abhängt.

1361 Siehe das Datenschutzhandbuch für myAnalytics-Administratoren (Stand: 14.03.2020), https://docs.microsoft.com/de-de/workplace-analytics/myanalytics/overview/privacy-guide (letzter Abruf am: 31.03.2020).

ständlich, dass der Arbeitgeber das Modell der Einwilligung wählt und kein persönlicher Druck aufgebaut wird, sich für myAnalytics anzumelden, da es ansonsten an der Freiwilligkeit mangeln würde und eine Einwilligung daher unwirksam wäre.

II. Dashboard mit Zugriff auf Informationen der einzelnen Arbeitnehmer

Anders als das individuelle Dashboard für den Arbeitnehmer, das durch eine Einwilligung problemlos legitimiert werden kann, birgt ein Dashboard für Vorgesetzte oder Teams mit Zugriff auf Informationen der einzelnen Arbeitnehmer aus datenschutzrechtlicher Perspektive ein größeres Risikopotential. Insbesondere besteht eine große Gefahr der Überwachung, wenn Verhaltens- und Leistungsdaten minutengenau und mit maximaler Detailtiefe durch Vorgesetzte überwacht werden können.

Vielerorts werden bereits (insbesondere im HR-Bereich) Dashboards eingesetzt, um einen Überblick über die Arbeitnehmer zu erhalten. Solange es sich bei den angezeigten und analysierten Daten um Stammdaten handelt und keine Überwachung ausgelöst wird, ist dies datenschutzrechtlich mit Bezug auf *People Analytics* unproblematisch.[1362] De facto ist es dieselbe Situation, wie wenn der Personalverantwortliche in die Akte blicken würde – in diesem Fall lediglich in digitaler Form.

Moderne Lösungen gehen jedoch weiter und ermöglichen auch eine Verhaltens- und Leistungsüberwachung auf Team-/Abteilungs- oder Unternehmensebene in diversen Abstufungen.

Es muss daher grundsätzlich zwischen zwei verschiedenen Dashboard-Typen unterschieden werden. Einerseits (nachfolgend **1.**) solche Dashboards, die nur die digitale Personalakte darstellen sowie andererseits „Überwachungsdashboards" mit unterschiedlicher Detailtiefe (nachfolgend **2.**). Während erstere keine Neuigkeit darstellen, sondern im Rahmen von Personalmanagementsystemen bereits seit Jahrzenten angewandt werden, gewinnen zweitere hauptsächlich mit dem Aufkommen von *Advanced People Analytics* an Popularität. Diese ermöglichen eine Leistungs- und Verhaltenserfassung und -bewertung in Echtzeit und eröffnen Verantwortungsträgern die Option, auf dynamische Veränderungen im Unternehmen flexibel und schnell zu reagieren.

1362 Siehe die diesbezüglichen Ausführungen zu Simple People Analytics, **E. § 1 III. 1.**

In beiden Varianten scheidet in aller Regel die Einwilligung mangels Freiwilligkeit aus, da nicht ausschließlich gleichgelagerte Interessen verfolgt werden bzw. kein Vorteil für den Arbeitnehmer entsteht, sondern er vielmehr negative Folgen daraus zu befürchten hat.[1363]

1. Dashboard für den HR-Bereich ohne kontinuierliche Erfassung von Leistungsdaten (vor allem Stammdaten)

Wie bereits angedeutet, handelt es sich beim Dashboard ohne Leistungsdatenerfassung um eine datenschutzrechtlich weitgehend unproblematische Digitalisierung der Personalakte, die kein People Analytics-spezifisches Problem ist. Es wird daher im Folgenden nur kurz am Rande auf etwaige Problembereiche bei der Digitalisierung hingewiesen. Zwar werden bereits in klassischen Personalmanagement-Systemen im Rahmen der Personalakte vielfach Simple People Analytics (siehe bereits **E. § 1 III. 1.**) angewandt; hierbei handelt es sich lediglich um die Fortschreibung von Trends. Zumeist werden die Stammdaten des Mitarbeiters, sein Kenntnis- und Wissenstand, Fortbildungen, etwaige Abmahnungen, Gehaltstabellen usw. angezeigt.

Sofern konzernweit ein HR-IT-System wie beispielsweise SAP SuccessFactors oder Workday eingesetzt wird, muss ein Erlaubnistatbestand zur Übermittlung von Daten an die Konzernzentrale oder andere Konzernunternehmen vorliegen. Nach Art. 88 Abs. 2 DSGVO lassen sich solche Übermittlungen in einer Konzernbetriebsvereinbarung regeln.[1364] Auf diese Problematik wird jedoch nicht näher eingegangen, da diese kein spezifisches Problem der Zulässigkeit von People Analytics-Systemen und -Verfahren ist.

Jedenfalls muss aber – unabhängig von etwaigen Übermittlungen – ein schlüssiges Berechtigungskonzept vorliegen, welches sicherstellt, dass nur diejenigen Arbeitnehmer Zugriff auf die Daten haben, für die ein solcher auch zur Erfüllung ihrer Aufgaben erforderlich ist. Hierüber hat der Betriebsrat, der ohnehin Mitbestimmungsrechte nach § 87 Abs. 1 Nr. 6 sowie umfassende Beratungsrechte nach § 90 Abs. 1 Nr. 2 BetrVG hat[1365], nach § 75 Abs. 2 BetrVG zu wachen.

1363 Vgl. hierzu auch **D. § 1 III. 2. a) bb) (2)**.
1364 *Lücke*, NZA 2019, 658 (666).
1365 Siehe bereits **E. § 1 IV. 1**.

2. Dashboard mit Leistungserfassung für Team- und Abteilungsleiter

Eine erweiterte Möglichkeit des Dashboards stellt Daten von Advanced People Analytics nicht nur für den konkreten Arbeitnehmer, sondern auch für die jeweils Personal- und Fachverantwortlichen dar. Dies bietet die Möglichkeit, jederzeit die Performance der eigenen Team- oder Abteilungsmitglieder einzusehen und rasch bei Fehlentwicklungen gegensteuern zu können bzw. „Top-Performer" gezielt weiter zu fördern oder Boni o.ä. zu gewähren.

Relevant ist, dass die Arbeitnehmer nicht einem dauerhaften Überwachungsdruck durch Analytics-Maßnahmen und ein damit verbundenes Monitoring ausgesetzt werden.[1366] Die Zulässigkeit solcher Maßnahmen hängt jedoch vom Einzelfall ab. So können – wie bereits unter **E. § 1 III. 2. a) cc) (4)** dargestellt – in Call-Centern sog. *Bedienerplatzreports*[1367] zulässig sein, wenn dies für eine effektive Steuerung der Arbeitsplätze notwendig ist, andererseits aber Belastungsstatistiken in der Versicherungsbranche unzulässig sein, wenn hierdurch das gesamte Arbeitsspektrum auf elektronischem Wege anhand quantitativer Kriterien durchgehend analysiert wird.[1368]

Letztlich hängt der zulässige Umfang der Datenverarbeitung insbesondere vom konkreten Zweck und der Absicherung für eine zweckfremde Verarbeitung ab. Dieser Maßstab gilt insbesondere auch für die Darstellung in Dashboards. Der jeweilige innerbetriebliche Empfänger der Daten spielt daher eine entscheidende Rolle.

Beispiel: Bei der Analyse der täglichen Bildschirmarbeitszeit durch einen (unabhängigen) Arbeitsmediziner ist die Gefahr eines individuellen Überwachungsdrucks überschaubar, wenn die Daten ausschließlich durch diesen im Rahmen von gesundheitspräventiven Maßnahmen evaluiert werden (z.B. wie viele Stunden sitzt ein konkreter Beschäftigter täglich vor dem Bildschirm). Hingegen könnte dieselbe Auswertung bei einer Anzeige für den Vorgesetzten zu einem unzulässigen Überwachungsdruck führen. Letzterer könnte aus der Zeitangabe schlussfolgern, dass bestimmte Arbeitnehmer zu wenig arbeiten und daraus personelle Maßnahmen herleiten.

Ebenso kann die Darstellung von Team-Leistungsdaten für den Teamleiter zur Koordinierung des Teams erforderlich sein, nicht hingegen auf

1366 Diesbezüglich gelten dieselben Voraussetzungen wie unter **E. § 1 III. 2. a) cc) (4)** dargestellt.

1367 BAG, Beschl. v. 30.08.1995 – 1 ABR 4/95, NZA 1996, 218.

1368 BAG, Beschl. v. 25.04.2017 – 1 ABR 46/15, NZA 2017, 1205.

dieser detaillierten Basis für den Abteilungsleiter; für letzteren reichen i.d.R. aggregierte Daten auf Team-Ebene aus, um wiederum die Teams zu koordinieren.

Es ist zu beachten, dass der Arbeitnehmer in bestimmte Datenverarbeitungen (z.B. im Beispiel in die Auswertung durch den Arbeitsmediziner) einwilligen kann, da in Situationen, in denen dem Arbeitnehmer lediglich Vorteile aus der Einwilligung erwachsen oder gleichgelagerte Interessen verfolgt werden, eine Freiwilligkeit nach § 26 Abs. 2 S. 2 Alt. 2 BDSG vermutet wird.[1369] Dieselbe Darstellung könnte bei einem anderen Empfänger (selbst wenn sie demselben Zweck diente) jedoch zu hohen Zweifeln an der Freiwilligkeit führen (z.B., wenn die Einwilligung zur Darstellung beim Vorgesetzten erfolgt). Bei letzterem könnte sich der Arbeitnehmer genötigt fühlen, die Einwilligung abzugeben, um keine Repressalien befürchten zu müssen.

Die Leistungsüberwachung mittels Dashboards ist nicht ausgeschlossen, wenn hierdurch kein Überwachungs- und Anpassungsdruck erzeugt wird. Dies wäre beispielsweise der Fall, wenn monatliche Leistungsbeurteilungen durch den Vorgesetzten erfolgen oder bestimmte Ziele zu Monatsbeginn vereinbart werden und am Ende des Monats überprüft wird, inwiefern diese Ziele durch die jeweiligen Arbeitnehmer eingehalten wurden. Letzteres könnte in elektronischem Wege erfolgen, wenn zu Monatsbeginn bestimmte Aufgaben verteilt werden und der laufende Fortschritt betreffend diese vereinbarten Ziele hierbei verfolgt wird (z.B. im Rahmen von Projekten). Zum Monatsende könnte eine Auswertung erfolgen, welche der vereinbarten Ziele inwieweit erreicht wurden. Anders als im unter Ziff. **E. § 1 III. 2. a**) **cc**) (**4**) dargestellten Beispiel werden durch diese (Projekt-)Fortschrittsüberwachung nicht alle wesentlichen Aspekte in quantitativer und qualitativer Hinsicht überwacht, sondern es erfolgt lediglich eine deutlich weniger detaillierte Überwachung der einzelnen Arbeitsabschnitte. Insbesondere bei zeitkritischen Projekten ist dies ohnehin notwendig, um bei eventuellen Problemen oder prognostizierten Engpässen schnell und flexibel reagieren zu können, z.B. indem ein weiterer Arbeitnehmer ins Team genommen wird. Eine solche Datenverarbeitung wäre erforderlich und verhältnismäßig für die Durchführung des Beschäftigungsverhältnisses nach § 26 Abs. 1 S. 1 BDSG.

Klar ist auch, dass dieses Beispiel nicht auf jeden Arbeitsplatz und Arbeitnehmer übertragbar ist, sondern nur dort, wo die Arbeit mit vorgege-

---

1369 Zum Kriterium der Freiwilligkeit der Einwilligung, siehe auch **D. § 1 III. 2. a**) **bb**) (**2**).

benen Arbeitszielen möglich ist. Dies ist jeweils im Einzelfall zu beurteilen. Insbesondere dort, wo projektbezogen mit klaren Zeitvorgaben (z.B. bei SCRUM-Projekten[1370]) gearbeitet wird oder ohnehin eine dauernde Erfassung von Arbeitsvorgängen erforderlich ist (z.B. in der Logistik) und Arbeitnehmer mit einer Überwachung der Kennzahlen rechnen müssen, erzeugen solche Maßnahmen keinen unzulässigen Überwachungsdruck und sind daher als zulässig zu erachten, soweit für die Leistungsbeurteilung keine weiteren Daten hiermit verknüpft werden, um ein detaillierteres Abbild des Beschäftigten zu bekommen.

Bei den innerbetrieblichen Empfängern muss darauf geachtet werden, dass ein Zugriff auf diese Daten ebenso nur im Rahmen der Erforderlichkeit möglich ist.

Aus betriebsverfassungsrechtlicher Hinsicht gelten dieselben Maßstäbe wie bei Advanced People Analytics, d.h. der Betriebsrat hat zwingende Mitbestimmungsrechte aus § 87 Abs. 1 Nr. 6 BetrVG hinsichtlich der zugrundeliegenden Datenerfassung; ggf. auch aus § 87 Abs. 1 Nr. 1 BetrVG, wenn nicht nur das Leistungsverhalten untersucht wird. Wird die Gestaltung der Lohnstruktur daran angeknüpft, so können auch Mitbestimmungsrechte aus § 87 Abs. 1 Nr. 10 und 11 BetrVG entstehen.[1371] Darüber hinaus besteht eine Unterrichtungs- und Beratungspflicht nach § 92 Abs. 1 BetrVG, da es sich insofern auch um Personalplanungsmaßnahmen i.w.S. handelt.[1372]

Aufgrund diverser Mitbestimmungsrechte und der Pflicht, mit dem Betriebsrat zu verhandeln, empfiehlt es sich dringend, konkretisierende („*spezifischere*“) Regelungen zu Dashboards in Betriebsvereinbarungen zu treffen. Hierdurch können die Unsicherheiten, die bei einer Anwendung von § 26 Abs. 1 S. 1 BDSG bestehen (Inwiefern sind die Daten erforderlich? Welche Empfänger benötigen die Daten? Ab welcher Ebene muss aggregiert werden? Ab welcher Aggregationsebene kann von einer Anonymität im Unternehmen ausgegangen werden?), vermieden werden. All diese Fragen lassen sich in einer Betriebsvereinbarung, die legitimierend für die Datenverarbeitung ist, regeln.

1370 Hier erfolgen einzelne „Sprints“ mit täglichen Besprechungen der Mitglieder. In jedem „Sprint“ werden Ziele festgelegt, die bis zu einem bestimmten Termin erledigt sein müssen, vgl. zur dieser Methode der Projektarbeit HdbIT-DSR/*Sarre*, § 1 Erstellung und Pflege von Software, Rn. 60.

1371 Hierzu siehe bereits oben **D. § 2 II. 1. c**).

1372 Siehe **D. § 2 II. 4**.

III. Dashboard mit Zugriff auf aggregierte Daten (Team-, Abteilungsebene)

Die dritte und datenschutzrechtlich weniger bedenkliche Maßnahme ist die Anzeige von aggregierten Daten z.B. auf Team- oder Abteilungsebene. Für diese Daten ist nach dem legitimationsbedürftigen Anonymisierungsvorgang[1373] und dem ggf. vorzunehmenden Kompatibilitätstest kein Datenschutzrecht mehr anwendbar, sodass der Verarbeiter die Daten nach freiem Belieben verarbeiten darf.

1. Notwendigkeit einer wirksamen Anonymisierung und k-Anonymität

Das Kernproblem, das sich hier stellt, ist allerdings die wirksame *Anonymisierung* der Daten.[1374] Die für solche Dashboards vorgenommene Anonymisierungstechnik ist die Aggregation von Daten. Eine solche liegt vor, wenn aus bestimmten Einzeldaten Durchschnittswerte gebildet oder diese durch allgemein gehaltene Aussagen (Merkmalsaggregation) ersetzt werden.[1375]

Beispiel: Wenn auf der Dashboard-Ebene die (expliziten) Identifizierungsmerkmale nicht angezeigt werden, hingegen aber die dafür beispielsweise Arbeitszeit des letzten Arbeitstages, wäre es für einen Teamleiter recht einfach festzustellen, von welchem Teammitglied diese Daten sind. In diesem Fall lägen weiterhin personenbezogene Daten vor. Etwas anderes gälte dann, wenn lediglich die durchschnittliche Arbeitszeit des Teams angezeigt wird. Selbst Ausreißer in den Daten wären in der Folge nicht mehr einer Person zuordenbar.

Als möglichen Anwendungsfall für die Merkmalsaggregation kann ein interdisziplinäres Team angeführt werden, in welchem zwei Programmierer, drei im IT-Endlevel-Support, eine Person im Marketing, eine weitere im Bereich Buchhaltung sowie ein Manager als Teamleiter arbeitet. Unterteilt man diese Personen in „IT-Personen“ und „Nicht-IT-Personen“, so sind die Merkmale derart aggregiert, dass eine Zuordnung zu Einzelpersonen nicht mehr möglich ist. Wird hingegen eine detaillierte Aggregation vorgenommen, z.B. nach Unternehmensbereichen, wären der Marketer, der Buchhalter und der Manager identifizierbar.

1373 Hierzu bereits **E. § 1 III. 1. b) aa)**.
1374 Grundlegend **D. § 1 I. 4. b)**.
1375 Vgl. *Dammann*, in: Simitis, Bundesdatenschutzgesetz, § 3 BDSG Rn. 207.

Diskutiert wird dies unter dem Stichwort der *k-Anonymität*.[1376] Dieser Faktor beschreibt die Anzahl der Personen, die dasselbe Merkmal haben müssen, sodass diese nicht als „Ausreißer" in den Daten identifiziert werden können. Eine höhere k-Anonymität kann beispielsweise durch die Vergrößerung bestimmter Intervalle erzielt werden.

Beispiel: Im Unternehmen soll eine Klassifizierung nach Gehaltsebenen erfolgen. Werden die Intervalle zu klein gehalten (30.000 – 30.500 Euro Jahresgehalt statt 30.000 – 35.000 Euro), könnte dies dazu führen, dass Beschäftigte hierdurch identifiziert werden, obwohl es zunächst den Anschein macht, dass anonyme Daten vorliegen. Eine Anonymisierung ließe sich durch Erhöhung des Intervalls herbeiführen.

Gefahrpotential entsteht insbesondere durch den Einsatz von Big Data, wenn beispielsweise eine Verlinkung mehrerer Datensätze erfolgt. Obwohl bestimmte Merkmale auf aggregierter Basis (mit dort ausreichendem k-Faktor) vorliegen, könnte eine Identifizierung einzelner Beschäftigter stattfinden.

Beispiel: Ein Arbeitgeber versucht Anonymität herzustellen, indem er die Datensätze aggregiert speichert und keine personenbezogenen Daten in der Datenbank ablegt. Es werden folgende Datensätze gespeichert:

Hausmeister in der Gehaltsspanne 30.000 – 40.000 Euro:	mittlere Leistung
Hausmeister in der Gehaltsspanne 50.000 – 60.000 Euro:	hohe Leistung
Außenbereichspflege in der Gehaltspanne 30.000 – 40.000 Euro:	mittlere Leistung
Außenbereichspflege in der Gehaltsspanne 50.000 – 60.000 Euro:	hohe Leistung

Auf den ersten Blick wirken diese Daten anonym und können beispielsweise die Erkenntnis bringen, dass ein höheres Gehalt zu einer höheren Leistung führt. Angenommen, es befindet sich nur ein Hausmeister „XY" in der Gehaltsspanne 50.000 – 60.000 Euro, so wäre die Angabe „hohe Leistung" ein zwar pseudonymisiertes, aber personenbezogenes Datum über XY. Wären die Tätigkeitsbereiche nicht mit der Gehaltsspanne verknüpft gespeichert worden, so läge eine höhere k-Anonymität vor, da die Personen der Außenbereichspflege ebenfalls miteinbezogen worden wären:

Leistung in der Gehaltsspanne 30.000 – 40.000 Euro:	mittel
Leistung in der Gehaltsspanne 50.000 – 60.000 Euro:	hoch

1376 *Article 29 Data Protection Working Party*, Opinion 05/2014 on Anonymization Techniques (WP 216), S. 16.

Eine direkte Zuordnung hätte daher nicht mehr erfolgen können, insbesondere wenn die Angabe der Leistung lediglich einen Durchschnittswert vieler Arbeitnehmer darstellt. Es hätte dann nicht mehr eruiert werden können, ob nun der einzelne Hausmeister in dieser Gehaltsspanne eine hohe oder niedrige Leistung erbringt.

Es zeigt sich an diesem Beispiel: Je mehr Merkmale in den Datensätzen vorhanden sind, die eine Zuordnung erlauben, desto höher ist eine Wahrscheinlichkeit der Identifizierung einer einzelnen Person.

Bei der Speicherung von solchen Daten muss also darauf geachtet werden, dass die jeweiligen k-Faktoren so hoch sind, dass durch eine Verknüpfung der Merkmale keine Identifizierbarkeit hergestellt werden kann. Eine Lösung könnte sein, die jeweiligen Faktoren individuell abzuspeichern und nicht zu verknüpfen. Im obigen Beispiel wäre es für die Berechnung der Durchschnittsleistung in einer gewissen Gehaltsspanne nicht erforderlich, dass die Daten mit dem Tätigkeitsbereich verbunden gespeichert werden.

Im dem weiter oben Beispiel von Microsoft MyAnalytics werden z.B. die Leseraten von E-Mails in zweifacher Hinsicht anonymisiert: Einerseits erfolgt ein Rendering der Leserate in die Kategorien „hoch" und „niedrig" statt der Angabe von Prozentzahlen, andererseits wird eine solche nicht angezeigt, wenn nicht mindestens fünf Empfänger die Nachricht erhalten haben (dies ist wieder ein Anhaltspunkt zur sog. k-Anonymität).[1377]

Die k-Anonymität ist nur ein mögliches Modell, die Bestimmbarkeit und somit die Anwendung des Datenschutzrechts auszuschließen.[1378] Für die Anwendbarkeit der DSGVO kommt es aber nicht darauf an, dass ein bestimmter k-Faktor vorliegt, sondern dass unter „vernünftigerweise" angewandten Mitteln zur Identifizierung eine Bestimmbarkeit ausgeschlossen ist (Erwägungsgrund 26).[1379] Für die Bewertung ist maßgeblich, wie hoch die Wahrscheinlichkeit einer erfolgreichen Re-Identifizierung einer Person ist. Ist dieses vernachlässigbar, weil es so gering ist, dann sind die Daten nicht personenbezogen und die DSGVO findet keine Anwendung.[1380]

1377 Vgl. https://docs.microsoft.com/de-de/workplace-analytics/myanalytics/overview/privacy-guide (letzter Abruf am: 16.04.2020) unter der Überschrift „Leseraten von E-Mails".

1378 Weitere Modelle zeigt *Götz*, Big Data im Personalmanagement, S. 75 auf.

1379 Zur Auslegung des Begriffs „vernünftigerweise" siehe bereits **D. § 1 I. 4. c) bb) (1)** unter dem Aspekt der Pseudonymisierung.

1380 Vgl. hierzu noch unter altem Datenschutzrecht *Brisch/Pieper*, CR 2015, 724 (727).

2. Risikobasierter Ansatz der DSGVO: Re-Identifizierungsrisiko

Ein weiterer Faktor ist das Geheimhaltungsinteresse der betroffenen Personen bzw. das Interesse Dritter an der Kenntnis bestimmter Informationen sowie Zugriffsmöglichkeiten, die das Re-Identifikationsrisiko bestimmen. Je unwichtiger die Daten und je kleiner der Zugriffskreis, desto eher sind Informationen anonym.

Beispiel: Während wohl wenig Aufwand betrieben wird, einzelne Personen herauszufiltern, wenn Gehaltsspannen in einem Unternehmen für Personengruppen veröffentlicht werden, wären die Geschäftskontakte hochrangiger Manager sicherlich höher gefährdet. Noch extremer ist es, wenn (abseits der People Analytics) beispielsweise Geheimdienstinformationen im Internet veröffentlicht werden.

Es zeigt sich bei diesen Beispielen deutlich der risikobasierte Ansatz der DSGVO.[1381] Dieser schlägt sich auch beim Risiko der Re-Identifizierung beim Einsatz von Big Data-Technologien nieder; wenn kein hohes Interesse an der Identifikation von Arbeitnehmern besteht, muss der Arbeitgeber auch nicht gezielt Schutzmaßnahmen vor solchen Technologien implementieren.

3. Betriebsverfassungsrechtlicher Kontext

Obwohl anonyme Daten vorliegen, dürfen betriebsverfassungsrechtliche Mitbestimmungsrechte nicht außer Betracht bleiben: Der Betriebsrat hat ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG, auch wenn nur anonyme Daten erfasst werden, denn das Mitbestimmungsrecht soll gerade auch den Datenschutz und die Persönlichkeitsrechte der Arbeitnehmer schützen und darauf hinwirken, dass Arbeitgeber wirksame Anonymisierungstechniken einsetzen.[1382] Sollen die genannten Daten genutzt werden, um das Verhalten von Arbeitnehmern im Betrieb zu beeinflussen, so hat der Betriebsrat auch nach § 87 Abs. 1 Nr. 1 BetrVG mitbestimmen.

Informations- und Beratungspflichten aus § 92 BetrVG verpflichten den Arbeitgeber den Betriebsrat bereits bei der Planung miteinzubeziehen, auch wenn nicht mit personenbezogenen Daten gearbeitet wird. Letztlich

---

1381 Hierzu bereits **E. § 1 I. 2. d) ee)** sowie **E. § 1 III. 2. b) (2)**; ferner *Veil*, ZD 2015, 347.

1382 Zum Schutzzweck von § 87 Abs. 1 Nr. 6 BetrVG, siehe **D. § 2 II. 1. b)**.

sollen die Statistiken dem Arbeitgeber dazu dienen, seine Personalmaßnahmen zu optimieren.

Unabhängig hiervon hat der Betriebsrat auch ein Mitbestimmungsrecht aus § 90 Abs. 1 Nr. 2 BetrVG, da solche Dashboards auch eine technische Anlage darstellen. Ob daneben auch eine Betriebsänderung nach § 111 S. 3 Nr. 5 BetrVG vorliegt, hängt von der Auswirkung der erweiterten anonymen Analysen auf die Arbeitsplätze und den Arbeitsablauf ab.[1383]

IV. Zusammenfassung

Dashboards stellen ein wichtiges Mittel zur Visualisierung der Ergebnisse aus den People Analytics dar. Da die (weiter oben dargestellten) Analysen lediglich Rohergebnisse liefern, die erst noch ein einem weiteren Verarbeitungsvorgang für die jeweiligen Endanwender aufgearbeitet und dargestellt werden müssen, sind diese in der datenschutz- und betriebsverfassungsrechtlichen Prüfung gesondert zu betrachten. Insgesamt gibt es drei Ebenen, die jeweils gesonderte Verarbeitungsvorgänge darstellen und einzeln bewertet werden müssen: (1) Die Erhebung der Daten durch IT-Systeme oder manuelle Eingaben von Daten durch Beschäftigte. (2) Die Analysen durch People Analytics-Systeme/-Maßnahmen, die die Rohdaten auswerten und hieraus weitere Erkenntnisse für das Management erzielen; sowie (3), die Umwandlung der Ergebnisse der Analysen in ein benutzerfreundliches Format – meist anhand von Dashboards über Web- oder Mobile-Applications, mit der Möglichkeit der Zusammenfassung und Aggregation von Daten, genauso wie – vereinzelt – der detailgenauen Betrachtung von Einzelergebnissen aus den Auswertungen, z.B. wenn der Teamleiter auf dem Übersichtsdashboard feststellt, dass die Teamleistung in dieser Woche gesunken ist und der Veränderung auf den Grund gehen möchte.

Dashboards sind eng verknüpft mit den zugrundeliegenden People Analytics-Auswertungen. Möglich ist es aber in diesem Zusammenhang, dass die Analysesoftware von einem Hersteller stammt, der mittels einer API[1384]

1383 Vgl. zu den Mitbestimmungsrechten (bei Advanced People Analytics) bereits **E. § 1 IV. 2.**

1384 „Application Programming Interface“, eine Anwendungs-Programmierschnittstelle, die einen standardisierten und veröffentlichten Zugriff auf das System ermöglicht, um weitere Anwendungen auf Basis des technischen Systems zu erstellen, vgl. auch *Fischer/Hofer*, Lexikon der Informatik, S. 45 Stichwort "API"; siehe aus der juristischen Literatur auch *Janik*, in: Geppert/Schütz,

die Auswertung durch andere Softwares ermöglicht. So könnte sich ein Unternehmen dafür entscheiden, ein anderes Dashboard einzusetzen als jenes, das vom Hersteller der PA-Software zur Verfügung gestellt wird (beispielsweise, weil es einfacher zu bedienen oder übersichtlicher ist). In solchen Fällen muss der Verwender der Software dann auch darauf achten, dass die Dashboard-Software den Datenschutzbestimmungen entspricht (insbesondere betreffend die Datensicherheit).

§ 4 Netzwerk-Graphen / Netzwerkanalysen

Eine besondere Art der Darstellung von Daten aus People Analytics stellen sog. Netzwerk-Graphen und Netzwerkanalysen dar. Auch solche werden grundsätzlich in Dashboards dargestellt, erfüllen aber einen anderen Zweck und geben deutlich vertieftere Blicke in die Arbeitnehmerstruktur, weshalb diesen in dieser Arbeit ein eigener Abschnitt gewidmet werden soll.

Durch die Digitalisierung der Arbeit und die konstante Erfassung von Systemdaten durch die eingesetzten Systeme (automatische Speicherungen z.B. durch Textverarbeitungssoftware in der Cloud, Auswertungen von Kollaborationslösungen wie Microsoft Teams oder Slack, Verbindungsdaten von Telefonanlagen, innerbetriebliche soziale Netzwerke wie Facebook Business oder Yammer) ist die „Vermessung der Belegschaft“[1385] möglich geworden.

People Analytics sind ein Teil dieser Vermessungsmöglichkeiten und werden immer breitflächiger eingesetzt. Der *Enterprise Social Graph* ist eine andere Form der Auswertung, die sich auf die innerbetrieblichen Kommunikationswege fokussiert und die Verbindungen zwischen einzelnen Aktoren im Netzwerk „Unternehmen“ analysiert. Hierdurch können Personen in Schlüsselpositionen sowie wichtige Kommunikationswege und -probleme identifiziert werden.[1386] Die organisatorische Netzwerkanalyse gehört ebenfalls zum breiten Themenfeld der People Analytics.

Mithilfe solcher Auswertungen lässt sich insbesondere feststellen, wo Vertrauen in Organisationen besteht und wer die Träger der Unterneh-

---

Beck'scher TKG-Kommentar, § 48 TKG Rn. 17 (allerdings spezifisch zu APIs bei Fernsehgeräten).

1385 So auch der Titel der Ausarbeitung zu diesem Thema von *Höller/Wedde*, Die Vermessung der Belegschaft.

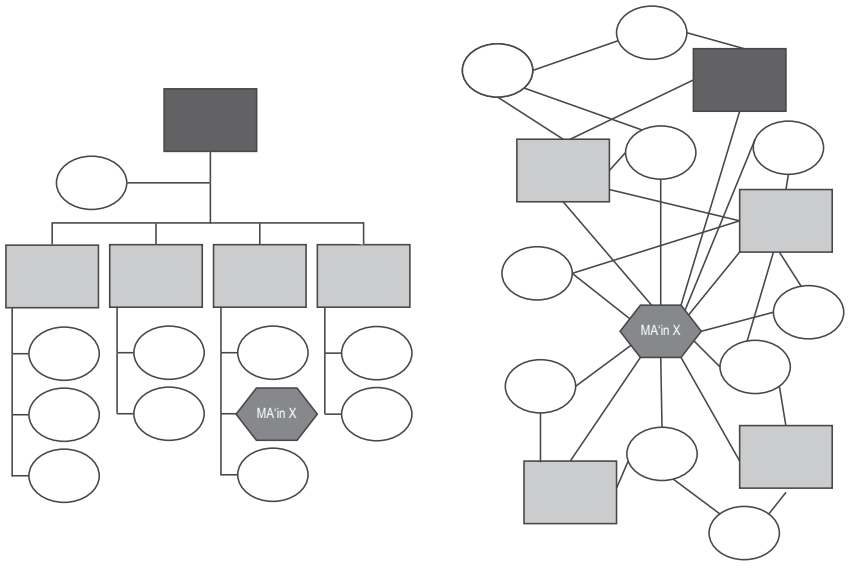
1386 Vgl. *Höller/Wedde*, Die Vermessung der Belegschaft, S. 10 ff.

menskultur sind. Dies hilft Unternehmen festzustellen, an welcher Stelle Innovation, Kreativität und Prozesse unterstützt oder behindert werden.[1387] Deutlich sichtbar wird in solchen Analysen, dass es neben der formellen Organisation (Hierarchie) auch noch eine informelle gibt und die Kommunikation nicht streng entlang von Hierarchielinien verläuft, sondern auch oftmals direkt zwischen den Wissensträgern (umso mehr, je schlechter eine Hierarchiestruktur funktioniert).

Beispiel: Eine Mitarbeiterin (X) befindet sich in der Hierarchiestruktur am unteren Ende und hat daher niemanden unter sich. Nach der formellen Organisation würde sie sich somit am Ende der Kommunikationskette befinden; Kommunikationswege nach formeller Struktur würden daher über den Vorgesetzten nach oben verlaufen und über andere Vorgesetzte wieder nach unten zu anderen Arbeitnehmern. Nach einer Analyse des unternehmensinternen Kommunikationsnetzes ergibt sich allerdings, dass X sich im Mittelpunkt jeglicher Kommunikationswege befindet, die Kommunikation also nicht über die formelle Struktur erfolgt, sondern sich die Arbeitnehmer anderer Hierarchiebäume direkt an sie wenden.

1387 *Thiel*, Organisationsentwicklung 2010, 78 (79).

Abbildung 2: Formelle vs. informelle Organisation (angelehnt an Thiel 2010, S. 80 Abbildung 2)



Dieses Beispiel zeigt, dass die Mitarbeiterin X wohl hohe Kompetenz und/oder Vertrauen bei anderen Arbeitnehmern besitzt, obwohl aus der formalen Hierarchiestruktur zwar auf den ersten Blick der (Fehl-)Schluss gezogen werden könnte, dass sie am unteren Ende der Kette entbehrlich ist. Aus der informellen Struktur ergibt sich aber, dass sie trotz ihrer niedrigen Hierarchieposition das wichtigste Kettenglied der Kommunikationswege zwischen verschiedenen Abteilungen ist. Es wäre daher ein fataler Fehler des Arbeitgebers, diese Arbeitnehmerin zu verlieren.

Würde beispielsweise die Frage gestellt werden: „Vom wem holen Sie Rat für wichtige technische Fragestellungen?“, dann zeigt das obere Diagramm, dass sowohl Linienmanager als auch Fachkräfte in erster Linie sie fragen, sie mithin eine hohe technische Kompetenz hat.[1388] Für den Arbeitgeber lohnt es also X mit einer Gehaltserhöhung, Beförderung oder sonstigen Incentives im Unternehmen zu halten, wenn sie über einen

1388 *Thiel*, Organisationsentwicklung 2010, 78 (80).

Arbeitgeberwechsel nachdenkt. Würde das Diagramm auch den Arbeitnehmern zur Verfügung gestellt, so könnte X über ihre herausragende Stellung in der Struktur Kenntnis erlangen (sofern es ihr noch nicht bewusst ist) und möglicherweise Forderungen stellen.

Solche Netzwerkgraphen können auf verschiedene Wege erzeugt werden: Einerseits ist die Erstellung eines solchen Mithilfe von (standardisierten) Fragebögen möglich (nachfolgend **I.**), andererseits können – wie im Beispiel des Office Graph – die IT-Daten ausgewertet werden, um Kommunikationswege und Kollaborationen aufzuzeigen (nachfolgend **II.**).

I. Netzwerk-Analyse anhand von (standardisierten) Fragebögen

Im „klassischen" Sinne ist eine Netzwerk-Analyse dergestalt möglich, dass den Arbeitnehmern Fragebögen ausgehändigt (oder über E-Mail oder das Intranet) zur Verfügung gestellt werden. In diesen Fragebögen werden – je nach Art der Analyse – verschiedene Fragen gestellt, um mehr über das organisationsinterne Netzwerk zu erfahren. *Thiel* listet in seiner Ausarbeitung zur sozialen Netzwerkanalyse verschiedene Netzwerktypen auf, die analysiert werden können:[1389]

Das Arbeitsnetzwerk, welches Verbindungen im Rahmen des Tagesgeschäfts abbildet („*Mit wem tauschen Sie Informationen, Dokumente oder Ressourcen im Alltagsgeschäft aus?*"), das Strategienetzwerk, das Richtungsentscheidungen aufzeigen soll („*Mit wem sprechen Sie über Zukunft und Vision der Organisation?*), das soziale Unterstützungsnetzwerk („*Mit wem sprechen Sie über Themen, die Sie sozial und beruflich in der Organisation beschäftigten?*"), das Innovationsnetzwerk („*Mit wem kommen Sie zu Diskussionen und Treffen zusammen, um neue Ideen zu entwickeln?*") sowie das Expertennetzwerk („*Von wem holen Sie sich Rat und Wissen für Ihre Arbeit?*").

1. Datenschutzrechtliche Analyse

Die Netzwerkanalyse kann nicht anhand von anonymisierten Daten stattfinden, da ansonsten die Beziehungen der einzelnen Netzwerkakteure nicht dargestellt werden können. Mithin müssen die Analysen mit personenbezogenen Daten erfolgen und unterliegen daher dem Datenschutz-

1389 *Thiel*, Organisationsentwicklung 2010, 78 (84).

recht. Es stellt sich die Frage, ob die Daten zur Durchführung des Beschäftigungsverhältnisses erforderlich sind i.S.v. § 26 Abs. 1 S. 1 BDSG.[1390]

Eine Erforderlichkeit liegt jedenfalls vor, wenn der Arbeitgeber die Daten zur Erfüllung seiner vertraglichen oder gesetzlichen Pflichten oder Wahrnehmung seiner Rechte benötigt.[1391] Diese Zweckbestimmung der „Durchführung des Arbeitsverhältnisses" ist allerdings weit zu verstehen, sodass grundsätzlich alle mit dem Arbeitsverhältnis in Zusammenhang stehenden Maßnahmen darunter zu fassen sind.[1392] Mithin auch die Netzwerkanalyse, wenn sie dem Zweck dient, die Arbeitsorganisation und somit die Durchführung des konkreten Arbeitsverhältnisses zu optimieren.

Letztlich erfolgt eine Verhältnismäßigkeitsprüfung, bei der die Interessen des Arbeitgebers an der Datenverarbeitung (hier: Kenntnis der Netzwerkstruktur(en) im Unternehmen) mit dem Geheimhaltungsinteresse bzw. Persönlichkeitsrecht der Arbeitnehmer abgewogen und in angemessenen Ausgleich gebracht werden müssen.[1393]

Bei der Analyse der Netzwerkstruktur mit Fragebögen muss darauf geachtet werden, dass das Ergebnis betriebliche Daten sind und nicht etwa private Kommunikationswege abgefragt werden („*Mit wem gehen Sie gerne in die Mittagspause? Mit wem tauschen Sie sich über private Angelegenheiten aus?*"). Bei solchen Maßnahmen überwiegt jedenfalls das Persönlichkeitsinteresse des Arbeitnehmers, da diese Daten allenfalls am Rande für das Arbeitsverhältnis von Interesse sein könnten. Hier lassen sich Parallelen unzulässigen Fragen des Arbeitgebers bei der Einstellung und zur Auswertung von privaten E-Mails herleiten, die ebenfalls aufgrund des Geheimhaltungsinteresses des Arbeitnehmers und mangelnden Bezug zum Arbeitsverhältnis unzulässig sind.

Die oben aufgezeigten Analysen stellen jedoch den betrieblichen Kontext in den Mittelpunkt, sodass das Recht auf Privatheit (bzw. Persönlichkeitsrecht) des Arbeitnehmers grundsätzlich in den Hintergrund rückt. Es stellt sich vor allem die Frage, ob diese Analysen „erforderlich" sind, es also kein milderes, gleich effektives Mittel zur Erreichung des angestrebten Ziels gibt. Die Vorteile und Ziele der Netzwerkanalyse stehen dabei im Fokus: Es soll aufgezeigt werden, welche Arbeitnehmer in Schlüsselposi-

---

1390 Zur weiten Zweckbestimmung des Zwecks „Durchführung des Beschäftigungsverhältnisses" siehe bereits **E. § 1 I. 1. b) bb)**.

1391 BeckOK DatenSR/*Riesenhuber*, § 26 BDSG Rn. 114.

1392 *Zöll*, in: Taeger/Gabel, DSGVO - BDSG, § 26 BDSG Rn. 38.

1393 *Maschmann*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, § 26 BDSG Rn. 18 f.

tionen im Unternehmen arbeiten bzw. wo wichtige Kommunikationswege verlaufen, um beispielsweise Probleme bei der formalen Hierarchie aufzudecken und die hierfür (eigentlich) vorgesehenen Kanäle verbessern zu können. Andernfalls könnten mitunter Arbeitnehmer übermäßig belastet werden, da für diese eine andere Aufgabe zugewiesen ist, sie aber immer nach Rat gefragt werden und hierdurch zusätzlicher Arbeitsaufwand in Form von Beantwortung von Fachfragen generiert wird.

Dafür ist das effektivste Mittel die Netzwerkanalyse, die gerade den Zweck hat, die informelle Organisationsstruktur zu beleuchten und in den Vordergrund zu bringen; mildere, gleich effektive Mittel sind nicht ersichtlich. Selbstverständlich muss dabei die Frage aufgeworfen werden, welche Erkenntnisse erzielt werden sollen. Soll lediglich das Expertennetzwerk im Unternehmen aufgezeigt werden, so wäre es nicht erforderlich, auch Fragen zum Strategie- oder Arbeitsnetzwerk zu stellen. Das gewählte Mittel muss mit dem angestrebten Ziel abgestimmt sein.

Im dargestellten Rahmen bestehen aus datenschutzrechtlicher Hinsicht daher keine Bedenken, wenn mittels der (manuellen) Netzwerkanalyse betriebliche Fragestellungen untersucht werden.

2. Betriebsverfassungsrechtlicher Kontext

Aus betriebsverfassungsrechtlichem Kontext kommt in erster Linie das Mitbestimmungsrecht aus § 94 Abs. 1 BetrVG in Betracht. Hiernach bedürfen Personalfragebögen der Zustimmung des Betriebsrats, wobei als Personalfragebogen eine formularmäßige Zusammenfassung von Fragen verstanden wird, die dem Arbeitgeber ein Bild von der Person und der Qualifikation verschaffen sollen.[1394]

Fragebögen im Rahmen von Netzwerkanalysen dienen jedoch nicht primär dazu, dem Arbeitgeber ein Bild von der Person und Qualifikation zu vermitteln, sondern das innerbetriebliche Netzwerk näher aufzudecken, weshalb weiter zu prüfen ist, ob § 94 Abs. 1 BetrVG tatsächlich für solche Fragebögen anwendbar ist. Die Norm dient dazu, sicherzustellen, dass der Arbeitgeber den Arbeitnehmern nur solche Fragen stellen kann, für die ein berechtigtes Auskunftsbedürfnis besteht.[1395]

1394 Hierzu siehe bereits **D. § 2 II. 2. a**).

1395 BAG, Beschl. v. 21.09.1993 – 1 ABR 28/93, AP BetrVG 1972 § 94 Nr. 4 unter B. II. 1. a) der Gründe; siehe auch die Regierungsbegründung zu § 94 BetrVG, BT-Drs. IV/1786, S. 50.

Das Schutzbedürfnis im Hinblick auf die Ausforschungsgefahr besteht jedoch auch bei diesen Fragestellungen wie obiges Beispiel zu unzulässigen Fragen bei der Netzwerkanalyse zeigt. Aus der Systematik mit Abs. 2 S. 1ergibt sich, dass sich die Fragebögen auf persönliche Angaben beziehen müssen.[1396] Es handelt sich um einen zustimmungsbedürftigen Fragebogen, wenn beispielsweise Fragen für Stellenbeschreibungen und Anforderungsprofile gestellt werden, die hieraus gewonnen Daten aber auch Rückschlüsse auf Leistung oder Eignung der Befragten zulassen.[1397] Aus dem Schutzzweck der Norm lässt sich daher herleiten, dass alle formalisierten und standardisierten Erhebungen durch den Arbeitgeber (so bspw. auch Mitarbeiterbefragungen) vom Zustimmungserfordernis des § 94 Abs. 1 BetrVG erfasst sind.[1398] Zwar werden solche im laufenden Beschäftigungsverhältnis in der Regel eingesetzt, wenn dem Arbeitnehmer andere Aufgaben übertragen werden sollen,[1399] das Telos gebietet jedoch keine Beschränkung auf diesen Anwendungsbereich.[1400] Zu beachten ist, dass es aufgrund von § 5 Abs. 3 BetrVG keiner Zustimmung bedarf, wenn eine Netzwerkanalyse mit Hilfe von Fragebögen lediglich auf der Ebene der leitenden Angestellten durchgeführt wird.[1401]

Neben § 94 Abs. 1 BetrVG kommt als weiterer Mitbestimmungstatbestand, insbesondere wenn die Fragebögen am Computer ausgefüllt werden sollen, immer § 87 Abs. 1 Nr. 6 BetrVG in Betracht, wenn verhaltens- und leistungsbezogene Daten erhoben werden.[1402] Allerdings erfordert letztere Norm, dass Leistung und Verhalten mithilfe einer technischen Einrichtung überwacht werden, wobei die Überwachungseignung ausreichend ist.[1403] Während das Intranet (in welchem z.B. die Fragebögen hochgeladen werden) jedenfalls ein mitbestimmungspflichtiger Tatbestand ist,[1404] weil sich aufgrund der Log-Dateien der Webserver eine Überwachung

1396 Richardi/*Thüsing*, § 94 BetrVG Rn. 10.
1397 Richardi/*Thüsing*, § 94 BetrVG Rn. 11, jedoch etwas im Widerspruch mit den unter Rn. 10 aufgeführten Angaben, dass Fragebögen zur Leistung und zum Verhalten des Arbeitnehmers nicht erfasst sein würden.
1398 ErfK/*Kania*, § 94 BetrVG Rn. 2; siehe auch BAG, Beschl. v. 21.09.1993 – 1 ABR 28/93, AP BetrVG 1972 § 94 Nr. 4
1399 GK-BetrVG/*Raab*, § 94 BetrVG Rn. 2.
1400 So wohl – jedenfalls bei nicht-anonymen Befragungen – auch *Moll/Roebers*, DB 2011, 1862 (1864).
1401 Vgl. GK-BetrVG/*Raab*, § 94 BetrVG Rn. 8.
1402 Richardi/*Thüsing*, § 94 BetrVG Rn. 10.
1403 Zum Tatbestand von § 87 Abs. 1 Nr. 6 BetrVG siehe bereits **D. § 2 II. 1. b**).
1404 Richardi/*Richardi/Maschmann*, § 87 BetrVG Rn. 499; ebenso beim Betrieb einer Facebook-Seite *Fitting*, § 87 Nr. 6 223a.

einfach realisieren lässt, ist dies mit spezifischem Blick auf die eingestellten Fragebögen zu hinterfragen. Für letztere ist bereits zweifelhaft, ob die Fragebögen selbst eine technische Einrichtung darstellen, da diese lediglich mit Hilfe anderer technischen Einrichtungen realisiert werden. Allerdings sind an die Voraussetzungen des § 87 Abs. 1 Nr. 6 BetrVG keine allzu hohen Anforderungen zu stellen.[1405] So ist es ausreichend, wenn hierzu im Intranet bspw. ein neues Software-Modul eingesetzt wird, das diese Befragungen ermöglicht.

Im Kern steht die Frage der Überwachungseignung: Bei digitalen Fragenbögen ist diese grundsätzlich vorhanden, da die Zugriffszeiten und -daten der einzelnen Arbeitnehmer ohne hohen Aufwand erfasst werden können und damit einhergehend eine Verhaltens- und Leistungsüberwachung möglich wird. Das gleiche gilt bei elektronischen Auswertungen von manuell erfassten Fragebögen, allerdings nur für jene Arbeitnehmer, die die Auswertung durchführen.

Zu beachten ist, dass sich das Mitbestimmungsrecht nicht auf den Inhalt der Fragebögen bezieht, sondern nur auf die Form.[1406] Lediglich, wenn die Befragung ausschließlich manuell durchgeführt wird (oder eine Auswertung extern erfolgt), entfällt die Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG.

Sofern die Arbeitnehmer zur Teilnahme an der Netzwerkanalyse verpflichtet werden oder ein ähnlicher Teilnahmedruck aufgebaut wird, betrifft dies das Ordnungsverhalten im Betrieb, sodass der Betriebsrat – ebenfalls nicht zum Inhalt, aber zur Teilnahmepflicht – ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG hat.[1407]

Soweit es sich bei der Netzwerkanalyse um eine Maßnahme der Personalplanung (dies der Regelfall sein) handelt, ist nach § 92 Abs. 1 BetrVG der Betriebsrat hierüber zu unterrichten und mit ihm zu beraten.[1408] Die Unterrichtungspflicht resultiert auch aus der Ermöglichung der allgemeinen Aufgabenerfüllung des Betriebsrats nach § 80 Abs. 2 BetrVG.[1409]

1405 *Fitting*, § 87 Nr. 6 Rn. 224 f.
1406 *Fitting*, § 87 Nr. 6 Rn. 226; *Moll/Roebers*, DB 2011, 1862 (1863).
1407 Ausreichend ist bereits, wenn die Arbeitnehmer in die Richtung gelenkt werden, *Moll/Roebers*, DB 2011, 1862 (1863); allgemein zu § 87 Abs. 1 Nr. 1 BetrVG siehe bereits **D. § 2 II. 1. a**).
1408 Vgl. **D. § 2 II. 4**.
1409 *Moll/Roebers*, DB 2011, 1862.

II. Automatisierte Erstellung eines „Enterprise Social Graph"

Eine moderne Form der Netzwerkanalyse, wenn auch hiermit etwas andere Fragestellungen erarbeitet werden, stellt der *Enterprise Social Graph* dar, der durch die Auswertung der innerbetrieblichen Kollaboration (meist durch die hierbei eingesetzten Softwarelösungen selbst) erstellt wird. Anders als bei der Netzwerkanalyse anhand von Fragebögen werden den Arbeitnehmern keine spezifischen Fragen gestellt, die diese beantworten sollen, sondern die Kommunikationswege und -häufigkeiten sowie Antwortzeiten und -anzahl, angesetzte Meetings (inkl. Teilnehmer), geteilte Dokumente usw. automatisiert ausgewertet und somit ein Netzwerk der digitalen Kollaboration aufgezeichnet. Ermöglicht wird diese Form der Auswertung durch die zunehmende Digitalisierung und immer leistungsfähigere Kollaborationslösungen, welche die gesamte innerbetriebliche Zusammenarbeit abbilden.

Als wohl populärstes Beispiel kann hier *Microsoft Office 365* genannt werden. In der Office-Suite lässt sich in vielen Unternehmen die komplette Zusammenarbeit abbilden. Gearbeitet wird in Microsoft Word, Excel, PowerPoint oder Outlook. Die Daten werden auf dem eigenen OneDrive-Speicher für individuelle Dokumente oder auf dem SharePoint-Server für im Unternehmen geteilte Dokumente, also in der (Azure) Cloud von Microsoft, gespeichert. Die Kommunikation erfolgt über Outlook und entweder einen On-Premise-Exchange-Server oder einen Exchange-Server in der Microsoft Cloud, ebenso wie die Telefonie. Nahtlos in das System fügt sich seit jüngerer Zeit Microsoft Teams ein, das kurze Chats und innerbetriebliche Telefonate und Videokonferenzen zwischen Arbeitnehmern (aber auch mit Externen) ermöglicht.

Durch das digitale Abbild des gesamten digitalen betrieblichen Lebens in einer Software-Suite lassen sich einfach sehr aufschlussreiche Auswertungen erstellen, ohne zunächst verschiedenartige Systeme verknüpfen und die Daten aufeinander anpassen zu müssen. Teilweise geschieht dies durch einen selbstlernenden Algorithmus, der die verschiedenen Quellen automatisch vernetzt und für den Benutzer veranschaulicht.[1410] Dies bedeutet aber keineswegs, dass die Systeme in sich geschlossen sind. Vielfach bieten die Software-Anbieter APIs[1411] an, um es Drittanbietern zu ermögli-

1410 *Ruchhöft*, CuA 2017, 8 (9).
1411 Siehe bereits Fn. 1384; ferner *Ruchhöft*, CuA 2017, 8 (10).

chen, diese Daten einfach auszulesen und so erweiterte Nutzungsmöglichkeiten zu generieren.[1412]

Leider ist auch dieses Thema bislang nur stiefmütterlich in der rechtswissenschaftlichen Literatur behandelt worden. In der Kommentierung von *Gola* zu § 26 BDSG ist lediglich der Hinweis vorhanden, dass solche Auswertungen allein im Rahmen von § 26 Abs. 1 S. 2 BDSG, also bei repressiven Maßnahmen, gerechtfertigt sein können.[1413] Andererseits weist insbesondere in die Praxis-Literatur darauf hin, dass aufgrund feingliedriger Einstellungen solche Anwendungen wie beispielsweise der Microsoft Graph durchaus datenschutzkonform gestaltet werden können.[1414]

Letztlich verbieten sich auch zu diesem Themenkomplex pauschalisierte Aussagen, sondern es muss im Einzelfall untersucht werden, inwiefern Netzwerkanalysen in Form eines Enterprise Social Graph durch Softwarelösungen angefertigt werden dürfen.

1. Datenschutzrechtliche Analyse

Im Vordergrund der Zulässigkeitsprüfung steht selbstverständlich (wiederum) das Datenschutzrecht, genauer § 26 Abs. 1 S. 1 BDSG. Es ist die Frage aufzuwerfen, ob und inwiefern automatisierte Analysen des Kommunikations- und Arbeitsalltags als erforderlich für die Durchführung des Arbeitsverhältnisses anzusehen sind. Im Kern handelt es sich bei dieser Abwägung, wie bereits mehrfach aufgezeigt, nicht um eine Erforderlichkeit im Sinne einer objektiven Notwendigkeit, sondern um eine Verhältnismäßigkeitsprüfung, verbunden mit einer Abwägung der Arbeitgeberinteressen mit denen der Arbeitnehmer.[1415]

1412 Bei Office 365 ist dies beispielsweise die Microsoft Graph-API, siehe https://developer.microsoft.com/de-de/graph (letzter Abruf am: 05.05.2020).

1413 *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 81.

1414 *Ruchhöft*, CuA 2017, 8 (11).

1415 Hierzu bereits ausführlich **D. § 1 IV. 2. b**), **E. § 1 I. 1. b**) **bb**), **E. § 1 III. 2. a**) **cc**) (**4**) sowie **E. § 3 I. 1. b**).

a) Legitimes Ziel

Zunächst muss es sich um ein legitimes Ziel handeln, das der Arbeitgeber mit der Einführung und Nutzung des Enterprise Social Graph verfolgt. Er benötigt also ein berechtigtes Interesse an den Daten.

Anders als bei Fragebögen, die spezifische Fragestellungen erfassen, werden beim Enterprise Social Graph alle elektronischen Logdaten mithilfe von künstlicher Intelligenz ausgewertet, um so bislang unentdeckte Zusammenhänge aufdecken zu können. Jegliche (soziale) Interaktionen wie Liken, Bloggen, Kommentieren, das Öffnen von Dokumenten (auch unbearbeitet), der Empfang, aber auch der Zeitraum zwischen Empfang und Lesen der E-Mail sowie zwischen Lesen und Versenden einer Antwort können bis ins kleinste Detail (bei Zeiträumen auf Millisekunden genau) erfasst und ausgewertet werden. Jede Interaktion stellt eine eigene Beziehung dar, die irgendwie durch einen Algorithmus bewertet werden muss.[1416] Im Unterschied zu spezifischen Fragestellungen, wo nur jene Beziehungen aufgezeigt werden, die konkret erarbeitet werden möchten, erfasst der Enterprise Social Graph auch Beziehungen, die für konkrete Fragestellungen völlig irrelevant sind. Zur Bewältigung dieser Datenflut kommen selbstlernende Algorithmen und künstliche Intelligenz[1417] zum Einsatz, die durch eine kontinuierliche Anpassung der Auswertung die relevanten Datensätze herausfiltern und für diese die spezifische Fragestellung bestmöglich gewichten und bewerten. Die Berechnungen sind hochkomplex und wären ohne leistungsfähige IT-Systeme von Menschenhand nicht zu bewerkstelligen (klassische *Big Data*-Anwendung[1418]).

Der Vorteil eines Enterprise Social Graph gegenüber der „klassischen" Netzwerkanalyse ist, dass eine Echtzeitauswertung stattfinden kann, während bei ersterer nur der Ist-Zustand zu einem bestimmten Zeitpunkt abgefragt werden kann. Ein innerbetriebliches Netzwerk ist hochdynamisch und verändert sich ständig. Durch eine Aufzeichnung über einen bestimmten Zeitraum lassen sich nicht nur tagesaktuelle Auswertungen erstellen, sondern auch die Veränderung im zeitlichen Verlauf darstellen, ohne hierfür regelmäßige Befragungen durchführen zu müssen.[1419] Diese Daten können gewinnbringend in die unternehmensinterne Organisati-

1416 Vgl. *Höller/Wedde*, Die Vermessung der Belegschaft, S. 25.
1417 Zur Funktionsweise von künstlicher Intelligenz und selbstlernenden Algorithmen siehe bereits grundlegend **C. § 2 II. 2**.
1418 Vgl. **C. § 2 II. 1**.
1419 *Höller/Wedde*, Die Vermessung der Belegschaft, S. 25.

ons- und Personalentwicklung einfließen, indem beispielsweise Missstände aufgedeckt und wichtige Akteure (sog. *Broker*) zwischen zwei in sich geschlossenen kleineren sozialen Netzwerken (sog. *Cliquen*) oder sogar zentrale Akteure, die eine Vielzahl von Cliquen vernetzen (sog. *Hidden Champions*) gefunden werden können.[1420]

Allerdings ist zu beachten, dass insbesondere bei erlaubter Privatnutzung der betrieblichen Infrastruktur auch nicht-betriebsbezogene Daten aufgezeichnet und analysiert werden, die der Privatsphäre der Nutzer zugeschrieben werden (z.B. Chats zwischen zwei befreundeten Arbeitnehmern). Auch diese würden dann eine Netzwerkstruktur darstellen. Durchaus möglich könnte es sein, dass der Arbeitgeber ebenfalls ein Interesse an diesen Daten hat. Ein solches wäre aber nicht mehr als legitim zu bezeichnen, da er für eine solche Auswertung, die rein dem Privatleben der Arbeitnehmer zuzuschreiben ist, keine Berechtigung hat; in diesem Bereich überwiegen die Grundrechte des Arbeitnehmers. Es kann eine Parallele zur Diskussion um das Einsichtsrecht des Arbeitgebers bei der erlaubten Privatnutzung des E-Mail-Accounts gezogen werden.[1421] Grundsätzlich ist nach h.M. ein Zugriff auf das E-Mail-Postfach möglich, jedoch nicht auf den Inhalt privater E-Mails.[1422]

Bei der Netzwerkanalyse ist die Auswertung von Chat-Beziehungen allerdings ein Problem: Die Software unterscheidet nicht zwischen privaten und dienstlichen Chats, sondern wertet nur die Verbindungsdaten aus, sodass private Chats zwingend miterfasst werden.

Sofern solche jedoch lediglich am Rande miterfasst werden und nicht gezielt untersucht werden (dies dürfte technisch derzeit auch noch nicht möglich sein), ist dies jedoch eine Frage der Angemessenheit der Maßnahme und nicht des Ziels. Ist das Ziel, einen Überblick über das betriebliche soziale Netzwerk und die Arbeitsbeziehungen zu erhalten, so hat der Arbeitgeber ein berechtigtes Interesse daran und es ist legitim.

1420 *Thiel*, Organisationsentwicklung 2010, 78 (81, 83 f.).

1421 Vgl. *Traut*, § 7. Überwachung der Nutzung von Internet und Social Media - Datenschutzrechtliche Grenzen, in: Thüsing/Wurth, Social Media im Betrieb, Rn. 35 f., wobei hier Chats aufgrund der Echtzeitkommunikation eher mit der Telefon- als mit der E-Mail-Nutzung verglichen werden; siehe aber Rn. 38 a.E. wonach dauerhaft fixierte Kommunikation in Form von Social Media ähnlich wie E-Mails zu beurteilen sein dürften; ferner bereits oben **D. § 3 I. 2. b) aa)**.

1422 Statt aller LAG Berlin-Brandenburg, Urt. v. 16.02.2011 – 4 Sa 2132/10, ZD 2011, 43; *Traut*, § 7. Überwachung der Nutzung von Internet und Social Media - Datenschutzrechtliche Grenzen, in: Thüsing/Wurth, Social Media im Betrieb, Rn. 38.

b) Geeignetes Mittel

Fraglich ist aber, ob die soziale Netzwerkanalyse durch Algorithmen, also durch einen Enterprise Social Graph überhaupt ein geeignetes Mittel darstellt, die vorhandenen Arbeitsbeziehungen korrekt abzubilden und ein korrektes Bild über das Unternehmen zu verschaffen. Die Datenqualität ist für die Beurteilung von entscheidender Bedeutung; wird das Netzwerk völlig falsch dargestellt, so ist das Mittel nicht tauglich zur Erreichung des angestrebten Ziels und die Datenverarbeitung durch eine solche Software unzulässig.

Noch vor wenigen Jahren wäre die Überprüfung der Verhältnismäßigkeit klar zugunsten der Arbeitnehmer ausgefallen, da es technisch (noch) nicht möglich war, das Arbeitsleben korrekt darzustellen: Ein Großteil der Kommunikation fand früher nicht über digitale Wege statt, die hätten vermessen werden können. Durch die Digitalisierung der Arbeit ist allerdings ein Wandel eingetreten; die momentane Corona-Krise verhilft diesen Auswertungstechnologien zu einer enormen Genauigkeit, da derzeit nahezu der gesamte Alltag digital erfasst wird, wenn Arbeitnehmer im Home-Office beispielswiese über Office 365 arbeiten und ausschließlich über Microsoft Teams (als Teil der Office-Suite) kommunizieren. Aber auch abseits der Krise geht Microsoft daraus aus, dass bereits 20 Stunden der wöchentlichen Arbeitszeit durch die Auswertung von Kalender- und E-Mails erfasst und ausgewertet werden können und somit 50 % der Zeit eines Vollzeitbeschäftigten.[1423] Hierdurch besteht eine hohe Aussagekraft des digitalen Abbilds, sodass die Analyse solcher Daten durchaus geeignet ist, aussagekräftige Informationen zu erteilen. Nach der derzeitigen Krise dürfte der Digitalisierungsgrad und somit die auswertbaren Daten um ein Vielfaches höher sein, selbst wenn wieder weitgehend Normalität eintritt. Da davon auszugehen ist, dass diejenigen Beschäftigen, die digital viel zusammenarbeiten auch im analogen Bereich mehr Kontakt haben, ist der „digitale Fußabdruck" auch repräsentativ für die Netzwerkanalyse.

Aus diesem Grund wird von Experten von einer hohen Aussagekraft innerbetrieblicher sozialer Graphen ausgegangen.[1424] Der Enterprise Social

1423 *Hanke*, Datenschutzprobleme und Gestaltungsmöglichkeiten in der Praxis, 2018, abrufbar unter: https://www.arbeitnehmerkammer.de/fileadmin/user_upload/Veranstaltungen/Veranstaltungsdokumentation/Downloads/Datenschutzrecht_20180221_Hanke.pdf (letzter Abruf am: 31.03.2020).

1424 *Höller/Wedde*, Die Vermessung der Belegschaft, S. 24.

Graph stellt daher ein geeignetes Mittel zur Erreichung des angestrebten Ziels dar.

c) Erforderlichkeit

Die Erforderlichkeit einer Maßnahme ist gegeben, wenn kein milderes, gleich effektives Mittel zur Verfügung steht. Wie bereits erläutert, dient der Enterprise Social Graph, die komplexen und sich ständig verändernden Beziehungen innerhalb eines Unternehmens in Echtzeit und im Zeitverlauf darstellen zu können. Da jede Interaktion eine neue Beziehung darstellt, handelt es sich hier um hochkomplexe Netzwerke, die nur mit immenser Rechenkapazität ausgewertet und mit selbstlernenden Algorithmen (KI) gewinnbringend analysiert werden können. Menschliche Auswertungen scheiden hingegen aus.

Es sind daher keine Gründe ersichtlich, an der Erforderlichkeit des Mittels zur Erreichung des angestrebten Ziels zu zweifeln.

d) Angemessenheit

Genauer geprüft werden muss allerdings – wie bereits im Rahmen des Prüfungspunktes „legitimes Ziel" angesprochen – die Angemessenheit der Maßnahme, also die Verhältnismäßigkeit im engeren Sinne. Bei dieser Prüfung werden die jeweiligen (Grund-)Rechtspositionen der beteiligten Akteure, also der Arbeitnehmer und des Arbeitgebers miteinander abgewogen. Zu beachten ist, dass es keinen Vorrang bestimmter Rechte gibt, sondern letztlich ein Begründungsvorgang erforderlich ist, bei welchem erörtert werden muss, warum – im spezifischen Fall – das Arbeitgeberinteresse an der Kenntnis des sozialen Netzwerks höher als das Geheimhaltungsinteresse des Arbeitnehmers ist. Maßgeblich ist u.a. die Eingriffsintensität der zugelassenen bzw. verbotenen Maßnahmen in die jeweiligen Rechtspositionen, die sich gegenüberstehen.[1425]

1425 Vgl. hierzu *Traut*, § 7. Überwachung der Nutzung von Internet und Social Media - Datenschutzrechtliche Grenzen, in: Thüsing/Wurth, Social Media im Betrieb, Rn. 38 f.

aa) Unterscheidung zwischen privaten und betrieblichen Daten kaum möglich

Sofern eine Analyse rein betrieblicher Daten stattfindet, so ist eine Maßnahme mangels Eingriffs in eine geschützte Rechtsposition der Arbeitnehmer klar zulässig. Dies ist beispielsweise der Fall, wenn statt eines betrieblichen Netzwerks Umsatzkennzahlen einzelner Unternehmensbereiche, Abteilungen oder Teams einer Analyse unterzogen werden.

Beim sozialen Netzwerk des Betriebs ist dies allerdings nicht so einfach, da auch ein betriebliches Netzwerk aus Menschen besteht, die auch persönlich bzw. privat in einer Beziehung stehen. Der Mensch ist keine Maschine, die nur Arbeitsaufgaben streng nach einem vorgegebenen Arbeitsablauf abarbeitet und die vorprogrammierten und vorgesehenen Beziehungen unterhält. Vielmehr gehört zu einem guten (und vom Arbeitgeber erwünschten) Betriebsklima auch zu einem großen Teil die private Interaktion. Diese erfolgt nicht nur persönlich unter Zimmerkollegen, sondern zu einem erheblichen Ausmaß auch im Rahmen digitaler Kommunikation, bspw. durch kurze Chats, E-Mails ggf. auch terminierte Meetings, die im Kalender erfasst werden – aktuell aufgrund zahlreichen Home-Office-Konstellationen noch umso mehr.

Eine Auswertung, die sich rein auf die betriebsbezogene Kommunikation erstreckt, ist mit der derzeitigen Technik (noch) nicht möglich, da die Programme nicht den Inhalt der Kommunikation analysieren und private Beziehungen aus den Auswertungen ausschließen. Es werden als Nebenprodukt immer private Verknüpfungen im Enterprise Social Graph erfasst.

bb) Bewertung der Eingriffsintensität

Hier stellt sich die Frage, ob die Erfassung solcher Daten als „Nebenprodukt" die Erstellung eines Enterprise Social Graph im Ganzen unzulässig macht. Hier ist auf die o.g. Maßstäbe zurückzugreifen, sodass es maßgeblich auf die Eingriffsintensität ankommt.

(1) Keine heimliche Netzwerkanalyse möglich

Offensichtlich dürfte sein, dass eine Netzwerkanalyse nicht heimlich durchgeführt werden darf, da dies die Eingriffsintensität enorm steigert

und auch nicht geboten ist. Allenfalls im Bereich der repressiven Maßnahmen nach § 26 Abs. 1 S. 2 BDSG kann im Einzelfall für einzelne Personen eine solche angemessen sein,[1426] wenn beispielsweise innerbetriebliche Betrugsfälle aufgedeckt und mögliche Mittäter identifiziert werden sollen. In allen anderen Bereichen müssen die Mitarbeiter vor der Einführung eines Enterprise Social Graph über den Verarbeitungszweck, die verarbeiteten Daten sowie Folgen informiert werden (vgl. Art. 13 DSGVO). Nur dann können Arbeitnehmer, die sich u.a. auch über private Angelegenheiten über betriebliche Kommunikationskanäle (mitunter zulässigerweise) austauschen auf andere Kanäle ausweichen, wenn sie nicht wünschen, dass private Verbindungen nicht aufgedeckt werden.

(2) Inhalt/Persönlichkeitsrelevanz bzw. Kernbereichsbezug

Eine besonders schwere Beeinträchtigung liegt vor, wenn ein Grundrecht im Kernbereich betroffen ist,[1427] z.B. im Bereich des Persönlichkeitsrechts muss ein Bürger die Möglichkeit im Bereich der privaten Lebensgestaltung haben, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art ohne die Angst einer (staatlichen) Überwachung zum Ausdruck bringen zu können. So ist der Zugriff auf private Tagebücher oder Film- und Tondokumente grundsätzlich untersagt.[1428]

Zusammen mit dem Kernbereich und deshalb gemeinsam zu behandeln ist die Persönlichkeitsrelevanz bzw. der Inhalt der Kommunikation. Es ist die Frage aufzuwerfen, welche Umstände und Inhalte werden erfasst und wie persönlich sind diese? Wird auf den Inhalt der Kommunikation zugegriffen?[1429]

1426 *Gola* ist der Auffassung, dass eine Rechtfertigung allein im repressiven Bereich stattfinden kann, ohne aber im Einzelnen darauf einzugehen, vgl. *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 81.

1427 BVerfG, Urt. v. 27.02.2008 – 1 BvR 370, 595/07, BVerfGE 120, 274 (335 f.) – Online-Durchsuchungen; BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (1189) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54.

1428 BVerfG, Beschl. v. 14.09.1989 – 2 BvR 1062/87, BVerfGE 80, 367 (373 f.) – Tagebuch; Urt. v. 27.02.2008 – 1 BvR 370, 595/07, BVerfGE 120, 274 (335 f.) – Online-Durchsuchungen.

1429 *Traut*, § 7. Überwachung der Nutzung von Internet und Social Media - Datenschutzrechtliche Grenzen, in: Thüsing/Wurth, Social Media im Betrieb, Rn. 33.

Derzeitige Softwarelösungen zum Enterprise Social Graph werten ausschließlich Verbindungsdaten der Kommunikation aus (Wer mit wem und wie häufig?) sowie kalendarische Einträge zu Meetings (hier aber ebenfalls nur Datum, Uhrzeit und Teilnehmer) im Falle des Office-Graphen.

In den Kernbereich von Grundrechten von Arbeitnehmern wird nicht eingegriffen; allenfalls kann das Persönlichkeitsrecht des Arbeitnehmers tangiert sein, wobei die Eingriffsintensität in das Persönlichkeitsrecht mangels Auswertung des Kommunikationsinhalts äußerst gering ist. So kann der Arbeitgeber aus der Analyse nicht ersehen, ob die Kommunikation betrieblichen Zwecken diente oder eine private Unterhaltung stattfand. Lediglich in Einzelfällen könnte eine solche Auswertung private Verbindungen aufdecken, beispielsweise wenn zwei fachfremde Arbeitnehmer einen sehr häufigen Chat-Kontakt haben, weil sie beispielsweise eine Liebesbeziehung pflegen. Der erhöhte Kontakt wäre in einem Netzwerkgraphen auffällig, wobei der Hintergrund dieser engen Beziehung durch die Analyse ebenfalls nicht offengelegt wird.

Zu beachten ist allerdings, dass aufgrund der notwendigen Information der Arbeitnehmer vor Einsatz eines solchen Systems diese die Möglichkeit haben, auf einen Kontakt über das Firmennetzwerk zu verzichten. Auf der sicheren Seite ist der Arbeitgeber jedenfalls, wenn er die private Kommunikation verbietet. Insbesondere aufgrund der unklaren Rechtslage zur Anwendbarkeit des TKG auf den Arbeitgeber bei erlaubter Privatnutzung sollte dieser, wenn Auswertungen der Verbindungsdaten stattfinden sollen, eine solche verbieten.[1430]

(3) Anlassbezogenheit und Dauer der Überwachung

Bei jeglicher Überwachungsmaßnahme – und eine solche stellt der Enterprise Social Graph ebenfalls dem Grunde nach dar – ist für die Beantwortung der Frage der Eingriffsintensität die Frage nach dem Überwachungsanlass sowie der Dauer der Überwachung zu stellen. Ein maßgeblicher Faktor ist die Anzahl der überwachten (unbeteiligten) Personen.[1431]

1430 Siehe hierzu bereits **D. § 3 I. 2**. Zwar fallen im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherte Daten zwar grundsätzlich nicht unter § 88 TKG, dennoch ist dies als Kriterium im Rahmen der Abwägung zu berücksichtigen, vgl. *Stück*, CCZ 2016, 285 (287) m.w.N.

1431 BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (1190) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54.

Schlussendlich sind diese Kriterien nichts anderes als eine strikte Anwendung des Verhältnismäßigkeitsgrundsatzes. Je eher ein Betroffener Anlass zur Überwachung gegeben hat, desto mehr muss er eine Einschränkung seiner persönlichen Rechte in Kauf nehmen. Für Personen, die keinen Anlass zur Überwachung gesetzt haben, ist eine solche von größerer Intensität.[1432]

Zur nicht-repressiven Netzwerkanalyse, die hier im Fokus der Untersuchung steht, haben die Betroffenen keinen Anlass geboten. Vielmehr möchte ein Arbeitgeber mehr über das betriebliche, informelle Netzwerk erfahren, um unbekannte Verbindungen zu erkennen und möglicherweise vorhergesehene Kommunikationskanäle zu verbessern (siehe bereits oben). Betroffen sind alle Arbeitnehmer des Betriebs, die digitale Kollaborationstools des Arbeitgebers nutzen (müssen).

Hinzu kommt, dass die Überwachung nicht nur stichprobenhaft und über begrenzte Zeiträume erfolgen kann, wenn ein tatsächliches Abbild über einen zeitlichen Verlauf erstellt werden soll. Die Überwachung der Kommunikation (und z.B. des Kalenders) zur Erstellung eines Enterprise Social Graphs muss dauerhaft erfolgen, damit sie überhaupt geeignet ist, den erstrebten Zweck zu erfüllen (siehe bereits oben **b**) und **c**)).

Dennoch ist ein Unterschied zu den vielfach vor den Gerichten ausgefochtenen Video-Überwachungsfällen herauszuheben. Während dort die Arbeitnehmer in ihrem gesamten Verhalten überwacht werden, mitunter sogar der Kommunikationsinhalt, sofern eine Audio-Aufzeichnung ebenfalls stattfindet, erfasst die Netzwerkanalyse nur einen marginalen Teil des betrieblichen Lebens (im durchschnittlichen Unternehmen etwa 50 % der Kommunikationsvorgänge[1433] und hiervon nur die Verbindungsdaten [„Metadaten"]). Die Gefahr eines „Gefühls des Überwachtwerdens"[1434] ist demnach auch ungemein geringer, wenn die Betroffenen ordnungsgemäß nach Art. 13 DSGVO informiert wurden. Transparente und klar kommu-

1432 St. Rspr.; vgl. statt aller BVerfG, Urt. v. 11.03.2008 – 1 BvR 2074/05, 1 BvR 1254/07, BVerfGE 120, 378 (402) = NJW 2008, 1505 – Automatische Kennzeichenerfassung m.w.N.

1433 *Hanke*, Datenschutzprobleme und Gestaltungsmöglichkeiten in der Praxis, 2018, abrufbar unter: https://www.arbeitnehmerkammer.de/fileadmin/user_upload/Veranstaltungen/Veranstaltungsdokumentation/Downloads/Datenschutzrecht_20180221_Hanke.pdf (letzter Abruf am: 31.03.2020).

1434 BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, BVerfGE 115, 320 (354 f.) = NJW 2006, 1939 – Rasterfahndung II; Urt. v. 11.03.2008 – 1 BvR 2074/05, 1 BvR 1254/07, BVerfGE 120, 378 (403) = NJW 2008, 1505 – Automatische Kennzeichenerfassung.

nizierte Regelungen zum eingesetzten Verfahren, zur Gewährleistung der Datensicherheit und Protokollierung verringern die Eingriffsintensität.[1435]

Ein Vergleich lässt sich vor allem zur Überwachung von Telefon- und E-Mail-Verbindungsdaten ziehen. Diese wurde in der Rechtsprechung und Literatur schon umfassend behandelt.[1436] Während nach hiesiger Auffassung das TKG auf Arbeitgeber keine Anwendung findet, sind die Abwägungskriterien auch beim allgemeinen Datenschutzrecht dieselben.

Im Bereich der Telefonie ist anerkannt, dass Arbeitgeber – bei verbotener Privatnutzung – die Verbindungsdaten, also Datum, Uhrzeit, Gesprächsdauer und Uhrzeit auch anlasslos aufzeichnen dürfen:

> „*Unter dem Gesichtspunkt des Persönlichkeitsrechts problematisch ist allein die Erfassung der vollständigen Zielnummer, und zwar ohne Differenzierung nach dienstlichen und privaten Gesprächen. Da es aber um Telefonate vom Dienstapparat geht, vom Arbeitnehmer aber erwartet werden kann, daß er seine privaten Angelegenheiten außerhalb der Arbeitszeit regelt, ist der Eingriff in das Persönlichkeitsrecht eng begrenzt.*“[1437]

Als problematisch wird in der Rechtsprechung vor allem die (vollständige) Erfassung der Zielrufnummer angesehen, da es sich dort auch um personenbezogene Daten des Empfängers handelt und für diese Speicherung eine eigenständige Legitimationsgrundlage erforderlich wäre.[1438] Aber auch im Innenverhältnis des Betriebs kann eine vollständige Erfassung im Hinblick auf das Behinderungsverbot des § 78 BetrVG problematisch sein, wenn die Gefahr besteht, dass Betriebsratsmitglieder bei ihrer Arbeit behindert werden. Dies wäre der Fall, wenn Kontakte zu einzelnen Arbeitnehmern minutiös aufgezeichnet würden.[1439]

Die zitierte Rechtsprechung behandelte im Kern immer die Erfassung der Verbindungsdaten zur Kostenkontrolle, nicht zur Auswertung im Rah-

---

1435 BAG, Beschl. v. 15.04.2014 – 1 ABR 2/13 (B), NZA 2014, 551 (553 f.) = BAGE 148, 26 = AP BetrVG 1972 § 29 Nr. 9.

1436 Einen Überblick geben *Thüsing/Traut*, § 9. Speicherung und Sichtung von E-Mails und E-Mail-Logfiles, in: Thüsing, Beschäftigtendatenschutz und Compliance, Rn. 31 ff. sowie *Thüsing/Traut*, § 10. Überwachung von Telefonverbindungsdaten, in: Thüsing, Beschäftigtendatenschutz und Compliance, Rn. 1 ff.

1437 LAG Niedersachsen, Urt. v. 13.01.1998 – 13 Sa 1235/97, NZA-RR 1998, 259 (260).

1438 Offen gelassen von BAG, Beschl. v. 27.05.1986 – 1 ABR 48/84, AP BetrVG 1972 § 87 Überwachung Nr. 15 = NZA 1986, 643 unter B. II. 2. e) der Gründe.

1439 Vgl. zum äquivalenten § 8 BPersVG BAG, Beschl. v. 01.08.1990 – 7 ABR 99/88, AP ZA-Nato-Trupppenstatus Art. 56 Nr. 20 unter B. II. 3. der Gründe.

men von People Analytics. Hierbei wurde das Interesse des Arbeitgebers zur Missbrauchskontrolle mit den Interessen der Arbeitnehmer bzw. Arbeitnehmervertretung abgewogen.[1440] Die Zulässigkeitsprüfung der Überwachung des (kostenlosen) E-Mail-Verkehrs hingegen erfolgte in Literatur und Rechtsprechung v.a. unter dem Aspekt der Fehlerbehebung sowie der rechtswidrigen Inanspruchnahme sowie wirtschaftlichen Schädigung im Sinne von „*fraud prevention*".[1441] Bei beiden Fällen ist ein sehr hohes (wirtschaftliches) Interesse des Arbeitgebers anzuerkennen, welches bspw. im Falle der internen Kommunikation der Betriebsratsmitglieder nicht bestand.

Im Rahmen von Netzwerkanalysen besteht ebenfalls ein wirtschaftliches Interesse des Arbeitgebers, jedoch nicht im Sinne der Kosten- und Missbrauchskontrolle, sondern der Effektivierung seiner Betriebsabläufe. Auf der anderen Seite steht das Persönlichkeitsrecht bzw. das Recht auf Privatheit der Arbeitnehmer.

Umfassende, anlasslose Aufzeichnungen der Verbindungsdaten sind bereits aufgrund § 78 BetrVG problematisch; jedenfalls müsste die Kommunikation der Betriebsratsmitglieder aus den Analysen ausgenommen werden, da hier das Interesse an einer ungestörten Betriebsratsarbeit überwiegt. Je höher der Konzern digitalisiert ist, desto mehr analysierbare Kommunikation findet statt und desto genauer kann das erzeugte Abbild werden. Für die Betriebsratsarbeit kann dies hochproblematisch sein, wenn Arbeitnehmer davor zurückschrecken, mit ihren Problemen den Betriebsrat zu kontaktieren, da sie befürchten müssen, dass der Arbeitgeber diese Kommunikation analysiert und dies negative Folgen für sie haben könnte.

Auch unter dem Aspekt der oben zitierten Rechtsprechung des LAG Niedersachsen müsste sichergestellt sein, dass private Kommunikation bei erlaubter Privatnutzung nicht erfasst wird.[1442]

1440 *Thüsing/Traut*, § 10. Überwachung von Telefonverbindungsdaten, in: Thüsing, Beschäftigtendatenschutz und Compliance, Rn. 2 ff.

1441 Hierzu m.w.N. *Thüsing/Traut*, § 9. Speicherung und Sichtung von E-Mails und E-Mail-Logfiles, in: Thüsing, Beschäftigtendatenschutz und Compliance, Rn. 58 ff. - der Begriff "fraud prevention" stammt aus der Vorauflage, dort Rn. 100 ff.

1442 Siehe hierzu aber bereits oben (**2**).

(4) Folgen

Die Folgen einer Überwachungsmaßnahme sind von entscheidender Bedeutung für die Eingriffsintensität. Hat ein Arbeitnehmer negative Folgen zu befürchten, kann das Gefühl des Überwachtwerdens vielfach Einschüchterungseffekte hervorrufen, welche Arbeitnehmer daran hindern könnten, ihre Grundrechte wahrzunehmen.[1443] So hat auch das BVerfG festgestellt, dass die Intensität des Grundrechtseingriffs in das allgemeine Persönlichkeitsrecht u.a. davon beeinflusst wird, welche nachteiligen sonstigen Folgen aufgrund der Maßnahme drohen oder nicht ohne Grund zu befürchten sind.[1444]

Hierbei stehen, wie sich in der Rechtsprechung des BVerfG zeigt, nicht die datenschutzrechtlichen Folgen im Fokus wie im Rahmen der Zweckänderung (vgl. **E. § 1 I. 2. d) dd)**), sondern es sind jegliche tatsächliche negative Folgen mit gleicher Gewichtung zu berücksichtigen, die Arbeitnehmer daran hindern könnten, ihre grundrechtlichen Freiheitsrechte auszuüben. Selbstverständlich dürfen – da es um immer noch eine datenschutzrechtliche Abwägung geht – die datenschutzrechtlichen Folgen auch nicht außer Acht gelassen werden.

Mögliche Folgen der Netzwerkanalyse könnten sein, dass (bei erlaubter Privatnutzung) private Beziehungen zwischen Mitarbeitern aufgedeckt werden und Kontakte zum Betriebsrat sichtbar werden (und Arbeitnehmer daher davon zurückschrecken, diesen zu kontaktieren) bis hin zu negativen personellen Maßnahmen, wenn beispielsweise ein Nachrichtenaufkommen registriert wird, das deutlich über dem betrieblichen Durchschnitt liegt und daher vermutet wird, dass private Chats während der Arbeitszeit stattfinden. Zwar handelt der konkrete Arbeitnehmer in letzterem Fall vertragswidrig und seine Interessen sind daher nur in geringem Maße schutzwürdig. Die durch die Netzwerkanalyse statuierte Überwachung selbst erfasst aber auch legale Verhaltensweisen (wie beispielsweise Chats in den Pausen bei erlaubter Privatnutzung sowie Kontaktierung des Betriebsrats) und könnte Arbeitnehmer davon abhalten, ihre Rechte wahrzunehmen. Um solche geschützten Interessen nicht zu beeinträchtigen

1443 BAG, Beschl. v. 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 (1191) = BAGE 127, 276 = AP BetrVG 1972 § 75 Nr. 54.

1444 Vgl. statt vieler BVerfG, Urt. v. 11.03.2008 – 1 BvR 2074/05, 1 BvR 1254/07, BVerfGE 120, 378 (403) = NJW 2008, 1505 – Automatische Kennzeichenerfassung Rn. 80; Beschl. v. 04.04.2006 – 1 BvR 518/02, BVerfGE 115, 320 (351 ff.) = NJW 2006, 1939 – Rasterfahndung II Rn. 107 ff.

und negative Folgen zu vermeiden oder minimieren, kann der Arbeitgeber beim Einsatz dieser Technologie entsprechende juristische Garantien vorsehen. Diese könnten beispielsweise Verarbeitungsverbot oder die Zusicherung, dass aus der Analyse keine bzw. nur in sehr eng begrenzten Fällen negative Folgen entstehen. Für die Garantien gelten dieselben Maßstäbe wie bei der Zweckvereinbarkeitsprüfung.[1445]

cc) Zwischenergebnis

Netzwerkanalysen sind aufgrund der hohen Eingriffsintensität und dauerhaften, anlasslosen Überwachung datenschutzrechtlich problematisch. Hieraus darf jedoch nicht geschlussfolgert werden, dass solche grundsätzlich unzulässig bzw. nur im Rahmen von § 26 Abs. 1 S. 2 BDSG möglich sind.[1446] Vielmehr bedarf es einer präzisen Regelung aller typischerweise in einem Unternehmen stattfindenden Kommunikationsvorgänge und einer Abwägung der dort widerstreitenden Interessen.

Keinesfalls darf eine Überwachungs-/Drucksituation – wie beispielsweise bei einer dauerhaften Videoüberwachung des Arbeitsplatzes – geschaffen werden. Auch die Privatnutzung betrieblichen Kommunikationsplattformen sollte (insbesondere unter dem Aspekt der unklaren Rechtslage zur Anwendbarkeit des TKG auf Arbeitgeber) verboten werden. Jedenfalls müssen die Arbeitnehmer im Vorfeld darauf hingewiesen werden, dass die Verbindungsdaten der Kommunikation überwacht und Analysen zugeführt werden. Im Hinblick auf die private Nutzung der Plattformen scheint es denkbar, dass eine Einwilligung gem. § 26 Abs. 2 S. 1 BDSG eingeholt wird, da die Arbeitnehmer keiner Drucksituation unterliegen; sie können auch schlicht auf (ggf. unzulässige) private Konversationen über das Firmennetzwerk verzichten, wenn sie eine Aufdeckung von Beziehungen vermeiden möchten. Auch aus diesem Blickwinkel dürfte eine Angemessenheit bei erlaubter Privatnutzung nicht ausgeschlossen sein.

Sofern die betriebliche Kommunikation im Zentrum der Analyse steht, ist die Eingriffsintensität in das Persönlichkeitsrecht der Arbeitnehmer – anders als bei der Videoüberwachung – eng begrenzt, sodass von einem Überwiegen der Arbeitgeberinteressen auszugehen ist.

Zur Absicherung können auch juristische Garantien durch den Arbeitgeber (entweder in Betriebsvereinbarungen oder durch eine Generalzusa-

---

1445 Siehe hierzu bereits **E. § 1 III. 2. b**) (**2**).

1446 So aber *Gola*, in: Gola/Heckmann, BDSG, § 26 BDSG Rn. 81.

ge) abgegeben werden, die im Rahmen der Folgenabwägung sich ebenfalls zugunsten einer Analyse auswirken.

e) Abschließende Bewertung

Grundsätzlich sind innerbetriebliche Netzwerkanalysen – mit Einschränkungen – zulässig. Es bedarf jedoch einer differenzierten Bewertung im Einzelfall, die – gerade im Hinblick auf die volle richterliche Überprüfbarkeit der Abwägung nach § 26 Abs. 1 S. 1 BDSG – immer mit Rechtsunsicherheiten belastet sind.

Aufgrund der Einschätzungsprärogative der Betriebspartner im Rahmen einer Regelung gem. § 26 Abs. 4 BDSG, Art. 88 Abs. 1 DSGVO[1447] ist zu empfehlen, eine die Datenverarbeitung legitimierende Betriebsvereinbarung abzuschließen. Hierdurch können bei Einhaltung der Datenschutzgrundsätze des Art. 88 Abs. 2, Art. 5 DSGVO (vgl. § 26 Abs. 4 S. 2 BDSG) Rechtsstreitigkeiten und insbesondere Bußgelder vermieden werden.

Eine umfassende Information der Arbeitnehmer vor der Datenerhebung und -verarbeitung ist nicht zuletzt aufgrund von Art. 13 DSGVO in jedem Falle erforderlich. Werden die Maßnahmen heimlich durchgeführt, so führt dies nicht nur zu einer Verletzung der Informationspflicht, sondern auch im Rahmen der Abwägung nach § 26 Abs. 1 S. 1 BDSG zu einer Unzulässigkeit der Datenverarbeitung.

2. Betriebsverfassungsrechtlicher Kontext

Nicht nur aus datenschutzrechtlichen, sondern auch aus betriebsverfassungsrechtlichen Gründen ist der Abschluss einer Betriebsvereinbarung erforderlich. Bei der Netzwerkanalyse bzw. bereits bei der Erhebung der Daten für eine solche, handelt es sich um eine Überwachungsmaßnahme nach § 87 Abs. 1 Nr. 6 BetrVG. Da Netzwerk-Graphen, wie bereits oben aufgeführt, insbesondere auch im Rahmen der (weit zu verstehenden[1448]) Personalplanung gem. § 92 BetrVG eingesetzt werden, muss der Arbeitgeber den Betriebsrat bereits in der Planungsphase („*rechtzeitig*“) darüber informieren. Zur Vermeidung von Wiederholungen wird auf die Ausführungen unter **E. § 1 IV. 2** verwiesen.

1447 Siehe hierzu bereits **E. § 1 III. 1. c) aa)**; allgemein **D. § 1 V. 2.**
1448 Zu § 92 BetrVG siehe bereits **D. § 2 II. 4.**

III. Zusammenfassung

Netzwerk-Graphen stellen ein mächtiges Mittel dar, um die informelle Organisation im Unternehmen darzustellen und zu analysieren. Im Grundsatz gibt es zwei Ansätze: Einerseits die Analyse anhand standardisierter Fragebögen, die darauf abzielen, ganz bestimmte Fragestellungen zu beantworten und einen bestimmten Typus von Netzwerk aufzudecken. Andererseits den Enterprise Social Graph, der die gesamte digitale Kommunikation innerhalb eines Unternehmens in Echtzeit abdecken kann.

Während ersteres aus datenschutzrechtlicher Sicht, bei korrekter Formulierung der Fragen (siehe **E. § 4 I. 1**) unproblematisch ist, bestehen bei letzterem schon erheblich größere Probleme, da eine anlasslose, dauerhafte Überwachung statuiert wird (siehe **E. § 4 II. 1**). Nichtsdestotrotz kann dieser zulässig sein; so überwiegen auch dort in vielen Fällen die Arbeitgeberinteressen. Aufgrund der Vielzahl der erfassbaren Kommunikationssituationen bedarf es einer präzisen und detaillierten Regelung. In jedem Fall müssen Analysen von Betriebsratskommunikationen gänzlich ausgeschlossen werden, da Arbeitnehmer sonst von der Wahrnehmung ihrer Rechte zurückschrecken könnten, wenn sie Repressalien des Arbeitgebers zu befürchten haben. Ebenso müssen eine Regelung für private Kommunikation über betriebliche Netzwerke getroffen und beispielsweise Einwilligungen von Arbeitnehmern eingeholt werden.

Dennoch lassen sich Netzwerkanalysen optimal in bereits vorhandene People Analytics integrieren, wenn Unternehmen ihre Arbeit weitgehend digitalisiert haben. Gerade bei der Nutzung von Kollaborationssuites wie Office 365 bedarf es nur eines geringen technischen Aufwandes zur Implementierung, da solche Funktionen von Haus aus integriert sind. Über APIs können die Daten aus der Software so in das Personalmanagementsystem integriert und ein noch größerer Nutzen erzeugt werden.

In jedem Fall muss ein vorhandener Betriebsrat aufgrund der betriebsverfassungsrechtlichen Mitspracherechte im Vorfeld informiert und bei der Planung und Einführung eingebunden werden. In diesem Zusammenhang empfiehlt es sich – zur Vermeidung von Rechtsunsicherheiten – eine gleichzeitig die Datenverarbeitung legitimierende Betriebsvereinbarung abzuschließen.