F. Entwicklung einer Muster-Betriebsvereinbarung

An vielen Stellen dieser Arbeit wurde darauf hingewiesen, dass der Abschluss einer Betriebsvereinbarung nicht nur aus betriebsverfassungsrechtlicher Sicht notwendig, sondern auch aus datenschutzrechtlichem Blickwinkel geboten ist, um Rechtsunsicherheiten bei der Auslegung des offenen Begriffs der „Erforderlichkeit" zu vermeiden.

Nach Art. 88 Abs. 1 DSGVO sowie § 26 Abs. 4 S. 1 BDSG kann eine Betriebsvereinbarung die Datenverarbeitung legitimieren, sofern die in Art. 5 DSGVO genannten Datenschutzgrundsätze eingehalten werden.[1449]

Unter **D. § 1 IV** sowie **D. § 1 V. 2** wurde ausführlich dargelegt, warum die Betriebspartner mit Hilfe einer Betriebsvereinbarung kein eigenständiges Datenschutzregime erzeugen können, sondern sich im Grundsatz an das vorgegebene Datenschutzniveau der DSGVO und des BDSG halten müssen, jedoch für Einzelfälle Spezialregelungen schaffen dürfen, die bei gerichtlichen Streigikeiten nicht vollumfassend am Begriff der Erforderlichkeit gemessen werden (Einschätzungsprärogative der Betriebspartner). Die Verhandlungspartner bei der Abwägung der Grundrechte nach § 75 Abs. 2 BetrVG einen Beurteilungsspielraum, der Rechtssicherheit schafft.[1450]

Nachfolgend soll ein möglicher Aufbau einer Betriebsvereinbarung dargestellt werden, die die Einführung von People Analytics sowie damit zusammenhängende datenschutzrechtliche Legitimationsfragen regelt. Es soll aufgezeigt werden, wo die Verhandlungspartner einen Regelungsspielraum besitzen und wie dieser ausgestaltet werden kann. Die Orientierung erfolgt an den in dieser Arbeit genannten Beispielen. Eine konsolidierte Fassung der hier erarbeiteten Betriebsvereinbarung findet sich im **Anhang II**.

1449 Unter altem Recht (§ 4 Abs. 1 BDSG a.F.) war dies aufgrund der Formulierung „andere Rechtsvorschriften" zunächst umstritten, aber letztlich h.M., vgl. *Körner*, NZA 2019, 1389 (1390); *Klösel/Mahnhold*, NZA 2017, 1428, jeweils m.w.N.

1450 Bejahend einen Beurteilungsspielraum im Hinblick auf die Erforderlichkeit der Datenverarbeitung (im Rahmen von § 75 Abs. 2 BetrVG) bei der Abwägung nationaler Grundrechte, BAG, Beschl. v. 29.06.2004 – 1 ABR 21/03, NZA 2004, 1278 (1280) = BAGE 111, 173 = AP BetrVG § 87 1972 Überwachung Nr. 41 (m. Anm. Ehmann); siehe bereits **E. § 1 III. 1. c) aa)**.

§ 1 Allgemeines

§ 26 Abs. 6 BDSG regelt, dass die Beteiligungsrechte der Interessensvertretungen der Beschäftigten unberührt bleiben, d.h. auf Basis der bislang aufgezeigten Mitbestimmungsrechte (insbesondere § 87 Abs. 1 Nr. 1 und 6 sowie §§ 94 f. BetrVG) kann der Betriebsrat Betriebsvereinbarungen zum Beschäftigtendatenschutz initiieren. § 88 BetrVG ermöglicht dem Betriebsrat auch den Abschluss (freiwilliger) Betriebsvereinbarungen in mitbestimmungsfreien Regelungsbereichen.[1451] Im Übrigen verhält sich das Datenschutzrecht nicht zu Mitbestimmungsrechten.

Aufgrund der Informations- und Transparenzanforderungen, aber auch der weitergehenden Beteiligungsrechte müssen insbesondere in bereits vorhandenen Betriebsvereinbarungen weitgehendere und detaillierte Regelungen getroffen werden als früher.[1452] Dies ergibt sich bereits Art. 88 Abs. 2 DSGVO selbst, wonach geeignete und besondere Maßnahmen im Hinblick auf die Transparenz der Verarbeitung in einer solchen Vereinbarung enthalten sind.[1453]

Unterschieden wird grundsätzlich hinsichtlich des Regelungsgehalts zwischen Rahmen- und Einzelbetriebsvereinbarungen.[1454]

§ 2 Anforderungen an eine datenschutzrechtliche Betriebsvereinbarung

I. Transparenzerfordernis des Art. 88 Abs. 2 DSGVO

Aufgrund von Art. 88 Abs. 2 DSGVO sollten Betriebsvereinbarungen in jedem Falle Regelungen zur Transparenz der Datenverarbeitung enthalten. Diese erfüllen entweder die Anforderungen der Art. 12 ff. DSGVO oder spezifizieren die Anforderungen weiter. Bisweilen wird empfohlen (spezifische) Regelungen zur Unterrichtung und Information der betroffenen Arbeitnehmer zu treffen.[1455]

Es ist umstritten, ob sich die Vorgabe zur Transparenz der Datenverarbeitung auf die inhaltliche Ausgestaltung und oder auch die formalen Regelungen selbst bezieht, letztere also in klarer und verständlicher Sprache

---

1451 Hierzu allgemein *Körner*, NZA 2019, 1389 (1391).
1452 *Körner*, NZA 2019, 1389 (1391 f.).
1453 Wie hier wohl *Dzida/Grau*, DB 2018, 189 (191).
1454 *Klösel/Mahnhold*, NZA 2017, 1428.
1455 Hierzu *Wybitul*, ZD 2016, 203 (207).

gefasst sein müssen. Teilweise wird vertreten, dass das Transparenzgebot auch für die Regelungen selbst gilt.[1456] Als Grundlage werden der Transparenzgrundsatz aus Art. 5 Abs. 1 lit. a DSGVO sowie Erwägungsgrund 58 herangezogen. In letzterem heißt es: „*Der Grundsatz der Transparenz setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist […]*". Die Gegenauffassung[1457] stützt sich auf den Wortlaut des Art. 88 Abs. 2 DSGVO („*Transparenz der Verarbeitung*"), erkennt aber teilweise[1458] gleichwohl eine Sinnhaftigkeit einer klaren und verständlichen Regelung unter Rückgriff auf Erwägungsgrund 41 S. 2 („[…] *sollten jedoch klar und präzise sein*") an. Eine Adressierung an juristische Laien sei aber aufgrund der notwendig hoch technischen und präzisen Regelung nicht möglich. Eine Lösung, die wiederum von anderen Autoren hierzu vorgeschlagen wird, ist die Betriebsvereinbarung mit einem Dokument zu „häufig gestellten Fragen (FAQ)" zu ergänzen, um Regelungstransparenz herzustellen.[1459]

Als „Minimallösung" wird teilweise eine Wiedergabe oder Bezugnahme auf die Transparenzvorschriften der Art. 12 - 15 DSGVO akzeptiert[1460], aber detailliertere Regelungen bzw. alternative Informationsmechanismen (z.B. Information des Betriebsrats statt des Einzelnen) als zweckmäßig erachtet.[1461] Eine weitere Ansicht verzichtet hingegen vollständig auf die Bezugnahme auf Pflichten nach Art. 12 ff. DSGVO, da der „Verantwortliche" ohnehin zuständig ist und daher eine (weitere) Regelung mit dem Betriebsrat bei Erfüllung dieser Pflichten nicht erforderlich sei.[1462] Über-

1456 Paal/Pauly/*Pauly*, Art. 88 DSGVO Rn. 14; Sydow/*Tiedemann*, Art. 88 DSGVO Rn. 20; *Grimm*, ArbRB 2018, 78 (80): "Kein IT-Deutsch"; *Korinth*, ArbRB 2018, 47 (49).

1457 BeckOK DatenSR/*Riesenhuber*, Art. 88 DSGVO Rn. 85; *Klösel/Mahnhold*, NZA 2017, 1428 (1431); *Wybitul*, ZD 2016, 203 (207 f.); wohl auch *Maschmann*, DB 2016, 2480 (2484).

1458 BeckOK DatenSR/*Riesenhuber*, Art. 88 DSGVO Rn. 85.1.

1459 *Dzida/Grau*, DB 2018, 189 (192); *Tiedemann*, ArbRB 2016, 334 Fn. 15; *Wybitul/Sörup/Pötters*, ZD 2015, 559 (561).

1460 *Tiedemann*, ArbRB 2016, 334 (336); *Kort*, DB 2016, 711 (714).

1461 *Wybitul*, ZD 2016, 203 (208); *Klösel/Mahnhold*, NZA 2017, 1428 (1431): Bloße Wiedergabe ausreichend, Betriebsvereinbarung hat allerdings auch Vorschriften zu enthalten, die die Transparenzanforderungen erfüllen.

1462 *Dzida/Grau*, DB 2018, 189 (193).

wiegend wird allerdings vertreten, dass eine bloße Wiedergabe des Gesetzestexts nicht ausreichend sei,[1463] um den Anforderungen zu entsprechen.

Gibt es mehrere Betriebsvereinbarungen im Unternehmen, so ist im Hinblick auf den Transparenzgrundsatz eine Erläuterung des Regelungszusammenhangs zwischen den einzelnen Betriebsvereinbarungen (z.B. einer Rahmenbetriebsvereinbarung und einer spezifischen Einzelbetriebsvereinbarung); eine solche Erläuterung an einer für alle Arbeitnehmer leicht zugänglichen Stelle (z.B. das Intranet) ist ausreichend.[1464]

Letztlich lässt sich die Lösung im den Datenschutzprinzipien selbst finden: Art. 5 Abs. 1 lit. a DSGVO bestimmt, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise, ebenfalls aber nach lit. b auch für festgelegte, eindeutige Zwecke verarbeitet werden müssen. Muss die Kollektivvereinbarung selbst sprachlich einfach gehalten werden, so sind präzise Regelungen („*Juristendeutsch*“) kaum möglich. Aus diesem Grund würde das Transparenzerfordernis somit anderen Regelungen zuwiderlaufen. Vielmehr muss es ausreichend sein, dass Betroffene anhand von FAQs oder sonstigen Erläuterungen klar nachvollziehen, für welche Zwecke ihre Daten genau verarbeitet werden. Hierdurch lässt sich auch die Form der Information nach Art. 12 ff. bzw. Art. 88 Abs. 2 DSGVO bestimmen: Die notwendigen Informationen müssen dabei nicht selbst im Normtext aufgenommen werden, sondern können an einer für alle Beschäftigten gut einsehbaren Stelle (z.B. das Intranet) veröffentlicht werden. Selbstverständlich muss bei mehreren Regelungen auch das Verhältnis zueinander klar dargestellt werden, um Normenklarheit zu schaffen.[1465] Eine Aufnahme aller Informationen in den Normtext würde diesen hingegen überfrachten und der Transparenz entgegenwirken. Möglich bleibt es aber selbstverständlich, technische Ausführungen noch durch eine – wenn auch unpräzisere – Erläuterung für den juristischen Laien beispielsweise als (nicht-normative) „Informationsbox“ in den Normtext aufzunehmen. Die in Art. 88 Abs. 2 DSGVO geforderten Transparenz-Maßnahmen kön-

1463 *Düwell/Brink*, NZA 2017, 1081 (1082); *Haußmann/Brauneisen*, BB 2017, 3065 (3066); Sydow/*Tiedemann*, Art. 88 DSGVO Rn. 20; *Grimm*, ArbRB 2018, 78 (80); *Wurzberger*, ZD 2017, 258 (262).

1464 *Korinth*, ArbRB 2018, 47 (49); *Tiedemann*, ArbRB 2016, 334 (336).

1465 Ein aktuelles Beispiel von einer unklaren Rechtslage zeigten die Corona-Verordnungen der Länder in Zusammenhang mit den Allgemeinverfügungen der Landkreise. Viele juristische Laien, aber auch Experten wussten nicht mehr, wie die aktuelle Rechtslage ist. Aus diesem Grund muss die Transparenz bei vielen Betriebsvereinbarungen unbedingt durch eine klare Auflistung sowie Darstellung der Hierarchie klar gemacht werden.

nen daher spezifische Regelungen zur Veröffentlichung der in Art. 12 ff. DSGVO geforderten Informationen sein.[1466] Eine reine Wiedergabe des Normtextes (z.B. in verändertem Wortlaut) wäre nicht zweckmäßig; ein Verweis hingegen unschädlich.

Für diese Sichtweise spricht auch die Umsetzung des Art. 88 Abs. 2 DSGVO im nationalen Beschäftigtendatenschutzrecht. So finden sich auch dort keine bloßen Wiederholungen der Art. 12 ff., weil dies (außer für „bestimmte Punkte", sofern dies aufgrund ihres inneren Zusammenhangs und für ihre Verständlichkeit für die Adressaten notwendig ist) sogar europarechtswidrig wäre.[1467]

II. Bezeichnung als datenschutzrechtliche Rechtfertigungsgrundlage

In jedem Falle ist es aber unter Berücksichtigung der Transparenzvorgaben erforderlich, dass in der Betriebsvereinbarung ausdrücklich klargestellt wird, dass eine Regelung nicht nur die Ausübung der betriebsverfassungsrechtlichen Mitbestimmungsrechte des Betriebsrats, sondern auch die datenschutzrechtliche Ermächtigungsgrundlage auf Basis von Art. 88 DSGVO bzw. § 26 Abs. 4 DSGVO darstellt.[1468] Nur so können Beschäftigte erkennen, dass die Rechtsgrundlage für die Verarbeitung nicht das „allgemeine" Datenschutzrecht ist, sondern der Arbeitgeber bei der Verarbeitung ihrer personenbezogenen Daten von einer Spezialermächtigung in Form einer Betriebsvereinbarung Gebrauch macht.

III. Regelung zur Konzerndatenübermittlung (Art. 88 Abs. 2 DSGVO)

Sofern Daten innerhalb eines Konzerns übermittelt werden, ist nach Art. 88 Abs. 2 DSGVO erforderlich, dass die Betriebspartner hierfür eine Regelung in der Betriebsvereinbarung treffen, um die Wahrung der menschlichen Würde, der berechtigten Interessen sowie der Grundrechte der betroffenen Arbeitnehmer sicherzustellen. Zwar ist die Vorschrift im Wortlaut deutlich weiter gefasst und könnte so zu verstehen sein,

---

1466 So auch *Haußmann/Brauneisen*, BB 2017, 3065 (3066).

1467 EuGH, Urt. v. 28.03.1985 – C-272/83, BeckRS 2004, 72839, 28 – Kommission/Italien; *Maschmann*, NZA-Beilage 2018, 115 (119).

1468 So auch *Grimm*, ArbRB 2018, 78 (79); *Klösel/Mahnhold*, NZA 2017, 1428 (1432).

dass zwingend Regelungen zur Konzerndatenübermittlung enthalten sein müssen; dies würde allerdings den Zweck der „Spezifizierungsklausel" verfehlen. Nur dort, wo auch tatsächlich eine Konzerndatenübermittlung stattfindet, müssen nach Art. 88 Abs. 2 DSGVO auch Regelungen dazu getroffen werden; insofern muss die Vorschrift teleologisch reduziert werden.[1469]

Obwohl das Thema „Konzerndatenübermittlung" in der Praxis, insbesondere bei People Analytics eine große Rolle spielt, da HR-Daten oftmals nicht nur beim Unternehmen selbst, sondern im Konzern in einer HR-Gesellschaft oder bei der Konzernmutter verarbeitet werden, ist dies nicht Gegenstand dieser Arbeit, die die Datenverarbeitung für Analysezwecke selbst in ihrer Zulässigkeit untersucht. Eine ausführliche Betrachtung der Einzelheiten zur Datenübermittlung in EU-Staaten sowie Drittstatten (mit und ohne Abkommen) würde den Rahmen sprengen und bleibt daher außen vor. In der nachfolgend aufgestellten Muster-Betriebsvereinbarung wird daher ausschließlich die Verarbeitung innerhalb eines Unternehmens betrachtet und geregelt.

IV. Schutzmaßnahmen bei Überwachungssystemen am Arbeitsplatz

Als dritten Aspekt, der von einer datenschutzrechtlichen Beschäftigtendatenschutzspezialregelung aufgegriffen werden muss, nennt Art. 88 Abs. 2 DSGVO die Überwachungssysteme am Arbeitsplatz. In diesem Bereich hat der Betriebsrat auch ein zwingendes Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG.[1470] Soweit in einer Betriebsvereinbarung also Regelungen zu Überwachungssystemen am Arbeitsplatz getroffen, bedarf es zwingend auch Schutzmaßnahmen nach Art. 88 Abs. 2 DSGVO aufgrund der hohen Gefahren für das Persönlichkeitsrecht der Betroffenen. Erfasst werden aufgrund des Wortlauts („Überwachungs*systeme*") nur automatisierte Kontrollverfahren.[1471] Diese bergen – im Vergleich zu nicht-automatisierten Verfahren wie beispielsweise dem Einsatz eines Detektivs – im Einzelfall ein weitaus höheres Gefahrenpotential für die Daten und Rechte der betroffenen Arbeitnehmer.

1469 BeckOK DatenSR/*Riesenhuber*, Art. 88 DSGVO Rn. 88; *Klösel/Mahnhold*, NZA 2017, 1428 (1432).

1470 Siehe bereits ausführlich **D. § 2 II. 1. b**).

1471 Paal/Pauly/*Pauly*, Art. 88 DSGVO Rn. 17; BeckOK DatenSR/*Riesenhuber*, Art. 88 DSGVO Rn. 91; *Wybitul*, ZD 2016, 203 (208).

Bei den untersuchten Advanced People Analytics-Methoden handelt es sich allesamt um Überwachungssysteme im Sinne dieser Vorschrift, da jedes elektronische Gerät, das dazu bestimmt ist, personenbezogene Daten über den Arbeitnehmer zu erheben, davon erfasst ist.[1472] Entsprechende Schutzmaßnahmen für die Rechte der Arbeitnehmer sind daher zwingend in einer legitimierenden Betriebsvereinbarung aufzunehmen.

§ 3 Rahmen- und Einzelbetriebsvereinbarung

Grundsätzlich ist es möglich, neben Einzelbetriebsvereinbarungen zu spezifischen Regelungsbereichen (z.B. Betriebsvereinbarung zum Home-Office, Betriebsvereinbarung zur Nutzung von SAP im Rahmen der Buchhaltung etc.) auch Rahmenbetriebsvereinbarungen zu schließen. Diese legen Bestimmungen für eine Vielzahl von Sachverhalten fest, ohne jedoch die Sachverhalte spezifisch zu regeln.[1473] Mangels abschließender Regelung sind Rahmenbetriebsvereinbarungen zwar nicht erzwingbar[1474], dennoch gerade im Informations- und Kommunikationsbereich von hoher Bedeutung, um beispielsweise Mindeststandards für (jegliche) Datenverarbeitungen im Betrieb, Unternehmen oder Konzern festzulegen.[1475]

Hierdurch lassen sich auch Einzelbetriebsvereinbarungen entzerren, indem beispielsweise Regelungen für Auskunfts- und Informationspflichten nach Art. 12 ff. DSGVO nicht in jeder Einzelbetriebsvereinbarung erneut aufgenommen werden müssen, sondern können mit Hilfe einer Rahmenvereinbarung „vor die Klammer" gezogen werden. Dies trägt u.a. auch zu der teilweise geforderten Transparenz der Regelungen[1476] bei.

Vielfach wird aus diesem Grund der Abschluss von Rahmenbetriebsvereinbarungen empfohlen.[1477]

Überdies können mit dem Instrument der Rahmenbetriebsvereinbarung – bei Bestehen eines Gesamt- oder Konzernbetriebsrats – auch Regelungen

---

1472 BeckOK DatenSR/*Riesenhuber*, Art. 88 DSGVO Rn. 17; insofern besteht eine Parallele zum Wortlaut des § 87 Abs. 1 Nr. 6 BetrVG.

1473 *Oberthür*, A. II. Arten von Betriebsvereinbarungen, in: Oberthür/Seitz, Betriebsvereinbarungen, Rn. 5.

1474 *Oberthür*, A. II. Arten von Betriebsvereinbarungen, in: Oberthür/Seitz, Betriebsvereinbarungen, Rn. 8.

1475 *Schulze/Pfeffer*, ArbRAktuell 2017, 358.

1476 Hierzu **F. § 2 I**.

1477 So etwa in jüngeren Zeitschriftenbeiträgen *Wybitul*, NZA 2017, 1488; *Körner*, NZA 2019, 1389 (1393); *Schulze/Pfeffer*, ArbRAktuell 2017, 358.

auf Unternehmens- bzw. Konzernebene getroffen werden, die für alle Betriebe gelten und konkrete Regelungen den örtlichen Betriebsräten überlassen werden, sofern die gesetzliche Zuständigkeitsverteilung gewahrt bleibt; eine Delegation von Kompetenzen ist dabei nicht möglich.[1478]

Im Bereich von People Analytics werden hingegen kaum Regelungen „nur" auf Betriebsebene getroffen werden, da die HR-Abteilung in aller Regel auf Unternehmens-, wenn nicht sogar auf Konzernebene angesiedelt ist und gerade Analysen zentral durchgeführt werden, sofern es das Datenschutzrecht (im Hinblick auf das fehlende Konzernprivileg) zulässt. Dennoch werden auch hier Rahmen- und Einzelbetriebsvereinbarungen eingesetzt, um allgemeine datenschutzrechtliche Standards für alle Datenverarbeitungen festzulegen und wiederum Einzelbereiche in spezifischen Betriebsvereinbarungen zu regeln.

Im Nachfolgenden werden zur Veranschaulichung auch Regelungen, die üblicherweise in einer Rahmenbetriebsvereinbarung geregelt würden, in der Einzelbetriebsvereinbarung aufgenommen, um eine vollständige Abdeckung der notwendigen Regelungen für eine „*People Analytics-BV*" zu erzielen.

Bevor jedoch auf die einzelnen Aspekte der Regelung eingegangen wird, wird zuvor noch aufgezeigt, welche Bereiche typischerweise in der Rahmenbetriebsvereinbarung und welche in der Einzelbetriebsvereinbarung „People Analytics" geregelt würden.

I. Rahmenbetriebsvereinbarung „IKT"

Wie bereits dargestellt, kommen in die Rahmenbetriebsvereinbarung vor allem Regelungen, die auf alle Datenverarbeitungen anwendbar sind und nicht anwendungsspezifisch für eine bestimmte Applikation oder Datenverarbeitungssituation sind. Hierzu zählen insbesondere Regelungen zu Auskunfts- und Informationsansprüchen (etwaige Konkretisierungen der Pflichten aus Art. 12 ff. DSGVO), allgemeine Bestimmungen zur Zweckbestimmung und -bindung, Vorgaben zur Systemdokumentation, ein etwaiger Ausschluss von Leistungs- und Verhaltenskontrollen, Vorgaben zur Auftragsverarbeitung (z.B. Unterrichtung des Betriebsrats, Gestaltungsvorgaben für Auftragsverarbeitungsverträge), Vorgaben zu sonstigen Über-

1478 *Oberthür*, A. II. Arten von Betriebsvereinbarungen, in: Oberthür/Seitz, Betriebsvereinbarungen, Rn. 7; zur Unzulässigkeit der Delegierung von Kompetenzen, BAG, Beschl. v. 21.01.2003 – 3 ABR 26/02, NJOZ 2003, 2274 f. Os. 2.

mittlungen an Dritte, ein Berechtigungskonzept, Bestandsverzeichnis (als Anlage) sowie das Verfahren bei Streitigkeiten.[1479]

Auch Vorgaben zur (wirksamen) Einwilligung von Arbeitnehmern im Beschäftigungskontext können Eingang in eine solche Rahmenbetriebsvereinbarung finden.[1480]

II. Einzelbetriebsvereinbarung „People Analytics“

In der Einzelbetriebsvereinbarung „*People Analytics*“ hingegen werden alle Spezifika für die geplanten Analytics geregelt. Wie sich bereits aus der bisherigen Untersuchung ergibt, gibt es an vielen Stellen „Einfallstore“ für betriebliche Sonderregelungen bzw. machen Spezialregelungen an vielen Stellen Sinn, um den unbestimmten Begriff der „Erforderlichkeit“ (für die Entscheidung über die Begründung bzw. Durchführung des Beschäftigungsverhältnisses) weiter zu konkretisieren bzw. eine Subsumtion unter den gesetzlichen Begriff zu vermeiden und hierdurch Rechtsunsicherheiten gar nicht erst entstehen zu lassen. Ebenfalls sinnvoll ist es auch in diesem Rahmen die Möglichkeit, spezieller Einwilligungen von Arbeitnehmern (z.B. für „persönliche Dashboards“) unter Beachtung des grundsätzlichen Prinzips der Freiwilligkeit der Einwilligung näher zu regeln.

Unter Rückgriff auf die untersuchten People Analytics-Anwendungsszenarien sollten folgende Punkte in einer Einzelbetriebsvereinbarung geregelt werden: Nutzung von IT-Logdaten für Analytics-Zwecke, zulässige Zweckänderungen, Profiling und Scoring, automatisierte (Einzelfall-)Entscheidungen, Einsatz von Dashboards und Netzwerk-Graphen/-Analysen.

Weiterhin – jedoch hier außer Betracht bleibend –müssen zwingend die Übermittlung von Daten innerhalb eines Konzerns geregelt und in diesem Rahmen Grenzen sowie Schutzmaßnahmen klar festgelegt werden, falls eine solche stattfinden soll.

§ 4 Einzelregelungen einer „People Analytics-BV“

Im Nachfolgenden sollen die (notwendigen) Regelungen einer Betriebsvereinbarung mit Schwerpunkt People Analytics untersucht und dabei die Regelungsspielräume der Betriebsparteien aufgezeigt werden. Der Fokus

1479 Siehe hierzu *Schulze/Pfeffer*, ArbRAktuell 2017, 358.
1480 Vgl. *Grimm*, ArbRB 2018, 122 (123).

wird auf die unter **F. § 3** aufgezählten Regelungsbereiche – auch im Rahmen von Rahmenbetriebsvereinbarungen – gelegt, sodass im Endeffekt eine schlüssige Gesamtregelung zu People Analytics in einem Unternehmen entsteht.

Es wird davon ausgegangen, dass keine Übermittlung innerhalb eines Konzerns stattfindet und die Daten ausschließlich im Unternehmen verarbeitet werden, also auch keine Auftragsverarbeitung (z.B. durch die Nutzung von Cloud-Anbietern) stattfindet. Insbesondere ersterer Aspekt bedürfte aufgrund von Art. 88 Abs. 2 DSGVO einer Regelung in einer Betriebsvereinbarung. Bei der Auftragsverarbeitung hingegen muss zunächst mit dem jeweiligen Drittanbieter verhandelt werden, inwiefern eine Anpassung auf die betrieblichen Gegebenheiten möglich ist; aus diesem Grund kann an dieser Stelle keine pauschale Aussage getroffen werden, sodass dieser Bereich ebenfalls außer Betracht bleibt.[1481]

I. Präambel

In einem ersten Schritt ist – nicht zuletzt aufgrund des Transparenzerfordernisses – jeder Betriebsvereinbarung eine Präambel voranzustellen, die festlegt, dass die geschlossene Betriebsvereinbarung gleichzeitig auch eine Legitimationsgrundlage für die Datenverarbeitung darstellt.[1482] Für eine *People Analytics*-Betriebsvereinbarung (im Folgenden: PA-BV) könnte diese wie folgt lauten:

> *Bereits aus der Bezeichnung „Human Ressources" geht hervor, dass das Humankapital eines Unternehmens – im Gegensatz zu den Anfängen der Personalarbeit – ein wesentlicher Faktor für den Erfolg eines Unternehmens ist. Entscheidend prägen also die fachlichen und sozialen Fähigkeiten der Mitarbeiter den wirtschaftlichen Erfolg unseres Unternehmens XY. Gerade in der aktuellen Zeit, in welcher Arbeit in hohem Maße digitalisiert wird und der persönliche Kontakt auch unter den Kollegen abnimmt sowie die Unternehmensstrukturen immer komplexer werden, ist es von entscheidender Bedeutung für die Zufriedenheit der Arbeitnehmerschaft, dass innerbetriebliche Prozesse möglichst effizient ablaufen und Probleme frühzeitig erkannt*

1481 Zu den Vorgaben der Auftragsdatenverarbeitung (noch unter altem Recht) bei der Nutzung von Persönlichkeitsanalysetools, vgl. *Eckhardt/Kramer*, DuD 2016, 144.

1482 Hierzu bereits **F. § 2 II**.

*und behoben werden. Hierfür setzt XY die Methode **People Analytics** ein, die den Entscheidungsträgern ermöglichen soll, etwaige Ungereimtheiten im Betriebsablauf bereits frühzeitig zu erkennen und gegensteuern zu können. Eine niedrige Reaktionszeit ist erforderlich, um mit den Maßnahmen nicht immer einen Schritt hinterherzuhinken, sondern eine Steuerung in Echtzeit zum Vorteil der Arbeitnehmerschaft zu ermöglichen.*

*XY setzt im Rahmen von People Analytics auf die **Auswertung von IT-Nutzungsdaten** und nutzt die Techniken des **Profilings und Scorings**, um den Arbeitnehmern und Entscheidungsträgern im Unternehmen in verständlicher Form alle für sie wesentlichen Informationen in **Dashboards** darzustellen und rasche Entscheidungen zu ermöglichen. Um Kommunikationsabläufe zu verbessern, wird die **Netzwerk-Analyse** eingesetzt.*

Alltägliche Prozesse sollen durch automatisierte Entscheidungen beschleunigt und vereinfacht, somit das Human Resources Management entlastet und schnelle Entscheidungen ermöglicht werden.

*Damit diese Form des modernen und evidenzbasierten Personalmanagements ermöglicht werden kann, wird folgende Vereinbarung geschlossen, die gleichzeitig auch als **datenschutzrechtliche Legitimationsgrundlage** für die hierfür erforderlichen Verarbeitungsvorgänge nach Art. 88 Abs. 1 DSGVO, § 26 Abs. 4 BDSG gilt. Um die gesetzlichen Vorgaben der DSGVO und des BDSG einzuhalten, regelt diese Vereinbarung die betriebsverfassungsrechtlichen und datenschutzrechtlichen Rahmenbedingungen für den Einsatz von People Analytics **abschließend**.*

Eine Präambel muss nicht die dargestellte Ausführlichkeit und Präzision besitzen, dennoch empfiehlt es sich – in „einfachem Deutsch“ – in der Präambel voranzustellen, welche Bereiche die Betriebsvereinbarung regelt, sodass ein interessierter Mitarbeiter einen schnellen Überblick über den Regelungsgegenstand bekommt, ohne sich durch den vollständigen, mitunter technisch und sprachlich sehr komplexen Regelungsbereich durcharbeiten zu müssen. Insbesondere wenn die Betriebsvereinbarung auch als datenschutzrechtliche Legitimationsgrundlage gilt, ist die PA-BV die Haupterkenntnisquelle dafür, ob eine Datenverarbeitung rechtmäßig ist oder nicht.

In der Information nach Art. 13 DSGVO ist diese daher auch als Legitimationsgrundlage aufzuführen.

II. Gegenstand und allgemeine Grundsätze der Datenverarbeitung

Im normativen Bereich der Betriebsvereinbarung sind in weiterer Folge der Anwendungsbereich und Gegenstand der Regelung klar abzugrenzen und notwendige Begriffe zu bestimmen. Hierbei sollte aufgrund von Art. 88 Abs. 2 DSGVO statuiert werden, dass die Regelung eine angemessene und besondere Maßnahme zur Wahrung der berechtigten Interessen, der menschlichen Würde und Grundrechte sowie des Schutzes der Persönlichkeit der beschäftigten Arbeitnehmer darstellt:

> ***§ 1 Anwendungsbereich, Gegenstand und allgemeine Grundsätze der Datenverarbeitung***
>
> *(1) Diese Betriebsvereinbarung gilt für alle Arbeitnehmer im Sinne des § 5 Abs. 1 BetrVG, mit Ausnahme der leitenden Angestellten, und für jegliche Datenverarbeitungen, die im Zusammenhang mit der Analyse von personenbezogenen Daten von Arbeitnehmern zum Zwecke des Personalmanagements (People Analytics) stattfinden. Die Begriffsdefinitionen, soweit nicht ausdrücklich anders definiert, entsprechen denjenigen aus Art. 4 DSGVO.*

Nota bene: Der Sprecherausschuss kann gem. § 28 Abs. 1 SprAuG mit dem Arbeitgeber Richtlinien über den Inhalt, Abschluss oder die Beendigung von Arbeitsverhältnissen der leitenden Angestellten schriftlich vereinbaren; dieser Inhalt gilt gem. Abs. 2 unmittelbar und zwingend. In diesem Zusammenhang könnte beispielsweise zwischen Arbeitgeber und Sprecherausschuss vereinbart werden, dass die Regelungen der Betriebsvereinbarung auch für leitende Angestellte gelten. Besteht kein Sprecherausschuss, muss eine individuelle Bezugnahme auf die PA-BV im Arbeitsvertrag oder einer Zusatzvereinbarung erfolgen.

> *(2) Gegenstand dieser Vereinbarung ist die Regelung angemessener und besonderer Maßnahmen zur Wahrung der berechtigten Interessen, der menschlichen Würde und der Grundrechte sowie des Schutzes der Persönlichkeit der Arbeitnehmer gem. Art. 88 Abs. 2 DSGVO beim Einsatz von People Analytics.*

Werden in der Vereinbarung bestimmte Begrifflichkeiten verwendet, die gesetzlich nicht definiert sind, empfiehlt es sich zur Vermeidung von Streitigkeiten auch diese in einer Norm zu Beginn zu definieren und bei mehrfacher Verwendung auf Definitionen in einzelnen Klauseln zu verzichten.

Dies erhöht die Lesbarkeit der Vereinbarung und schafft weitere Transparenz:

> ***§ 2 Begriffsbestimmungen***
>
> 1. *„Scoring“ ist die Verwendung eines Wahrscheinlichkeitswertes, welcher über ein wissenschaftlich-anerkanntes, mathematisches Verfahren berechnet wird, über ein bestimmtes zukünftiges Verhalten einer natürlichen Person im Hinblick auf die Untersuchungsfrage.*
>
> 2. *„Score“ ist das Ergebnis eines Scoring-Vorgangs und stellt einen bestimmten Wahrscheinlichkeitswert über ein bestimmtes zukünftiges Verhalten einer natürlichen Person im Hinblick auf die Untersuchungsfrage dar. Dieser kann entweder in Prozent oder in Form einer Punktezahl im Rahmen eines vorgegebenen Schemas in Erscheinung treten.*
>
> 3. *„Ranking“ ist ein Verfahren, bei welchem in einer abschließenden Liste die Inhalte der Liste nach einem vorgegebenen, wissenschaftlich-anerkannten, mathematischen Verfahren mit Blick auf die Passgenauigkeit zur Untersuchungsfrage gereiht werden. Das zugrundeliegende Verfahren stellt in der Regel ein „Scoring“ bzw. eine Kombination verschiedener Score-Werte dar.*
>
> 4. *„Dashboard“ ist eine Visualisierungsform für Daten. Dashboards werden im Rahmen dieser Betriebsvereinbarung dazu eingesetzt, um die aus People Analytics gewonnenen Daten für die jeweilige Zielperson der Analyse übersichtlich darzustellen.*
>
> 5. *„Netzwerk-Graph“ ist ein grafisches Tool zur Darstellung der informellen Hierarchie im Unternehmen. Er basiert auf der Auswertung von Kommunikationsdaten der Arbeitnehmer im Unternehmen.*

III. Datenschutzrechtliche Grundsätze für die Datenverarbeitung und Überwachungsmaßnahmen

Neben der Bezugnahme auf die allgemeinen datenschutzrechtlichen Grundsätze (in § 1 PA-BV) sollten auch noch spezifische Grundsätze für die Datenverarbeitung im Rahmen von People Analytics getroffen werden. Hierzu gehören besondere Regelungen zur Zweckbindung und -vereinbar-

keit sowie zu Überwachungsmaßnahmen[1483]. Insbesondere letztere sind – wie unter **E. § 1 III. 2. a**) und **E. § 4 II. 1** dargestellt – grundsätzlich ebenfalls Überwachungsmaßnahmen, sodass der nicht-repressive Einsatz aufgrund von Art. 88 Abs. 2 BDSG einer besonderen Regelung bedarf.

> ***§ 3 Datenschutzrechtliche Grundsätze für die Anwendung von People Analytics***
>
> *(1) Die in Art. 5 Abs. 1 lit. a bis f DSGVO festgelegten Datenschutzgrundsätze sind Inhalt dieser Vereinbarung und gelten für jegliche Verarbeitungen personenbezogener Daten der Arbeitnehmer und Beschäftigten nach § 26 Abs. 8 BDSG für die Zwecke von People Analytics (vgl. § 1 Abs. 1 dieser Vereinbarung).*
>
> *(2) Personenbezogene Daten aus informationstechnischen Systemen, die nicht für die Zwecke von People Analytics erhoben wurden, dürfen – außer im Rahmen einer anonymisierten Verarbeitung – nicht für diesen Zweck verarbeitet werden. Ein Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO findet nicht statt. Ausnahmen sind gesondert unter Bezugnahme zu dieser Regelung spezifizieren.*

Obwohl insbesondere im Bereich der *Simple People Analytics* eine Zweckvereinbarkeit oftmals gegeben ist, empfiehlt es sich, eine solche Regelung aufzunehmen. Hierdurch werden Streitigkeiten über eine Zweckvereinbarkeit der Nutzung von IT-Daten für People Analytics-Zwecke vermieden. Zudem ist sichergestellt, dass die Arbeitnehmer bereits zum Zeitpunkt der Erhebung informiert sind und nicht befürchten müssen, dass etwaige Daten später mit dem Argument der Zweckkompatibilität für Auswertungen heranzogen werden. Für *Advanced People Analytics* ist nach hiesiger Auffassung ist eine Zweckkompatibilität ohnehin nicht gegeben,[1484] sodass in diesem diese Klausel nur deklaratorisch ist und keinen weitergehenden Regelungsgehalt besitzt. Sie kann dennoch zu einer höheren Akzeptanz bei den Beschäftigten bzw. der Interessensvertretung sorgen. Mangels rechtlicher Gefahren für die Arbeitnehmer werden allerdings zweckkompati-

1483 *Grimm*, ArbRB 2018, 122 (124).
1484 Siehe **E. § 1 III. 2. b**) (**3**).

ble Anonymisierungsvorgänge für anonymisierte APA-Maßnahmen vom strengen Zweckbindungsgrundsatz ausgenommen.[1485]

(3) *Zur Gewährleistung der Transparenz der Datenverarbeitung werden die Arbeitnehmer bei der Nutzung von IT-Daten in einfacher und verständlicher Sprache über die Kategorien der über sie erhobenen IT-Daten in regelmäßigen Abständen (monatlich) per E-Mail informiert. Die Spezifizierung der Kategorie hat so ausführlich wie möglich zu erfolgen.*

Mögliche Kategorien sind beispielsweise bei E-Mail-Daten: Empfänger (sofern intern), Absender (sofern intern) Sendedatum/-zeit; bei Instant-Messaging (intern): Empfänger bzw. Sender sowie Übermittlungszeit; Office-Auswertungen: Dateiname, Zeitstempel der Dateiöffnung, Zeitstempel der Speicherung.

Eine Information des Betroffenen ist nach Art. 13 DSGVO nur bei der Erhebung notwendig. Dabei ist es ausreichend, dass der Verarbeiter dem Betroffenen die Information auf einer Website bereitstellt.[1486] Sofern die betroffene Person allerdings bereits über die Information der Verarbeitung verfügt, ist keine Information erforderlich (Art. 13 Abs. 4 DSGVO). Zu einer regelmäßigen Information ist der Arbeitgeber nicht verpflichtet. Dennoch kann eine solche sinnvoll sein, um das Bewusstsein über die erfolgende Datenverarbeitung zu stärken, damit eine solche nicht in „Vergessenheit“ gerät. Werden die Daten nicht bei der betroffenen Person erhoben, so muss der Verantwortliche nach Art. 14 Abs. 3 DSGVO unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer angemessenen Frist nach Erlangung, jedoch spätestens nach einem Monat den Betroffenen informieren. Auch hier entfällt die Informationspflicht – analog der Regelung bei der Direkterhebung – nach Art. 14 Abs. 5 lit. a DSGVO, wenn und so weit die betroffene Person bereits über die Information verfügt.[1487] Insofern gilt das soeben Gesagte.

1485 Diese bedürften aufgrund der Statistik-Ausnahme in Art. 5 Abs. 1 lit. b DSGVO ohnehin keinem Kompatibilitätstest.

1486 EuArbRK/*Franzen*, Art. 5 DSGVO Rn. 5; einschränkend BeckOK DatenSR/*Schmidt-Wudy*, Art. 13 DSGVO Rn. 85: nur wenn die Daten ausschließlich für den Betroffnen abrufbar sind; a.A. *Bäcker*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 13 DSGVO Rn. 59: aktive Unterrichtung erforderlich; Bereitstellung auf Website nicht ausreichend.

1487 *Bäcker*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, Art. 14 DSGVO Rn. 52.

(4) Soweit es die Auswertungsziele zulassen, werden keine personenbezogenen Daten durch die Systeme der XY erhoben. Ist eine anonyme Datenerhebung nicht möglich, so werden die Daten unverzüglich nach der Erhebung in größtmöglichem Maße aggregiert bzw. anonymisiert. In jedem Falle findet eine Pseudonymisierung der Daten statt.

Aufgrund des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) müssen die Daten auf das für die Zwecke der Verarbeitung erforderliche Maß beschränkt sein; selbiges ergibt sich auch aus § 26 Abs. 1 S. 1 BDSG. Sofern also personenbezogene Auswertungen (wie beispielsweise bei Netzwerk-Graphen) nicht erforderlich sind, sondern aggregierte Daten (z.B. auf Abteilungsebene) ausreichen, sind die Daten zu anonymisieren bzw. – soweit möglich – bereits anonymisiert zu erheben. Die Pseudonymisierung hingegen ist eine technisch-organisatorische Maßnahme zur Datensicherung[1488] und wirkt für den Verarbeiter selbst daher nicht pauschal legitimierend. Im Rahmen der Interessensabwägung kann sie jedoch ermöglichende Wirkung haben, sofern hierdurch weniger Gefahren für die Rechte der Arbeitnehmer bestehen.[1489] Dies wäre der Fall, wenn der Zuordnungsschlüssel gesondert aufbewahrt wird und daher sichergestellt ist, dass eine zufällige Re-Identifizierung des Betroffenen ausscheidet. Der Schlüssel kann beim selben Verantwortlichen liegen, sofern er ausreichend vor unbefugten Zugriffen geschützt ist; eine Einschaltung eines Datentreuhänders ist nicht erforderlich.[1490]

(5) Sofern für die Analysen keine Zuordnung zu einer bestimmbaren Person notwendig ist, sondern eine Auswertung unter einem Pseudonym ausreichend ist, wird der Zuordnungsschlüssel durch eine doppelte Verschlüsselung gesichert. In diesem Rahmen ist es erforderlich, dass die Geschäftsführung von XY und der (Gesamt-)Betriebsrat nur gemeinsam die Entschlüsselung vornehmen können. Die Verschlüsselung muss dem Stand der Technik entsprechen. Eine Entschlüsselung darf nur im Falle eines Straftatverdachts oder einer groben Pflichtverletzung durch den Arbeitnehmer erfolgen.

1488 *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 5 Rn. 2; *Article 29 Data Protection Working Party*, WP 203, S. 3; weitere Nachweise in Fn. 277.

1489 Hierzu **D. § 1 I. 4. c) bb)**.

1490 Vgl. Erwägungsgrund 29; ausführlich unter **D. § 1 I. 4. d)**.

Durch die doppelte Absicherung des Zuordnungsschlüssels wird, sollten Daten bei etwaigen Straftaten oder groben Pflichtverletzungen für repressive Zwecke erforderlich sein, sichergestellt, dass kein einseitiger Missbrauch der Daten stattfindet. Die Voraussetzungen sind geringer als die die des § 26 Abs. 1 S. 2 BDSG, da dort eine grobe Pflichtverletzung nicht ausreichend, sondern ein Straftatverdacht erforderlich ist. Durch klar festgelegte Situationen, in denen eine Dekodierung erfolgen darf, werden die personenbezogenen Daten der Arbeitnehmer besonders gesichert und die Pseudonymisierung entfaltet im Rahmen der Interessenabwägung für Analytics eine privilegierende Wirkung.

IV. Transparenzvorgaben sowie Informations- und Auskunftsrechte der Arbeitnehmer

Im Nachfolgenden werden in Bezug auf verschiedene Anwendungsszenarien mögliche und sinnvolle (allgemeine) Regelungen zur Transparenz dargestellt sowie Konkretisierungsansätze für die allgemeinen Informations- und Auskunftspflichten aus Art. 13 ff. DSGVO aufgezeigt.

§ 4 Datenschutzrechtliche Information

(1) In Form einer „Datenschutzrechtlichen Information zur Erhebung von Beschäftigtendaten“[1491] *wird den Arbeitnehmern eine leicht zugängliche Information über die Pflichten des Arbeitgebers nach dieser Betriebsvereinbarung, dem BDSG und der DSGVO sowie über die Rechte der Arbeitnehmer in Form einer PDF zur Verfügung gestellt. Diese Information wird laufend aktualisiert und die Arbeitnehmer bei Änderungen per E-Mail informiert. Die Information ist in einer verständlichen, klaren und einfachen Sprache zu verfassen. In der in § 3 Absatz 3 genannten zyklischen Information ist diese Information mit einem Hyperlink zu verknüpfen.*

(2) In der Information nach Absatz 1 ist zu erläutern, in welchem Regelungszusammenhang diese Betriebsvereinbarung zu anderen Betriebsvereinbarungen sowie sonstigen betrieblichen Vorgaben und Regelungen steht. Die Normenhierarchie ist grafisch darzustellen.

1491 Beispiel aus *Grimm*, ArbRB 2018, 122 (124).

Die Arbeitnehmer sollen zusätzlich zur monatlichen Information über ihre verarbeiteten Daten allgemeine datenschutzrechtliche Informationen erhalten, um sich einen schnellen Überblick über ihre Rechte und deren Wahrnehmung verschaffen zu können. Dies dient der formellen Transparenz.[1492]

§ 5 Einrichtung einer FAQ-Seite

Zusätzlich zur Veröffentlichung des Normtextes dieser Betriebsvereinbarung wird im Intranet eine „Frequently Asked Questions (FAQ)"-Seite eingerichtet, auf welcher der Normtext dieser Vereinbarung in leichter und verständlicher Sprache erläutert wird. Ergeben sich (allgemeine) Fragen von Arbeitnehmern zu dieser Vereinbarung, sind diese inklusive Beantwortung in den Katalog aufzunehmen. Die FAQ gelten nicht normativ, dienen jedoch aus Auslegungshilfe für die Regelungen in dieser Vereinbarung.

Diese Regelung erfolgt ebenfalls in Erfüllung des Transparenzgebots.[1493]

§ 6 Verzeichnis der Verarbeitungstätigkeiten

Der Arbeitgeber erstellt – zusätzlich zu einem Verzeichnis nach Art. 30 DSGVO – ein Verzeichnis der Verarbeitungstätigkeiten für die einzelnen Verarbeitungsvorgänge nach dieser Betriebsvereinbarung. Es sind die Vorgaben des Art. 30 DSGVO einzuhalten und das Verzeichnis dieser Betriebsvereinbarung anzuhängen.

Das spezifische Verzeichnis der Verarbeitungstätigkeiten dient dazu, einen schnellen Überblick über die nach dieser Betriebsvereinbarung legitimierten Verarbeitungsvorgänge, Kategorien und Empfängern von Daten sowie Löschfristen und technisch-organisatorische Sicherungsmaßnahmen zu erhalten.

§ 7 Informations- und Auskunftsrechte der Arbeitnehmer

(1) Es gelten die gesetzlichen Informations- und Auskunftsrechte gem. Art. 13 ff. DSGVO und §§ 32 ff. BDSG.

1492 *Grimm*, ArbRB 2018, 122 (124).
1493 Siehe hierzu bereits **F. § 2 I.**

(2) In Ergänzung zu den gesetzlichen Informations- und Auskunftsrechten erfolgen in dieser Vereinbarung Konkretisierungen zur Information durch den Arbeitgeber im Rahmen der einzelnen Verarbeitungssituationen.

(3) Die Informationserteilung erfolgt per E-Mail an die dienstliche E-Mail-Adresse des Arbeitnehmers. In begründeten Fällen kann der Arbeitnehmer vom Arbeitgeber eine schriftliche Information verlangen. In jedem Fall ist die Information unentgeltlich zur Verfügung zu stellen. Eine mündliche Information scheidet aus.

§ 7 PA-BV dient zur Konkretisierung der datenschutzrechtlichen Informationspflichten. Da Art. 12 Abs. 1 DSGVO für die Information die Schriftform oder eine andere Form, „gegebenenfalls auch elektronisch“, vorschreibt, ist eine Konkretisierung nach Art. 88 Abs. 2 DSGVO zulässig. Die mündliche Informationserteilung hingegen ist nach Art. 12 Abs. 1 S. 3 DSGVO zwar grundsätzlich ebenfalls zulässig, aufgrund der Komplexität der Analytics-Sachverhalte aber nicht zweckdienlich. Aus diesem Grund wird eine solche Informationserteilung ausgeschlossen. Art. 12 Abs. 1 S. 3 DSGVO ermöglicht lediglich eine mündliche Informationserteilung, falls der Betroffene dies verlangt. Es wird jedoch keine Pflicht des Verantwortlichen statuiert, sodass in einer Betriebsvereinbarung abweichende Regelungen möglich sind.

V. Datenschutzrechtliche Legitimationen

Zusätzlich zur Bezeichnung als datenschutzrechtliche Legitimationsgrundlage in der nicht-normativen Präambel ist es erforderlich, dass die datenschutzrechtlichen Legitimationen für die einzelnen Anwendungsfelder von People Analytics klar festgelegt werden, um den Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. a DSGVO) sowie der Rechtmäßigkeit und Verarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. b DSGVO) einzuhalten.

Im Folgenden werden einige im Rahmen der Untersuchung genannten Szenarien für zulässige People Analytics beispielshaft geregelt.

1. Advanced People Analytics

In einem ersten Schritt sollte die Erhebung bestimmter IT-Systemdaten zur Nutzung für People Analytics legitimiert werden. Pauschale Aussagen verbieten sich an dieser Stelle, sodass verschiedene mögliche Szenarien für den Einsatz von People Analytics dargestellt sowie Regelungsvorschläge aufgezeigt werden sollen.

Szenario 1: Das Unternehmen XY ist ein Versicherungsunternehmen und möchte wissen, wie viele Versicherungsanträge, Policenanpassungen und Beschwerden ein Sachbearbeiter pro Niederlassung im Schnitt pro Tag verarbeitet. Die eingesetzte Software lässt hierbei jeden Vorgang, den ein Sachbearbeiter vornimmt, in diese drei Kategorien einordnen und speichert zu jedem Vorgang den Bearbeiter sowie einen Zeitstempel. Bei der Einführung des Systems war eine Auswertung der Daten für Analysezwecke nicht geplant.

Zu beachten ist hier, dass das Unternehmen lediglich eine Auswertung auf Niederlassungsebene wünscht, die Daten im System aber auf Bearbeiterebene gespeichert werden. Diese Daten werden für die Zuordnung der Vorgänge für Kundenrückfragen sowie Missbrauchsfälle gespeichert. Für die Nutzung in People Analytics müssen diese also aggregiert werden.

§ 8 Vorgangsanalyse von Versicherungsfällen pro Niederlassung

(1) XY ist es gestattet, die personenbezogenen Daten der Arbeitnehmer für die Zwecke der Vorgangsanalyse von Versicherungsfällen auf Niederlassungsebene auszuwerten.

(2) Als Vorgangsanalyse von Versicherungsfällen wird die Berechnung einer durchschnittlichen Anzahl von bearbeiteten Fällen pro Sachbearbeiter und Niederlassung verstanden. Es erfolgt eine Untergliederung der Daten in die Kategorien „Gesamt", „Versicherungsanträge", „Policenanpassungen" und „Beschwerden".

(3) Vor einer Weiterverarbeitung sind die aus dem System ABC verwendeten Daten auf Niederlassungsebene zu aggregieren. Die Bearbeiterkennung des Sachbearbeiters ist aus dem Datensatz zu entfernen. Darüber hinaus hat XY sicherzustellen, dass keine Identifizierbarkeit eines Sachbearbeiters möglich ist. Die Verknüpfung mit weiteren Daten zu weite-

ren Verarbeitungszwecken ist vorbehaltlich einer gesonderten Regelung verboten.

Im vorliegenden Fall ist eine rückwirkende Verarbeitung der Daten nach § 3 Abs. 2 PA-BV möglich, da es sich um anonymisierte Daten handelt. Aufgrund der Anonymität der Daten sind diese nach erfolgter Anonymisierung nicht mehr vom Datenschutzrecht erfasst. Zur Sicherstellung, dass nicht durch Verknüpfung mit anderen Daten diese wieder unbemerkt personenbezogen werden, wird ein Verknüpfungsverbot für die Daten festgelegt.

Szenario 2: Im Unternehmen XY beschwert sich eine Vielzahl von Arbeitnehmern beim Betriebsarzt über Kopf- und Rückenschmerzen. Der Betriebsarzt vermutet als Ursache zu lange Bildschirmarbeitszeiten, verbunden mit zu wenig Pausen. Er möchte seine Vermutung durch eine Auswertung der täglichen PC-Arbeitszeiten der betroffenen Arbeitnehmer bekräftigen und hierdurch auch andere potenziell gefährdete Arbeitnehmer identifizieren, um bei diesen gezielt ein Programm zur Gesundheitsprävention durchführen zu können.

In diesem Szenario ist es nicht die HR-Abteilung, die personenbezogene Daten für People Analytics nutzen möchte, sondern der Betriebsarzt. Die tägliche Bildschirmzeit des jeweiligen Arbeitnehmers stellt kein sensitives Datum im Sinne des Art. 9 Abs. 1 DSGVO dar.

Insbesondere handelt es sich nicht um Gesundheitsdaten gem. Art. 4 Nr. 15 DSGVO, da die Kenntnis der Bildschirmarbeitszeit noch keine Rückschlüsse auf den Gesundheitszustand des Beschäftigten zulässt. Werden diese im Rahmen der betriebsärztlichen Untersuchung mit den Daten vom Betriebsarzt verknüpft, werden diese allerdings zu sensitiven Daten, da diese dann in den Kontext zur Gesundheit gestellt werden. Spätestens zu diesem Zeitpunkt schreibt das Gesetz in § 22 Abs. 1 Nr. 1 lit. b BDSG vor, dass die Verarbeitung durch das ärztliche Personal selbst oder unter deren Verantwortung erfolgt. Der Datenbestand muss also von Zugriffen durch den Arbeitgeber geschützt werden und von den sonstigen Daten abgesondert werden.[1494]

Unabhängig von einer etwaig gesetzlich vorgeschriebenen Absonderung sind die Daten zur Bildschirmnutzung unter dem Aspekt der Erforderlich-

1494 Siehe hierzu bereits **E. § 1 III. 2. c) dd) (2) (d)**.

keit der Datenverarbeitung auch schon vor einer Verknüpfung mit Gesundheitsdaten vor Zugriffen durch den Arbeitgeber zu schützen, da sich hierdurch eine Überwachung der Arbeitnehmer statuieren ließe, die im Rahmen der Bewertung der Eingriffsintensität zu berücksichtigen ist.[1495] Da bei der Verarbeitung (auch durch die Betriebsärztin) Beschäftigungszwecke verfolgt werden, kann eine solche (anders als beispielsweise reine Gesundheits-Apps zur Aufrechterhaltung der Fitness der Arbeitnehmer) in einer Betriebsvereinbarung geregelt werden.

§ 9 Erfassung der Bildschirmarbeitszeit zur Gesundheitsvorsorge

(1) Die Betriebsärztin Maxi Musterfrau erfasst im Rahmen des Arbeitsschutzes und der Gesundheitsvorsorge die Bildschirmarbeitszeiten der Arbeitnehmer. Die Verarbeitung und Erfassung dieser personenbezogenen Daten wird für die Auswertung zur Vermeidung von Überbelastungen durch diese Betriebsvereinbarung legitimiert.

(2) Der Datenbestand ist gesondert vom sonstigen Datenbestand der XY zu erfassen und insbesondere vor Zugriffen durch den Arbeitgeber durch geeignete Maßnahmen nach dem Stand der Technik zu schützen. Verantwortliche Verarbeiterin ist allein Maxi Musterfrau; eine Weitergabe der Daten an Dritte, auch an den Betriebsrat, ist nicht gestattet.

(3) Jeder Arbeitnehmer hat jederzeit die Möglichkeit der Datenverarbeitung für den in Absatz 1 genannten Zweck zu widersprechen. Im Falle eines Widerspruchs ist der gesamte Datensatz zu diesem Arbeitnehmer, der im Rahmen von Absatz 1 erhoben wurde, unverzüglich zu löschen und der Arbeitnehmer über die erfolgte Löschung zu informieren.

(4) Die Betriebsärztin verarbeitet diese Daten ausschließlich zur Gesundheitsvorsorge und Prävention sowie im Rahmen von Behandlungen der betroffenen Arbeitnehmer.

Hierbei sollte der Betriebsarzt in der Betriebsvereinbarung explizit erwähnt werden, sodass eine Weitergabe der Daten an einen (Folge-)Betriebsarzt ausscheidet bzw. nur mit Einwilligung der Arbeitnehmer erfolgen kann. Hintergrund hierfür ist, dass in der Regel ein besonderes Vertrauensverhältnis zum Arzt besteht, welches Grundlage für das Unterlassen

1495 Vgl. zu den Kriterien bei Überwachungsmaßnahme **E. § 4 II. 1. d) bb)**.

eines Widerspruchs sein kann. Im Rahmen der Interessensabwägung sind etwaige Widerspruchsrechte zu berücksichtigen.[1496]

Zu beachten ist, dass einem Arbeitnehmer eine nicht-gewünschte Gesundheitsvorsorge, die nur zu seinem eigenen Schutz dient, nicht aufgedrängt werden kann. So lässt sich auch die gesetzliche Wertung des Art. 9 Abs. 2 lit. b DSGVO verstehen, wonach eine Datenverarbeitung zum Schutz lebenswichtiger Interessen ohne Einwilligung nur möglich ist, wenn der Betroffene zur Abgabe einer solchen außerstande ist. Im Kontext der Betriebsvereinbarung bedeutet dies allerdings nicht, dass eine Verarbeitung nur aufgrund einer Einwilligung erfolgen kann, weil der Arbeitgeber durchaus auch ein zu berücksichtigendes Interesse an der Gesundheit seiner Arbeitgeber hat. Vielmehr hat er Fürsorgepflichten nach § 62 HGB sowie insbesondere § 618 BGB.[1497] Insofern sind bei dieser Verarbeitungssituation die Besonderheiten im Beschäftigungskontext zu berücksichtigen, sodass die Betriebspartner in einer Betriebsvereinbarung eine legitimierende Sonderregelung treffen dürfen, die die Rechte der Arbeitnehmer nach § 75 Abs. 2 BetrVG wahrt.

Gleichwohl wäre hier statt einer Erlaubnis mit Widerspruchsvorbehalt aufgrund der gleichlaufenden Interessen nach § 26 Abs. 2 S. 2 BDSG auch eine Einwilligung des Arbeitnehmers denkbar, deren Spezifika in der BV geregelt werden könnten.

Szenario 3: Das Unternehmen XY hat in der Hauptniederlassung eine Abteilung, die sich mit der Nachstellung und Überprüfung von Versicherungsfällen beschäftigt. Dort ist es in der Vergangenheit gehäuft zu Unfällen gekommen, da PKWs für längere Zeit in der geschlossenen Halle betrieben und Arbeitnehmer aufgrund einer hohen CO-Konzentration durch Abgase ohnmächtig wurden. Um weitere Unfälle zu vermeiden, schafft der Arbeitgeber Wearables an, die den CO-Gehalt der Luft sowie die Vitalparameter der in diesem Bereich beschäftigten Arbeitnehmer überwachen und bei einer Überschreitung gewisser Grenzwerte einen weiteren Arbeitnehmer in der Nähe alarmieren und ggf. bei auffälligen Vitalparametern den Betriebsarzt informieren.

1496 Vgl. zur Vorgängerregelung *Article 29 Data Protection Working Party*, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), S. 55 f.

1497 *Hoffmann*, in: Pielow, Beck'scher Online-Kommentar Gewerbeordnung, § 105 GewO Rn. 182 ff.

In diesem Szenario werden zwei verschiedene Kategorien von Daten verarbeitet: Einerseits werden die Daten zum (groben) Aufenthaltsort eines Arbeitnehmers, verbunden mit dem CO-Gehalt der Luft erfasst, andererseits sensitive Daten in Form der Vitalparameter des Beschäftigten zur schnellen Information des Betriebsarztes im Notfall. Für letztere bedarf es einer besonderen Legitimation, da diese Kategorie von Daten durch Art. 9 Abs. 1 DSGVO einen erweiterten Schutz erhält. Gem. § 26 Abs. 4 S. 1 BDSG können solche Daten jedoch auf Grundlage einer Kollektivvereinbarung verarbeitet werden, sofern die Datenschutzgrundsätze eingehalten werden. Aus § 26 Abs. 3 S. 1 BDSG ergibt sich, dass die Verarbeitung von sensitiven Daten, die zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht – hier: Arbeitsschutz – erforderlich sind und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt, zulässig ist. Besondere Schutzmaßnahmen müssen nach § 22 Abs. 2 BDSG getroffen werden. Diese Regelung entspricht dem in Art. 9 Abs. 2 lit. b DSGVO statuierten Grundsatz. Da in einer Kollektivvereinbarung das Recht nur spezifiziert werden darf, müssen diese Grundsätze (Erforderlichkeit zur Erfüllung einer rechtlichen Pflicht sowie kein Überwiegen der Interessen des Arbeitnehmers) auch in einer Betriebsvereinbarung eingehalten werden.[1498]

Aus dem Grundsatz der Datenminimierung lässt sich ableiten, dass – insbesondere – die Daten zu den Vitalparametern nicht dauerhaft im Datenbestand des Betriebsarztes (zum gesonderten Datenbestand siehe bereits **Szenario 2**) erfasst, sondern nur im Alarmfall übermittelt werden dürfen. Sofern eine Momentaufnahme der erfassten Vitalparameter bei der Überschreitung eines Grenzwertes nicht ausreichend zur Beurteilung des Gesundheitszustandes ist, kann auch eine Übermittlung von Daten in einem Zeitfenster von beispielsweise 15 oder 30 Minuten vor der Überschreitung stattfinden. Dies kann dadurch datenschutzfreundlich implementiert werden, indem die Daten zunächst immer nur für einen gewissen Zeitraum lokal auf dem Wearable gespeichert und erst im Alarmfall an den Betriebsarzt übermittelt werden.

Für die Alarmierung eines nahen Beschäftigten hingegen gibt es mehrere Ansatzpunkte, wie eine solche datenschutzfreundlich und datenminimierend erfolgen kann. Einerseits könnte mit einer Kurzreichweiten-Technologie wie Bluetooth eine Alarmierung der in der Nähe befindlichen Arbeitnehmer erfolgen; bei dieser Lösung besteht allerdings das Problem,

1498 Zur Reichweite des Art. 88 DSGVO bzw. § 26 Abs. 4 BDSG, siehe **D. § 1 V. 2.**

dass die Reichweite in vielen Fällen nur wenige Meter beträgt[1499] und daher eine Alarmierung von Kollegen mitunter nicht sichergestellt werden kann, also keine ausreichende Sicherheit bietet und daher möglicherweise nicht geeignet zur Erfüllung des verfolgten Ziels ist. Ebenfalls unsicher wäre die Speicherung des letzten Bluetooth-Gerätes in der Nähe und Alarmierung dessen, da sich der alarmierte Arbeitnehmer bereits auf dem Heimweg oder an einer anderen Stelle im Unternehmen befinden könnte, sodass andere Arbeitnehmer näher sind und schneller Hilfe leisten könnten. Eine dauerhafte Erfassung der Position von allen Arbeitnehmern im Unternehmen ist aber ebenfalls unter dem Aspekt der Überwachungsvermeidung unzulässig.

Die Lösung, die im Unternehmen XY angewandt wird, ist daher die Folgende: In der Halle des Unternehmens befindet sich ein Empfänger, welcher die in der Nähe befindlichen Wearables registriert. Kein Wearable wird einem konkreten Arbeitnehmer zugeordnet, sondern es meldet sich mit einer zufälligen und regelmäßig neu generierten ID an diesem Empfänger an. Die Reichweite des Empfängers ist so eingestellt, dass immer mindestens ein weiteres Wearable registriert wird. Falls dies nicht möglich ist, erfolgt eine Verstärkung des Signals des Empfängers, bis ein Signal erfasst wird. Sollten trotz Verstärkung keine Wearables registriert werden, erfolgt eine Alarmierung über einen vordefinierten E-Mail- und SMS-Notfall-Verteiler.

Sobald das Wearable einen Alarm auslöst, wird neben der zufälligen ID auch der auf dem Wearable gespeicherte Name des betroffenen Arbeitnehmers an den Empfänger übermittelt.

§ 10 Einsatz von Wearables im Hochrisikobereich

(1) XY stellt seinen Arbeitnehmern, die in der Versicherungsfall-Werkstatt arbeiten, Wearables zur Verfügung, die den CO-Wert der Luft sowie die Herzfrequenz und die Sauerstoffsättigung des Bluts erfassen.

(2) Arbeitnehmer, die sich im Hochrisikobereich aufhalten, sind während der Zeit des Aufenthalts verpflichtet, ein Wearable zu tragen. XY hat für die Einhaltung dieser Pflicht durch geeignete Maßnahmen zu sorgen.

1499 *Möckel*, Bluetooth: Wie hoch ist die Reichweite?, 2019, abrufbar unter: https://www.heise.de/tipps-tricks/Bluetooth-Wie-hoch-ist-die-Reichweite-4523661.html (letzter Abruf am: 28.05.2020).

(3) XY verarbeitet die Daten zum CO-Gehalt der Luft und des Standorts des Wearables zum Zwecke des Arbeitsschutzes. Das Wearable generiert hierbei alle zehn Minuten eine neue, zufällige ID zur Anmeldung am Access Point. Die generierte ID darf nicht einem bestimmten Arbeitnehmer zuordenbar sein. Es erfolgt keine dauerhafte Speicherung der registrierten IDs.

(4) Der Access Point muss so positioniert und eingestellt werden, dass er alle Wearables im Hochrisikobereich sowie mindestens zwei, aber maximal vier weitere Wearables außerhalb dieses Bereiches zur Alarmierung erfasst.

(5) Überschreitet der CO-Wert[1500] des Raumes 30 ppm, so wird der Träger des Wearables vor einer hohen Konzentration gewarnt. Überschreitet der Wert 500 ppm, wird der Träger zum sofortigen Verlassen des Raumes aufgefordert. Bei einem Überschreiten des Grenzwertes von 6.400 ppm erfolgt eine erneute Warnung des Arbeitnehmers und eine Alarmierung aller nach Absatz 4 erfassten Personen. Im letzten Fall übermittelt das Wearable den Namen des Beschäftigten an die alarmierten Personen, um eine rasche Hilfe zu gewährleisten. Werden nach Absatz 4 keine weiteren Personen erfasst, so erfolgt eine Alarmierung über den Verteiler notfall@xy.com.

(6) Bei Überschreiten eines CO-Wertes von 10.000 ppm wird zusätzlich die Betriebsärztin über den Vorfall informiert und neben dem Namen und des konkreten CO-Werts auch die Herzfrequenz sowie die Sauerstoffsättigung der letzten 15 Minuten in ihren Datenbestand übermittelt; die Verarbeitung der Gesundheitsdaten des betroffenen Arbeitnehmers für diesen Zweck wird durch diese Vorschrift legitimiert. Die Übertragung der Daten muss über einen verschlüsselten Kanal nach dem aktuellen Stand der Technik erfolgen.

Die dargestellte Regelung könnte eine Mindestregelung für das **Szenario 3** darstellen. Die Absätze 1 bis 3 regeln hierbei die Verpflichtung des Arbeitgebers, entsprechende Geräte für jeden Arbeitnehmer zur Verfügung zu stellen sowie die Sicherstellung der Verpflichtung der Arbeitnehmer zum

1500 Die im nachfolgenden aufgeführten CO-Grenzwerte wurden an die Grenzwerte der Tabelle auf der Website https://www.kohlenmonoxidmelder.com/kohlenmonoxid/ (letzter Abruf am 28.05.2020) angelehnt.

Tragen solcher. Im Übrigen wird die Datenverarbeitung zum Zwecke des Arbeitsschutzes legitimiert. Um ein Überwachungspotential zu vermeiden, vereinbaren die Betriebspartner die Generierung zufälliger, nicht-zuordenbarer IDs und eine Sendebegrenzung des Empfängers sowie Schwellen für Datenübermittlungen (Absätze 4 und 5). In Absatz 6 wird die Verarbeitung sensitiver Daten durch den Betriebsarzt legitimiert und geregelt, wobei ein deutlich höherer, extrem gesundheitsschädigender Grenzwert für die Übermittlung von Vitaldaten angesetzt wird, um dem besonderen Schutz von Gesundheitsdaten Rechnung zu tragen.

Die zugrunde zulegende Interessenabwägung spricht indes auch nicht gegen derartige eine Verarbeitung dieser Daten: Durch das System wird das höchste Rechtsgut des Arbeitnehmers, das Leben, geschützt und der Eingriff in das Persönlichkeitsrecht durch die Begrenzung der Verarbeitungsvorgänge personenbezogener Daten auf Grenzwertüberschreitungen minimiert. Da der Arbeitgeber zum Gesundheitsschutz verpflichtet ist (§ 618 BGB) und ein enorm hohes Gefahrpotential besteht, gibt es kein Widerspruchsrecht der Arbeitnehmer. Auch die Festlegung einer bestimmten Betriebsärztin für die Datenübermittlung erfolgt aufgrund der Notwendigkeit eines schnellen Handelns (im Gegensatz zum **Szenario 2**) bewusst nicht.

2. Scoring von Bewerbern / Automatisiertes Bewerbermanagement

Eine datenschutzrechtliche Legitimation von Datenverarbeitungen im Bewerbungskontext ist mangels Zuständigkeit des Betriebsrats für Bewerber (vgl. § 5 BetrVG) nicht möglich; da etwaige Betriebsvereinbarungen keine normative Wirkung entfalten, können diese eine Datenverarbeitung nach § 26 Abs. 4 BDSG bzw. Art. 88 DSGVO nicht legitimieren; der Arbeitgeber muss eine etwaige Datenverarbeitung im Rahmen § 26 Abs. 1 S. 1 BDSG legitimieren.[1501]

Dennoch hat der Betriebsrat ein Mitbestimmungsrecht nach §§ 94 Abs. 2, 95 BetrVG (Allgemeine Beurteilungsgrundsätze, Auswahlrichtlinien), wenn ein Scoring durchgeführt wird, da hierfür die Bewerber nach

1501 Siehe **E. § 1 III. 2. c) dd) (3)**; zur Zulässigkeit des Scorings von Bewerbern nach § 26 Abs. 1 BDSG, **E. § 1 III. 2. c) dd) (2) (a)**.

bestimmten, vorgegebenen Kriterien bewertet und ggf. sortiert werden.[1502] Dies sollte ebenfalls in einer Betriebsvereinbarung geregelt werden; da dies jedoch kein spezifisch datenschutz-rechtliches Problem ist und die Auswahlrichtlinien und Beurteilungskriterien vom Einzelfall abhängen, wird an dieser Stelle nicht näher darauf eingegangen.

3. Scoring von Arbeitnehmern / Dashboards

§ 94 Abs. 2 BetrVG gibt dem Betriebsrat bei der Aufstellung allgemeiner Beurteilungsgrundsätze ein Mitbestimmungsrecht. Hat der Arbeitgeber also die Absicht, seine Mitarbeiter zu scoren, so ist es zunächst erforderlich, allgemeine Beurteilungsgrundsätze festzulegen, die Grundlage des Scorings sein sollen.[1503]

In diesem Zusammenhang sollte gleichzeitig die datenschutzrechtliche Legitimation in der Betriebsvereinbarung geregelt werden, auch wenn sich nach hiesiger Auffassung die meisten Auswertungen bereits auf § 26 Abs. 1 S. 1 BDSG stützen lassen.[1504]

Unterschieden werden muss zwischen dem Scoring der Arbeitsleistung und des (sonstigen) betrieblichen Verhaltens. Zwar hat der Arbeitgeber ein berechtigtes Interesse an einer Überwachung der Primärleistungspflicht, andererseits darf diese unter Berücksichtigung des Persönlichkeitsrechts der Arbeitnehmer nicht lückenlos ausgestaltet werden, da ansonsten ein Überwachungsdruck aufgebaut werden könnte, der die Arbeitnehmer daran hindern könnte, ihre Freiheitsrechte wahrzunehmen.[1505] Bei der Überwachung des betrieblichen Verhaltens hingegen ist die Gefahr der Erzeugung eines Leistungsdrucks geringer, sodass sich hier eher längerfristige Überwachungsmaßnehmen für People Analytics statuieren lassen. Streng darauf geachtet werden muss allerdings, dass wirklich nur das arbeitsbezogene Verhalten ausgewertet wird, da andernfalls der Eingriff in das Persönlichkeitsrecht der Arbeitnehmer nicht mehr zu rechtfertigen ist.[1506]

1502 *Göpfert/Dußmann*, NZA-Beilage 2016, 41 (45); *Lützeler/Kopp*, ArbRAktuell 2015, 491 (493); *Fitting*, § 95 Rn. 11; allgemein zu § 95 BetrVG, oben **D. § 2 II. 3**.

1503 Zum Mitbestimmungsrecht des § 94 Abs. 2 BetrVG, vgl. **D. § 2 II. 2. b**).

1504 Siehe **E. § 1 III. 2. c**) **dd**) (**2**) (**b**) und (**c**).

1505 Hierzu bereits **E. § 1 III. 2. a**) **cc**) (**4**).

1506 Zum Scoring des betrieblichen Verhaltens, siehe oben **E. § 1 III. 2. c**) **dd**) (**2**) (**c**).

Szenario 1: Das Unternehmen XY setzt seine neue Kollaborationssoftware *Collabo* ein. Dieses Tool bietet über *AnalyzeIt* eine Schnittstelle an, die es Arbeitnehmern erlaubt, ihre tägliche Arbeitszeit zu analysieren. Die Analysen zeigen jeweils auf, wie viele Minuten täglich ein Arbeit-nehmer mit dem Beantworten von E-Mails verbracht hat, wie viele geschriebene E-Mails tatsächlich beantwortet werden, welcher Anteil der täglichen Arbeitszeit in Meetings verbracht wird und wieviel davon tatsächliche „Focus-Time“ ist, in welcher der Arbeitnehmer ungestört an seinen Projekten arbeiten kann. Die persönlichen Auswertungen sollen nur dem Arbeitnehmer angezeigt werden. Die Team-, Abteilungs- und Unternehmensführung soll hingegen jeweils aggregierte Auswertungen auf Team-, Abteilungs- und Unternehmensebene erhalten.

Ausgangspunkt der Betrachtung sind verschiedene Datenverarbeitungsvorgänge: Einerseits der Auswertungsvorgang mit personenbezogenen Daten für den Arbeitnehmer selbst, andererseits die Anonymisierung und Aggregation der Daten auf Team-, Abteilungs- und Unternehmensebene, um eine Übersicht zu generieren. Die Darstellung erfolgt in Dashboards und in wöchentlichen E-Mails mit einer Zusammenfassung der letzten Woche, in welcher die Veränderung zur Vorwoche aufgezeigt werden soll.

Die Datenverarbeitung für das Arbeitnehmerdashboard kann nicht auf eine Betriebsvereinbarung oder eine gesetzliche Legitimationsgrundlage gestützt werden.[1507] Möglich ist es aber, die Rahmenbedingungen für eine (wirksame) Einwilligung des Arbeitnehmers in der Betriebsvereinbarung festzulegen, wie sich aus Erwägungsgrund 155 ergibt.[1508]

Die Verarbeitung zum Zwecke der Aggregation hingegen kann in einer Betriebsvereinbarung geregelt werden. Dort muss insbesondere festgelegt werden, welcher k-Faktor[1509] notwendig ist, um den Datenschutz der einzelnen Arbeitnehmer wirksam zu realisieren. Sofern eine ausreichende Anonymisierung gesichert ist, überwiegen die Interessen des Arbeitgebers am Anonymisierungsvorgang, sodass dieser auch in einer Betriebsvereinba-

1507 Es mangelt an bereits der Geeignetheit der Datenverarbeitung für das erstrebte Ziel, vgl. **E. § 3 I. 1.**

1508 Zu einer möglichen Regelung der Einwilligung von Arbeitnehmern in einer Betriebsvereinbarung, vgl. *Grimm*, ArbRB 2018, 122 (123).

1509 Anonymisierungsgrad, der angewendet werden muss, um eine tatsächliche Anonymität der Daten und somit Nicht-Anwendbarkeit des Datenschutzrechts sicherzustellen, vgl. **E. § 3 III.**

rung legitimiert werden kann. Aufgrund der „Statistik-Ausnahme“ (vgl. bereits **E. § 1 I. 2. c**)) wäre auch eine Zweckänderung bereits erfasster Daten unproblematisch ohne weiteren Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO möglich.

Durch den Einsatz von Scoring-Technologien erfolgt eine Zweckänderung der ursprünglich zu einem anderen Zwecke erhobenen IT-Daten, für welche eine Regelung durch die Betriebspartner getroffen werden sollte.[1510]

§ 11 Nutzung von AnalyzeIt

(1) XY setzt zur Optimierung der Arbeitsabläufe im Unternehmen AnalyzeIt ein. AnalyzeIt ermöglicht es, Auswertungen des täglichen (digitalen) Arbeitstages auf Arbeitnehmerbasis zu erstellen. Zur Sicherung des Datenschutzes werden individualisierte Auswertungen nur aufgrund einer Einwilligung von Arbeitnehmern erstellt.

(2) In diesem Rahmen wird die Technik des Scorings eingesetzt. Unter Ausnahme von § 3 Abs. 2 dieser Vereinbarung ist die zweckändernde Nutzung der hierfür erforderlichen Daten auf Grundlage einer Einwilligung für das persönliche Dashboard möglich.

(3) AnalyzeIt verarbeitet folgende Kategorien von Daten: Einträge im persönlichen Kalender des Arbeitnehmers, E-Mail-Sender und -Empfänger sowie Versende- und Empfangszeitpunkt, Speicherdatum eines E-Mail-Entwurfs. Es erzeugt einen individuellen, täglichen Produktivitätsscore auf Basis dieser Daten.

(4) Bei der Erstellung des Produktivitätsscores ist sicherzustellen, dass ein wissenschaftliches, mathematisch-anerkanntes Verfahren eingesetzt wird, das zu aussagekräftigen Ergebnissen führt. Auf der AnalyzeIt-Plattform muss die Berechnung des Scores gegenüber dem Arbeitnehmer in Grundzügen erläutert werden. In jedem Falle muss es dem Arbeitnehmer möglich sein, den berechneten Score nachvollziehen zu können.

1510 So bereits oben **E. § 1 I. 1. b**) **bb**); in Bezug auf Leistungsdaten, jedoch ohne spezifisch auf Scoring einzugehen, ebenso *Lambrich/Cahlik*, RDV 2002, 287 (290 f.).

(5) Es ist durch technisch-organisatorische Maßnahmen sicherzustellen, dass nur der Arbeitnehmer selbst Zugriff auf seine individualisierten Auswertungen hat.

(6) Für die Einwilligung des Arbeitnehmers gilt § 26 Abs. 2 BDSG. Die Einwilligung hat durch eine elektronische Zustimmung des Arbeitnehmers mittels einer Check-Box auf der Analytics-Plattform zu erfolgen. Die Freiwilligkeit der Einwilligung wird vermutet. Es ist ausdrücklich darauf hinzuweisen, dass der Arbeitnehmer jederzeit seine Einwilligung widerrufen kann. Abweichend von Art. 7 Abs. 3 S. 2 DSGVO gilt, dass die aufgrund der Einwilligung verarbeiteten personenbezogenen Daten für das persönliche Dashboard rückwirkend und unverzüglich gelöscht werden. Der Arbeitnehmer kann seine Einwilligung jederzeit widerrufen. Die Widerrufserklärung kann im AnalyzeIt-Dashboard direkt oder per E-Mail an widerruf@xy.com erklärt werden.

(7) XY ist gestattet, aggregierte Auswertungen der in Absatz 2 genannten Daten auf Team-, Abteilungs- und Unternehmensebene für Zwecke der People Analytics zu erstellen. Personelle Maßnahmen mit einer negativen Auswirkung auf Arbeitnehmer aufgrund dieser Daten sind ausgeschlossen.

(8) Bei der Aggregation der Daten ist sicherzustellen, dass die Daten nicht mehr einer bestimmbaren Person zuordenbar sind. Im Allgemeinen wird bei einer Aggregation von Daten von mindestens vier Arbeitnehmern von einer Anonymität ausgegangen. Sollte im Einzelfall eine Zuordnung zu einer bestimmbaren Person möglich sein, so sind der Betriebsrat und der betroffene Arbeitnehmer unverzüglich zu informieren und weitere Maßnahmen vorzunehmen, dass weitere Identifizierungen nicht stattfinden. Die individualisierbaren Daten sind unverzüglich zu löschen.

(9) Die aggregierten Auswertungen des eigenen Teams-, der eigenen Abteilung und des Unternehmens sind den Arbeitnehmern zur Verfügung zu stellen. Dies soll, wenn möglich, im persönlichen Dashboard des Arbeitnehmers erfolgen.

Da § 3 Abs. 2 PA-BV regelt, dass die zweckändernde Verarbeitung von personenbezogenen Daten für People Analytics nicht zulässig ist, wird in Abs. 2 dieser Regelung eine Ausnahme von diesem Grundsatz für die

Datenauswertungen für das persönliche Dashboard festgelegt. Aufgrund der Anonymisierung dürfen im Rahmen der aggregierten Darstellung die Daten ohnehin weiterverarbeitet werden, sodass es einer weiteren Ausnahme an dieser Stelle nicht bedarf. In Erweiterung zu den gesetzlichen Vorgaben zur Transparenz von Scoring-Verfahren[1511] wird in Absatz 5 geregelt, dass dem Arbeitnehmer die Berechnung des Score-Werts erläutert werden und der Arbeitnehmer das Ergebnis zumindest nachvollziehen können muss. In Absatz 6 werden die gesetzlichen Vorgaben zur Einwilligung spezifiziert und das Vorliegen einer Freiwilligkeit vermutet. Eine unwiderlegliche Vermutung an dieser Stelle würde die Berücksichtigung des Einzelfalls nicht mehr erlauben und somit gegen den Grundsatz in Art. 7 Abs. 4 DSGVO verstoßen.

In Absatz 7 wird ein individueller k-Faktor als Regel herangezogen; der Arbeitgeber bleibt aber dennoch verpflichtet, die Daten wirksam zu anonymisieren. Diese Regelung legitimiert die Verarbeitung bei einer k-Anzahl von vier Personen, auch wenn hierbei im Einzelfall später festgestellt wird, dass die Gruppengröße für die wirksame Anonymisierung zu klein war. Für diesen Fall wird durch § 7 Abs. 8 PA-BV sichergestellt, dass der Arbeitgeber für den Zeitraum bis zur Anpassung der Gruppengröße eine Legitimationsgrundlage besitzt und hierdurch keinen Datenschutzverstoß begeht. Aufgrund der geringen Wahrscheinlichkeit eines Eingriffes in das Persönlichkeitsrecht einzelner Arbeitnehmer und der eng begrenzten Zeit des Eingriffs, überwiegt das Interesse des Arbeitgebers an der Datenverarbeitung. Notwendig ist diese Regelung, da es schwierig ist, sicherzustellen, dass Auswertungen möglichst präzise sind, gleichzeitig aber keine Rückschlüsse auf einzelne Personen Rückschlüsse zulassen.

Szenario 2: Das Unternehmen XY setzt eine neue Personalverwaltungssoftware ein. In dieser werden die Stammdaten, die betrieblichen Fortbildungen, jährliche Zielvereinbarungen und das Ergebnis halbjährlicher Mitarbeitergespräche erfasst. Ein neues Plugin *ScoreIt* ermöglicht es nun die Mitarbeiter zu scoren und die Passgenauigkeit mit den Anforderungen der Stelle mit einem Punktewert von 0 bis 10 anzeigen zu lassen. Zur Verbesserung der Effizienz sollen mit Hilfe des Scores Entwicklungspotentiale aufgezeigt bzw. Perso-

1511 Diese sind als sehr gering einzustufen, zumal auch Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g und Art. 15 Abs. 1 lit. h DSGVO Informationen über die involvierte Logik nur bei einer automatisierten Einzelfallentscheidung fordern; hierzu bereits **E. § 1 III. 2. c) bb)**.

nalmaßnahmen vorgeschlagen werden. Automatisierte Entscheidungen, z.B. in Form von Anmeldungen für Fortbildungen oder Seminare erfolgen nicht.

Dieses Szenario ist ein mögliches Beispiel für die in **E. § 3 II. 1** erfolgte Untersuchung. Mangels kontinuierlicher Leistungserfassung liegen keine Überwachungsmaßnahmen vor, sodass diese Art der Datenverarbeitung – im Vergleich zu anderen Advanced People Analytics – eher unproblematisch ist.

Auch hier steht aus rechtlicher Sicht zunächst die Problematik einer Zweckänderung im Raum: Im vorliegenden Fall wäre zwar vertretbar, dass auch das weitergehende Scoring für die Durchführung des Arbeitsverhältnisses erforderlich ist, da die Zweckbestimmung des § 26 Abs. 1 S. 1 BDSG sehr weit gefasst ist. Sollen möglicherweise auch noch andere Daten daraus gewonnen werden (z.B. der zukünftige Personalbedarf), die nicht in unmittelbarem Zusammenhang mit der Durchführung des *konkreten* Arbeitsverhältnisses stehen, so ist eine Zweckänderung zwingend erforderlich.[1512] Auch ist nicht sicher, ob ein Gericht das Scoring als vom Erhebungszweck gedeckt beurteilen würde, sodass in jedem Falle Regelungen zur Zweckänderung bzw. -kompatibilität getroffen werden sollten.

Sofern der weitergehende Zweck ebenfalls im Beschäftigungskontext anzusiedeln ist, dürfen die Betriebsparteien aufgrund Art. 88 DSGVO spezifischere Vorschriften zur Zweckkompatibilität treffen.[1513] Voraussetzung ist allerdings, dass die Datenschutzgrundsätze, in diesem Zusammenhang insbesondere die in Art. 6 Abs. 4 DSGVO festgelegten Grundsätze zur Zweckänderung wahren. Insbesondere darf keine Lockerung dieses Gebots stattfinden.[1514]

Mitspracherechte des Betriebsrats bestehen vor allem in § 94 Abs. 2 BetrVG, also in den allgemeinen Beurteilungsgrundsätzen, die dem Scoring zugrunde liegen.

§ 12 Nutzung von ScoreIt

(1) XY setzt in Ergänzung der Personalverwaltungssoftware PersoPlus das Plugin ScoreIt ein. ScoreIt ermöglicht es, die vorhandenen Stammdaten der Arbeitnehmer, Zielvereinbarungen und unterjährigen Mitarbeiterge-

1512 Siehe **E. § 1 I. 1. b) dd)**.
1513 So wohl auch *Körner*, NZA 2019, 1389 (1392).
1514 *Kort*, NZA-Beilage 2016, 62 (64); siehe hierzu bereits **D. § 1 V. 2.**

spräche auszuwerten, mit den Stellenbeschreibungen abzugleichen und verschiedene Punktewert von 0 bis 10 für Entwicklungspotential, Passgenauigkeit auf die Stelle, Passgenauigkeit auf Beförderungsstellen sowie den Gesamteindruck über den Arbeitnehmer zu generieren. Dieser Score dient der Unterstützung der Personalverantwortlichen bei Personalmaßnahmen.

(2) Bei der Verwendung von ScoreIt ist darauf zu achten, dass ein wissenschaftlich-anerkanntes, mathematisches Verfahren verwendet wird, das nachvollziehbare Punktewerte generiert. Es muss XY zu jedem Zeitpunkt möglich sein, den konkreten Punktewert zu erläutern.

(3) XY ist, in Ausnahme des Grundsatzes von § 3 Abs. 2 dieser Vereinbarung, legitimiert, die Daten auf PersoPlus für das Scoring durch ScoreIt in zweckverändernder Weise weiterzuverarbeiten. Hierbei wird davon ausgegangen, dass eine Zweckkompatibilität im Sinne des Art. 6 Abs. 4 DSGVO besteht. Der Arbeitgeber darf keine besonderen Kategorien von Daten im Sinne des Art. 9 DSGVO verwenden. Durch technisch-organisatorische Maßnahmen muss sichergestellt werden, dass die Daten entsprechend dem aktuellen Stand der Technik gegen unbefugte Zugriffe Dritter abgesichert werden.

(4) Die generierten Scorewerte dürfen nicht als alleinige Grundlage für Personalmaßnahmen herangezogen werden. Automatisierte Einzelfallentscheidungen sind verboten. Jede vorgeschlagene Maßnahme muss inhaltlich durch einen entscheidungsbefugten Vorgesetzten überprüft und genehmigt werden. Jede benachteiligende Maßnahme, die auf einem Scorewert beruht, ist unter Zugrundelegung der für den Score erheblichen Datenbasis gegenüber dem Arbeitnehmer und dem Betriebsrat zu begründen.

(5) Der betroffene Arbeitnehmer hat den Anspruch, jederzeit Einblick in seinen Scorewert zu nehmen und eine Begründung zur Zusammensetzung in Textform zu fordern. Ebenfalls hat er die Möglichkeit gegen den generierten Wert Widerspruch einzulegen und seinen Standpunkt darzustellen. XY ist verpflichtet, den Scorewert unter Berücksichtigung der Stellungnahme des Arbeitnehmers zu überprüfen und ihm das Ergebnis der Überprüfung schriftlich mitzuteilen.

Im ersten Absatz wird die Verwendung des Plugins *ScorteIt* geregelt sowie die verschiedenen Kategorien von Daten, die Grundlage für das Scoring sind, benannt. Absatz 2 regelt in Anlehnung an – den unionsrechtswidrigen[1515] – § 31 BDSG die Vorgaben für das Scoring, wobei – über die Vorgaben hinaus – noch sichergestellt wird, dass der Arbeitgeber den Score jederzeit erläutern können muss. Dies erfolgt auch gegenüber dem Arbeitnehmer in Textform (Absatz 5). Ersteres wird bereits durch das Transparenzerfordernis des Art. 5 Abs. 1 lit. a DSGVO gefordert; letzteres erfolgt – jedenfalls im Hinblick auf das SCHUFA-Urteil des BGH[1516] zur Vorgängerreglung – wohl überschießend zur aktuellen Rechtslage nach DSGVO und BDSG und zum Vorteil des Arbeitnehmers.[1517] Die Legitimation in Absatz 3 zur Zweckänderung basiert auf einer Einschätzung der Zweckkompatibilität nach Art. 6 Abs. 4 DSGVO und ist durch Art. 88 DSGVO gedeckt. Dass von einer Zweckkompatibilität ausgegangen wird, soll eine Beweislastumkehr statuieren. Ob und inwiefern dies im Hinblick auf die nach h.M.[1518] geltende Beweislastregelung in Art. 5 Abs. 2 DSGVO rechtlich zulässig ist, ist in Wissenschaft und Literatur noch nicht geklärt. Ein Scoring von Gesundheitsdaten hingegen scheidet aufgrund der strengen Voraussetzungen des § 26 Abs. 3 S. 1 BDSG aus.[1519] Absatz 4 der Regelung sichert, dass keine (verbotene) automatisierte Einzelfallentscheidung nach Art. 22 DSGVO vorliegt. Zuletzt wird in § 8 Abs. 5 DSGVO noch ein weitgehendes Widerspruchsrecht statuiert, welches es in dieser Form nach Art. 22 Abs. 3 DSGVO nur bei der automatisierten Einzelfallentscheidung gibt, nicht jedoch, wenn ein menschlicher Entscheider die Entscheidung unter Berücksichtigung eines Scores trifft.[1520]

1515 Ausführlich oben **E. § 1 III. 2. c) bb) (1)**.

1516 BGH, Urt. v. 28.01.2014 – VI ZR 156/13, ZD 2014, 306.

1517 So wird von einem großen Teil der Literatur die Rechtsprechung weiterhin für anwendbar erachtet, vgl. *Klar*, BB 2019, 2243 (2251); *von Lewinski/Pohl*, ZD 2018, 17 (23); kritisch BeckOK DatenSR/*Schmidt-Wudy*, Art. 15 DSGVO Rn. 78.3.

1518 Zum Regelungsgehalt von Art. 5 Abs. 2 DSGVO: Beweislastregelung zulasten des Verantwortlichen: *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 5 DSGVO Rn. 186; *Pötters*, in: Gola, Datenschutz-Grundverordnung, Art. 5 DSGVO Rn. 34; Ehmann/Selmayr/*Heberlein*, Art. 5 DSGVO Rn. 32; *Wolff*, D. I. Grundsätze der Datenverarbeitung, in: Schantz/Wolff, Das neue Datenschutzrecht, Rn. 449; wohl auch *Hamann*, BB 2017, 1090 (1092); keine Beweislastregelung: Sydow/*Reimer*, Art. 5 DSGVO Rn. 53; *Veil*, ZD 2018, 9 (10): Beweislastregel "nur" i.R.d. Haftung.

1519 Hierzu **E. § 1 III. 2. c) dd) (2) (d)**.

1520 Zum Inhalt des Rechts nach Art. 22 Abs. 3 DSGVO vgl. bereits **D. § 1 V. 3. e)**.

4. Automatisierte Entscheidungen im laufenden Beschäftigungsverhältnis

Während im vorherigen Szenario automatisierte Einzelfallentscheidungen explizit ausgeschlossen wurden, soll im Nachfolgenden ein Regelungsbeispiel für automatisierte Entscheidungen auf Basis des durch das fiktive Tool *ScoreIt* generierten Scores dargestellt werden. Die Untersuchung beschränkt sich auf automatisierte Entscheidungen im laufenden Beschäftigungsverhältnis, da der Betriebsrat für Bewerber mangels Zuständigkeit keine datenschutzrechtliche Regelungskompetenz besitzt.[1521]

Da der Anwendungsbereich für automatisierte Einzelfallentscheidungen nach Art. 22 DSGVO im laufenden Beschäftigungsverhältnis sehr begrenzt ist,[1522] wird im Nachfolgenden ein Beispiel für eine Automatisierung aufgezeigt, welches mangels rechtlicher Wirkung aber nicht von Art. 22 Abs. 1 DSGVO erfasst ist.

> **Szenario:** Auf Basis von *ScoreIt* sollen die Scores zum Entwicklungspotential sowie der Passgenauigkeit auf die jetzige Stelle und Beförderungsstellen zur Grundlage für Fortbildungsvorschläge genommen werden. Der Schulungsanbieter bietet eine standardisierte Schnittstelle bereit, die von der Personalsoftware genutzt werden kann, um Schulungen und deren einzelne Lernziele automatisiert auszuwerten und mit Arbeitnehmerprofilen abzugleichen. Eine Datenübermittlung an den Anbieter findet nicht statt. Werden bei einem Arbeitnehmer Defizite in bestimmten Bereichen erkannt, kann über diese Schnittstelle eine passende Schulung gefunden werden, um den Arbeitnehmer in diesen Bereichen fortzuentwickeln. XY möchte nun automatisiert den Arbeitnehmern entsprechende Schulungen anbieten.

Das genannte Szenario zeigt ein mögliches Anwendungsbeispiel für eine in **E. § 2 II. b**) untersuchte automatisierte Einzelfallentscheidung. Da es sich lediglich um einen Vorschlag handelt und die Entscheidung daher keine rechtliche Wirkung entfaltet, fällt dieses Szenario nicht unter Art. 22 Abs. 1 DSGVO. Dennoch sollte aufgrund der betriebsverfassungsrechtlichen Mitbestimmungsrechte des Betriebsrats und des zugrundeliegenden Scorings eine kollektivrechtliche Regelung getroffen werden, die das Szenario regelt.

1521 Im Detail **E. § 1 III. 1. c**) **bb**) sowie **E. § 1 III. 2. c**) **dd**) (**3**).
1522 Vgl. **E. § 2 III**.

§ 13 Automatisierte Fortbildungsvorschläge auf Basis von ScoreIt

(1) ScoreIt soll neben dem in § 12 genannten Anwendungsszenario auch dafür genutzt werden, Arbeitnehmern auf Basis ihres Entwicklungsscores und der Passgenauigkeitsscores maßgeschneiderte Fortbildungen vorzuschlagen, um die fachlichen und persönlichen Kompetenzen weiter zu fördern.

(2) In diesem Zusammenhang ist XY legitimiert, die durch ScoreIt generierten Daten, in Ausnahme von § 3 Abs. 2 dieser Vereinbarung, für Fortbildungszwecke zu verarbeiten.

(3) Der Arbeitnehmer erhält hierzu eine E-Mail mit einem Fortbildungsvorschlag und entsprechenden Terminen für die Fortbildung. In dieser E-Mail ist dem Arbeitnehmer die Entscheidungsgrundlage für den Vorschlag auf Basis ihres Scores darzustellen. Ferner soll, nach Möglichkeit, die durch die Maßnahme zu erzielende Scoreverbesserung aufgezeigt werden. In keinem Fall wird der Arbeitnehmer durch einen automatisierten Vorschlag zur Teilnahme an einer Fortbildung verpflichtet.

(4) Soll ein Arbeitnehmer zu einer Fortbildung auf Basis von ScoreIt verpflichtet werden, so ist sicherzustellen, dass ein Vorgesetzter den generierten Vorschlag unter Zugrundelegung bisheriger Personalgespräche und Erfahrungswerten überprüft und die Teilnahme zur Fortbildung unter Ausübung des Direktionsrechts persönlich anordnet.

(5) Bei begrenzten Ausbildungskapazitäten ist dem Betriebsrat vor Übermittlung der Vorschläge die Vorschlagsliste des Systems vorzulegen. Dieser hat nach Erhalt der Liste eine Woche Zeit, um die Liste zu überprüfen und eigene Vorschläge einzubringen. XY und Betriebsrat einigen sich unter Beachtung des von ScoreIt generierten Scores auf eine gemeinsame Liste.

(6) In jedem Falle ist dem Betriebsrat eine Liste der geplanten Fortbildungen zu übermitteln, sodass dieser eigene Vorschläge einbringen kann. Unter Berücksichtigung des von ScoreIt generierten Werts entscheiden Arbeitgeber und Betriebsrat über die Teilnahme der Vorschläge des Betriebsrats an den angebotenen Fortbildungen. Die betroffenen Arbeitnehmer werden nach dem in Absatz 3 geregelten Verfahren über die Fortbildung informiert.

Die Absätze 1 und 2 regeln, für welche Zwecke die Scores – neben den in § 13 PA-BV bereits geregelten Verarbeitungssituationen – genutzt werden dürfen. Zwar könnte die Verarbeitung für Fortbildungszwecke womöglich bereits unter die weite Formulierung der „Personalmaßnahmen" subsumiert werden; sicherheitshalber sollte dieser Zweck aber nochmals explizit erwähnt werden, da durch einen reinen Vorschlag noch keine Personalmaßnahme stattfindet. In Absatz 3 wird die Einbeziehung und Information des Arbeitnehmers geregelt und sichergestellt, dass die Verarbeitung und der generierte Vorschlag der in Art. 5 Abs. 1 lit. a DSGVO geforderten Transparenz entspricht. Zum Ausschluss einer – möglicherweise verdeckten – automatisierten Einzelfallentscheidung nach Art. 22 Abs. 1 DSGVO regelt Absatz 4, dass eine Anordnung einer Fortbildung (nachteilige rechtliche Wirkung) nur auf Basis der Datengrundlage und nicht allein des Scores erfolgen darf.[1523] Zur Sicherung der in §§ 96 ff. BetrVG geregelten Mitbestimmungsrechte des Betriebsrats dienen die Absätze 5 und 6 der Regelung.[1524]

5. Netzwerk-Analysen

Netzwerk-Analysen stellen ein besonderes Anwendungsfeld von Advanced People Analytics dar, insbesondere wenn diese in Form eines „Enterprise Social Graph" aus Echtzeitdaten generiert werden sollen. Aufgrund der zu regelnden Feinheiten und dem kritischen Spannungsfeld zwischen (zulässiger) Netzwerk-Analyse und unzulässiger Überwachung der Beschäftigten ist die präzise Regelung einer solchen Technik in einer Betriebsvereinbarung geboten.

Hinweis: Vorweg wird auf die unsichere Rechtslage im Hinblick auf die Anwendbarkeit der Regelungen des TKG auf Arbeitgeber, die ihren Arbeitnehmern die Privatnutzung der betrieblichen Kommunikation erlauben, hingewiesen.[1525] Obwohl nach hiesiger Auffassung die §§ 88 ff. TKG auf Arbeitgeber nur beschränkt Anwendung finden, ist aufgrund

---

1523 Andernfalls hat inhaltlich bereits der Algorithmus die Entscheidung getroffen und es liegt ein Fall des Art. 22 Abs. 1 DSGVO vor; siehe hierzu **D. § 1 V. 3. c) aa)**.

1524 Zu den Beratungs- und Mitbestimmungsrechten des Betriebsrats vgl. bereits **E. § 2 II. b) bb)**.

1525 Inzwischen dürfte die Rechtsprechung dazu tendieren, die §§ 88 ff. TKG nicht mehr auf Arbeitgeber anzuwenden, dennoch ist dies bislang nicht höchstrichterlich geklärt. Hierzu im Detail **D. § 3 I. 2.**

der strafrechtlichen Risiken sowie der anderslautenden Auffassung der Datenschutzbehörden eine private Nutzung der betrieblichen Telekommunikation durch Arbeitgeber zu untersagen, wenn der Kommunikationsverkehr (auch lediglich Verbindungsdaten) überwacht und einer Analyse zugeführt werden soll.

Regelungen zur Netzwerkanalyse und Privatnutzung betrieblicher IT ist aufgrund der Mitbestimmungsrechte des Betriebsrats nach § 87 Abs. 1 Nr. 1 und 6 BetrVG optimalerweise in einer Betriebsvereinbarung zu regeln.[1526]

Szenario: Neben einem Textverarbeitungsprogramm, Tabellenkalkulationsprogramm und Präsentationsprogramm beinhaltet die obige Kollaborationssoftware *Collabo* des Unternehmens XY auch ein E-Mail-Programm, wobei die E-Mails ebenfalls durch den *Collabo*-Server verarbeitet werden. Daneben gibt es ein Instant-Messaging-Programm *TeamIt*, über welches sich Chat-Nachrichten und Dateien versenden lassen und Videokonferenzen veranstaltet werden können. Die Arbeitnehmer nutzen zur innerbetrieblichen Kommunikation – auch über die vom Arbeitgeber zur Verfügung gestellten Mobiltelefone – vor allem *TeamIt* zur Kommunikation. Das Management von XY stellt fest, dass innerbetriebliche Kommunikationsabläufe nicht über die vor-gesehenen Hierarchien erfolgen. Es wird vermutet, dass verteilt im Unternehmen einzelne Arbeitnehmer immer wieder als Experten in Anspruch genommen werden. Das Management möchte diese identifizieren.

Eine mögliche Regelung dieses Sachverhalts könnten die folgenden Ausführungen darstellen:

§ 14 Verbot der Privatnutzung der betrieblichen Kommunikation und Durchführung von Netzwerk-Analysen

(1) Die Nutzung der betrieblichen Kommunikationsplattformen (E-Mail, Telefonie und TeamIt) für private Zwecke ist verboten.

(2) XY nutzt die Verbindungsdaten der betrieblichen Kommunikationsplattformen für Netzwerk-Analysen durch den Einsatz eines Enterprise Social Graph. Ziel der Analysen ist es, das informelle Netzwerk des

1526 Zu letzterem *Müller*, öAT 2019, 1 (3).

Netzwerks darzustellen und hierdurch die formale Hierarchie des Unternehmens zu optimieren.

(3) Nach Information der Arbeitnehmer über die Zweckerweiterung der Verarbeitung der Verbindungsdaten ist XY legitimiert, die personenbezogenen Verbindungsdaten für Netzwerkanalysen zu nutzen. Die Arbeitnehmer sind mindestens eine Woche vor Aktivierung des Enterprise Social Graph umfassend in Textform per E-Mail sowie durch deutlich sichtbaren Hinweis im Intranet zu informieren. Diese Information umfasst auch die Warnung, dass hierdurch bei unerlaubter Privatnutzung private Beziehungen zwischen einzelnen Arbeitnehmern aufgedeckt werden können.

(4) Personelle Maßnahmen auf Basis der durch den Enterprise Social Graph gewonnen Erkenntnisse dürfen nicht zum Nachteil der Arbeitnehmer angewandt werden. Ausnahme sind repressive Maßnahmen, die unter den Voraussetzungen des § 26 Abs. 2 BDSG ergriffen werden.

(5) Der Zugriff auf den Enterprise Social Graph ist auf das erforderliche Minimum zu beschränken; jeder Zugriff auf das System ist zu dokumentieren.

(6) Dem Betriebsratsvorsitzenden und seinem Stellvertreter sind unter den Voraussetzungen des Absatz 5 Einsicht in den Enterprise Social Graph zu gewähren; die hierdurch erlangten Kenntnisse unterliegen der Geheimhaltungspflicht.

(7) Die Daten der Netzwerkanalyse sind spätestens nach einem Jahr nach Erhebung zu löschen; wurde das mit der Verarbeitung erstrebte Ziel vorher erreicht, sind die Daten nach Zielerreichung unverzüglich zu löschen.

Wie bereits eingangs aufgeführt, wird in Absatz 1 aufgrund der Rechtsunsicherheit die Privatnutzung verboten. In Absatz 2 wird das verfolgte Ziel statuiert und in Absatz 3 die hierfür notwendige Datenverarbeitung nach vorheriger Information der Arbeitnehmer legitimiert.

Über die gesetzlichen Vorgaben nach Art. 13 f. DSGVO hinaus ist wegen der grundsätzlichen hohen Eingriffsintensität der Maßnahme aufgrund einer „Dauerüberwachung" bei (unerlaubter) Privatnutzung noch eine zu-

sätzliche Warnung aufzunehmen, welche Folgen eine solche haben könnte.

Absatz 4 stellt eine Garantie dar, dass die Analysen in aller Regel keine negativen Folgen für Arbeitnehmer haben werden; dies ist ein Kriterium, das im Rahmen einer Güterabwägung ebenfalls von entscheidender Bedeutung ist.[1527] Lediglich bei Straftatverdacht dürfen die Daten für repressive Maßnahmen verwendet werden. In den Absätzen 5 und 6 wird zur Vermeidung von Missbrauch der Zugriff auf das Minimum beschränkt (auch auf Betriebsratsebene) und eine Dokumentationspflicht für Zugriffe statuiert.

Zuletzt wird eine Speicherbegrenzung in überschießender Tendenz zum Grundsatz nach Art. 5 Abs. 1 lit. e DSGVO von höchstens einem Jahr festgelegt. Somit scheidet aus, dass die Daten unter dem Vorwand der Erforderlichkeit nahezu unbegrenzt gespeichert werden.

VI. Technische und organisatorische Sicherungsmaßnahmen

Ferner sollten in der Betriebsvereinbarung Regelungen zu technischen und organisatorischen Sicherungsmaßnahmen nach Art. 25 DSGVO aufgenommen werden, die konkret auf das jeweilige Unternehmen bzw. den jeweiligen Betrieb abgestimmt sind.[1528]

§ 15 Spezifische technische und organisatorische Sicherungsmaßnahmen

(1) Es ist sicherzustellen, dass alle aufgrund dieser Vereinbarung verarbeiteten Daten nach dem Stand der Technik verschlüsselt werden. Beim Einsatz eines symmetrischen Verschlüsselungsverfahrens ist (Stand: Mai 2021) mindestens AES-256 einzusetzen.

(2) Die Daten sind darüber hinaus, soweit möglich, zu pseudonymisieren. Eine Rückführung zum Klarnamen darf erst im Rahmen der Anzeige der Daten für den Endanwender erfolgen.

(3) Es ist ein Berechtigungskonzept zu erarbeiten, in welchem alle Arbeitnehmer mit Zugriff auf die personenbezogenen Daten in dieser Betriebs-

1527 Siehe hierzu **E. § 4 II. 1. d) bb) (4)**.
1528 Vgl. *Körner*, NZA 2019, 1389 (1392).

vereinbarung konkret benannt werden und begründet wird, weshalb ein Zugriff auf die Daten erforderlich ist. Über jede Berechtigungsvergabe ist der Betriebsrat zu informieren. Alle Personen mit einem Zugriff auf die personenbezogenen Daten nach dieser Vereinbarung sind zur Geheimhaltung zu verpflichten.

(4) Ferner ist ein Löschkonzept zu entwickeln, welches dieser Betriebsvereinbarung angehängt wird und verpflichtend ist. In diesem müssen für jede Kategorie der im Rahmen dieser Vereinbarung erhobenen Daten Speicherfristen sowie der konkrete Vorgang der Löschung und dessen Dokumentation festgelegt werden. Des Weiteren sollen Überprüfungsmöglichkeiten des Betriebsrats hinsichtlich einer sicheren Löschung festgelegt werden. Dieses Löschkonzept dient der Sicherstellung der Datenminimierung und Speicherbegrenzung und ist mit dem Betriebsrat abzustimmen. Es ist an geeigneter Stelle im Intranet zu veröffentlichen.

Die Regelungen der Absätze 1 und 2 dienen dem technischen Datenschutz. Durch die Sicherstellung einer Verschlüsselung sowie weitgehender Pseudonymisierung der Daten werden die Risiken für die Betroffenen bei Datenpannen minimiert. Im Falle eines Datenlecks ist dann zwar gem. Art. 33 DSGVO die Datenschutzbehörde zu informieren, bei ausreichender Sicherung gem. Art. 34 Abs. 3 lit. a DSGVO jedoch nicht der Betroffene. Das Berechtigungs- und Löschkonzept ist eine organisatorische Maßnahme zum Datenschutz; durch einen möglichst geringen Zugriffskreis an (internen) Datenempfängern sowie der Verpflichtung zur Geheimhaltung wird sichergestellt, dass keine unbefugten Dritten Kenntnis der Daten erlangen.

VII. Verfahren bei Streitigkeiten

Zur Vermeidung von Streitigkeiten über die Reichweite eines Mitbestimmungsrechts und darüber, ob es sich bei den einzelnen Klauseln um freiwillige Vereinbarungen nach § 88 BetrVG handelt, empfiehlt es sich, die Anrufung einer Einigungsstelle durch jede Seite sowie die Verbindlichkeit der Entscheidung dieser vorzusehen.[1529] Hierdurch lässt sich vermeiden, dass mitunter hochkomplexe IT-Fragen vor Gericht ausgefochten werden müssen; die Parteien können stattdessen eine Einigungsstelle anrufen, die

1529 *Körner*, NZA 2019, 1389 (1393).

sich auf IT-Betriebsvereinbarungen spezialisiert und somit für die Entscheidung die notwendige Fachkompetenz hat.

§ 16 Verfahren bei Streitigkeiten / Einigungsstelle

(1) Bei Streitigkeiten über die Anwendung, Auslegung oder Reichweite dieser Vereinbarung sind sowohl XY als auch der Betriebsrat berechtigt, die Einigungsstelle anzurufen.

(2) Die Entscheidung der Einigungsstelle ist verbindlich.

VIII. Sonstiges

Die weiteren zu treffenden Regelungen betreffen das Inkrafttreten, die Laufzeit der Vereinbarung sowie Kündigungsfristen, Nachwirkung, eine Neuverhandlungspflicht bei Kündigung sowie eventuelle Anpassungspflichten bei Änderungen von Rahmenbedingungen. Schlussendlich sollten noch in den Schlussbestimmungen der Ausschluss mündlicher Nebenabreden sowie eine salvatorische Klausel vorgesehen werden.[1530] Von Abdruck dieser wird abgesehen.

1530 Formulierungsvorschläge bei *Grimm*, ArbRB 2018, 122 (127).