Karin Schuler/Thilo Weichert

Beschäftigtendatenschutzgesetz – was ist und was sein sollte

I. Ankündigungen

Die Hoffnung stirbt zuletzt; manchmal ist sie aber schon fast tot. Im rot-grüngelben Koalitionsvertrag von 2021 steht:

Wir schaffen Regelungen zum Beschäftigtendatenschutz, um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen.[1]

Wenig später nahm Arbeitsminister Hubertus Heil den Bericht des Beirats für ein Beschäftigtendatenschutzgesetz entgegen und erklärte:

Der Abschlussbericht des Beirats zum Beschäftigtendatenschutz kommt genau zum richtigen Zeitpunkt. Die neue Koalition will in dieser Legislatur Regelungen zum Beschäftigtendatenschutz schaffen, um Rechtsklarheit für Arbeitgeber und Beschäftigte zu erreichen und die Persönlichkeitsrechte der Beschäftigten effektiv zu schützen.[2]

Am 31.08.2022 legte aber Digitalminister Volker Wissing eine Digitalstrategie der Bundesregierung für die kommende Legislaturperiode vor. Hier hätte man eine Verortung des Vorhabens erwartet. Allerdings kann man sich des Eindrucks nicht erwehren, dass statt klarer Bekenntnisse das Prinzip „Rumeierei" verfolgt wird. In der Digitalstrategie heißt es unter anderem.

Wir werden mit modernen Regelungen zum Beschäftigtendatenschutz grundrechtswahrend und rechtssicher den Weg ebnen, um die Potenziale neuer Technologien für eine moderne Arbeitswelt zu nutzen.

Und weiter:

Wir wollen uns 2025 daran messen lassen, ob: (…) sich die Regeln für den Beschäftigtendatenschutz in der betrieblichen Praxis bewährt haben und aus Sicht aller Beteiligten zu mehr Rechtssicherheit beitragen.[3]

Abstrakter geht es kaum noch. Von einem klaren Bekenntnis zum Beschäftigtendatenschutzgesetz ist nichts zu erkennen.

Wer hoffte, dass das, was in einem Koalitionsvertrag angekündigt wird, tatsächlich politisch gewollt sei und umgesetzt würde, der könnte angesichts solcher vagen Formulierungen ausgerechnet in einer Digitalstrategie ernüchtert sein.[4] Nicht mehr an der Verabschiedung eines Beschäftigtendatenschutzgesetzes will sich die Regierung messen lassen, sondern nur noch daran, ob die bestehenden Gesetze zu mehr Rechtssicherheit beitragen. Fragt man Insider, ob an einem Beschäftigtendatenschutzgesetz ernsthaft gearbeitet wird, dann erhält man hinter vorgehaltener Hand eine abschlägige Antwort.

Offiziell erklärte das BMAS allerdings auf explizite Nachfrage noch im September 2022:

In Umsetzung des Koalitionsvertrages ist vorgesehen unter gemeinsamer Federführung von BMAS und BMI ein eigenständiges Beschäftigtendatenschutzgesetz zu schaffen. In einem ersten Schritt werden dazu gemeinsame Eckpunkte erarbeitet. Die sich daran anschließende Ausarbeitung eines Referentenentwurfs soll noch in der ersten Hälfte der Legislaturperiode erfolgen. Die Ergebnisse des Beirats zum Beschäftigtendatenschutz bilden eine wichtige Grundlage bei der inhaltlichen Gestaltung der Regelungen und finden bei der Erarbeitung der Eckpunkte sowie des Referentenentwurfes entsprechend Berücksichtigung. Vertreterinnen und Vertreter der Sozialpartner wurden bereits im Rahmen der Beiratsarbeit angehört. Bei der weiteren Ausarbeitung sowohl der Eckpunkte als auch des Referentenentwurfs wird das BMAS sowohl die Sozialpartner als auch weitere relevante Stakeholder einbeziehen.[5]

Demnach wäre mit einem Entwurf bis spätestens Oktober 2023 zu rechnen. Die Hoffnung auf ein Beschäftigtendatenschutzgesetz soll also noch nicht ganz beerdigt werden. Allerdings sind die Vorzeichen wenig ermutigend.

II. Der Beirat zum Beschäftigtendatenschutz

Hubertus Heil, Bundesarbeitsminister auch in der 19. schwarz-rot-regierten Legislaturperiode, hatte am 20.06.2020 einen „Beirat zum Beschäftigtendatenschutz" eingesetzt, der die Grundlage für ein Gesetz legen sollte. Schwarz-Rot hatte sich damals im Koalitionsvertrag auferlegt *zu prüfen, ob ein eigenständiges Gesetz zum Beschäftigtendatenschutz, das die Persönlichkeitsrechte der Beschäftigten am Arbeitsplatz schützt und Rechtssicherheit für den Arbeitgeber schafft,* sinnvoll und notwendig wäre. Um alle Aspekte zu berücksichtigen, wurde dieser Beirat tarifpartei- und disziplinübergreifend besetzt, und zwar mit kompetenten Vertreterinnen und Vertretern von Arbeitgebern und Arbeitnehmern, Wissenschaftlern, Praktikern, Datenschützern, Ethikern, Rechtsanwälten, Juristen und Informatikern. Die Leitung des Beirats wurde in prominente Hände gelegt – in die der früheren Bundesjustizministerin und Arbeitsrechtlerin Herta Däubler-Gmelin.[6]

Der Beirat führte – auch in der Coronazeit – eine Vielzahl von Beratungen und Anhörungen (u.a. mit Vertretern der Bundesvereinigung der Arbeitgeberverbände, des Deutschen Gewerkschaftsbunds, der Datenschutzkonferenz, der Datenethikkommission, mit betrieblichen Datenschutzbeauftragten, Betriebsräten und Unternehmensvertretern) durch. Sein Ergebnis ließ auf sich warten. Zuletzt war vorgesehen den Abschlussbericht noch in der 19. Legislaturperiode im Sommer 2021 abzuliefern. Daraus wurde nichts. Erst im Januar 2022, also schon in der 20. Legislaturperiode, wurde ein Kurzbericht veröffentlicht, der eine allgemeine Orientierung gibt, wohin es mit einem

Beschäftigtendatenschutzgesetz gehen könnte.[7] Die Entwürfe für einen über 100 Seiten umfangreichen Langbericht sahen nie das Licht der Öffentlichkeit. Der Grund: Die Arbeitgebervertreter verweigerten sich einer kontroversen Darstellung und verließen schließlich sang- und klanglos den Beirat. Rechtsanwalt Tim Wybitul, der regelmäßig Arbeitgeber vertritt, erklärte: „Ich kann nichts unterschreiben, was ich nicht später vor Gericht und vor meinen Mandanten gut vertreten kann." Angeblich habe es im Langbericht keine abweichenden Voten geben sollen. Dies kann nicht zutreffen. Selbst im Kurzbericht wird zwischen Beiratsmehrheit und -minderheit unterschieden. Dass sich die Arbeitgeberseite beschwerte, mit ihrer Meinung nicht hinreichend berücksichtigt zu werden, ist wenig überzeugend. Es war nämlich ausgerechnet die Arbeitgeberseite gewesen, die beim Beiratsstart zunächst für einen Konsensbericht plädiert hatte.[8]

Die Geschichte des Beirats zum Beschäftigtendatenschutz ist eine weitere traurige Episode einer never-ending Tragödie, die nun mit einem stillschweigenden Verzicht auf das in der 20. Legislatur angekündigte Gesetz ihre Fortsetzung finden könnte.

III. Das bisher unvollendete Gesetz

Diese Tragödie hat eine ca. 50-jährige Geschichte: 1971 sprach sich ein im Auftrag des Bundesministeriums des Innern erstelltes Expertengutachten zur Schaffung gesetzlicher Datenschutz-Grundlagen für eine spezifische Regelung für Beschäftigte aus.[9] Mit dem Volkszählungsurteil des Bundesverfassungsgerichts (BVerfG) 1983 wurde diese Forderung nach einem bereichsspezifischen Gesetz zusätzlich verfassungsrechtlich grundiert.[10] In späteren Entscheidungen bekräftigte das BVerfG, dass es Aufgabe des Rechts sei zu verhindern, dass sich im Privatrecht, wozu das Arbeitsrecht gehört, „für einen Vertragsteil die Selbstbestimmung in Fremdbestimmung verkehrt".[11] Die der Aussage zugrundeliegende Beschreibung eines Machtgefälles zwischen Vertragsparteien gilt ohne Einschränkungen für das Verhältnis zwischen Arbeitgeber und Arbeitnehmer.

Angesichts dieser verfassungsrechtlichen Vorgaben war es konsequent, dass seit der Volkszählungsentscheidung die Regierungsparteien in ihren Koalitionsabsprachen auf Bundesebene immer wieder ankündigten ein Beschäftigtendatenschutzgesetz[12] zu schaffen. Alle Versuche, ein solches Gesetz zu verabschieden, scheiterten aber am politischen Widerstand der Arbeitgeberseite.[13] Nur ein einziges Mal fand sich in einem Koalitionsvertrag keine Selbstverpflichtung zur Erarbeitung eines solchen Gesetzes – in der 2005 beginnenden 16. Legislaturperiode. Just in dieser Periode gab es in Deutschland derart viele Überwachungsskandale im Beschäftigtenbereich, dass sich die CDU-SPD-Regierung 2009 noch kurz vor der nächsten Bundestagswahl genötigt sah mit dem damaligen § 32 Bundesdatenschutzgesetz (BDSG) zumindest minimale Schutzvorschriften ins Gesetz aufzunehmen.[14] Die damals ergänzte (und seitdem ob ihrer Interpretierbarkeit immer wieder kritisierte) Regelung wurde, leicht modifiziert, nach der Umsetzung der Datenschutz-Grundverordnung (DSGVO) 2019 in den aktuell gültigen § 26 BDSG überführt.

Nicht nur auf nationaler, sondern auch auf europäischer Ebene blieben alle Versuche, den Persönlichkeitsschutz Beschäftigter zu verbessern, in ersten Ansätzen stecken. Eine von der EU-Kommission initiierte Konsultation zum Arbeitnehmerdatenschutzrecht in den Jahren 2001/2002 hatte keine weiteren Initiativen zur Folge. Ein Grund hierfür war wohl, dass selbst auf nationaler Ebene die EU-Mitgliedstaaten fast durchgängig keinen Regelungsbedarf oder – vielleicht wegen des Widerstands der Arbeitgeberseite – keine Einigungsmöglichkeit sahen.

Mit der seit 2009 geltenden europäischen Grundrechte-Charta (GRCh) werden sowohl ein Grundrecht auf Datenschutz (Art. 8) als auch umfassende Arbeitnehmerrechte auf oberster Regulierungsebene garantiert.[15] Zudem können weitere Grundrechte betroffen sein – sowohl der Beschäftigten[16] als auch der Unternehmen[17]. In der DSGVO wurde in Art. 88 ein allgemeiner rechtlicher Rahmen für die nationalen Gesetzgeber sowie für kollektivrechtliche Normen vorgegeben. Die eigentliche Normsetzung soll durch die Mitgliedstaaten erfolgen.[18] Der europäische Gesetzgeber will bisher keine die DSGVO präzisierende Regelung ausarbeiten.

Die politischen Ansagen sowohl in der 19.[19] als auch nun in der 20. Legislaturperiode des Bundestags waren und sind eigentlich klar. Dem entsprechen Forderungen aus Gewerkschaften[20], der arbeitsrechtlichen Praxis[21], dem institutionellen Datenschutz[22] und der Wissenschaft[23]. Die gesetzgeberische Zielsetzung ist ein umfassendes Gesetz zum Datenschutz für Beschäftigte. Kurz vor Ende der 19. Legislaturperiode verständigten sich CDU und SPD – ohne großes öffentliches Aufsehen – auf ein Betriebsrätemodernisierungsgesetz.[24] Darin wurden einige Datenschutzfragen geregelt, insbesondere die Mitbestimmungspflicht beim Einsatz künstlicher Intelligenz (§ 90 Abs. 1 Nr. 3 BetrVG) sowie die Klärung der unsäglichen Streitfrage zur Verantwortlichkeit des Betriebsrats für seine eigene Datenverarbeitung (§ 79a BetrVG).[25] Eine umfassende Regelung des Beschäftigtendatenschutzes erfolgte nicht.

Auch wenn die Begeisterung für ein umfassendes Gesetz in der Bundesregierung weiterhin wenig ausgeprägt scheint, könnte sich nun Druck auf europäischer Ebene aufbauen. Eine Vorlage des Verwaltungsgerichts (VG) Wiesbaden beim Europäischen Gerichtshof (EuGH) stellt diesem die Frage, ob der deutsche Gesetzgeber mit § 26 Abs. 1 S. 1 BDSG (bzw. mit dem inhaltlich identischen § 23 Abs. 1 S. 1 HDSIG) seiner Konkretisierungs- bzw. Spezifizierungspflicht nach Art. 88 DSGVO in Bezug auf den Beschäftigtendatenschutz nachgekommen ist, indem er einfach die europäische Regelung wiederholte.[26] In seinem Votum kommt der Generalanwalt beim EuGH zu dem Ergebnis, dass die deutschen Regelungen nicht mit EU-Recht vereinbar seien, da das Wiederholungsverbot[27] verletzt würde und im nationalen Recht keine spezifischeren Regelungen erlassen worden seien.[28] Solche spezifischeren Regelungen müssten gemäß Art. 88 Abs. 2 DSGVO „geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person" enthalten, was bei § 26 Abs. 1 S. 1 BDSG

nicht zuträfe.[29] Der EuGH folgt in der Regel dem Entscheidungsvorschlag des Generalanwalts. Wäre dies auch hier der Fall, dann wäre die Generalklausel des § 26 BDSG nicht mehr anwendbar[30]; die Gesetzgeber in Deutschland müssten wohl tätig werden.

Derweil verstärkt sich das Machtgefälle zwischen Arbeitgebern und deren Dienstleistern einerseits und den Beschäftigten und ihren Vertretungen andererseits durch immer komplexere Systeme und Verfahren, die zweckübergreifend und oft unternehmensübergreifend ausgeklügeltere intransparente Auswertungen über die Beschäftigten ermöglichen, ohne dass diesen adäquate Rechte zustehen.[31]

IV. Grundüberlegungen zum BeschDSG

Die eingangs geäußerte Hoffnung ist also nicht nur noch lebendig, sie ist auch höchst notwendig. Und daher muss man sich mit den möglichen und notwendigen Inhalten eines Beschäftigtendatenschutzgesetzes (BeschDSG) befassen.[32] Dem sollen einige grundsätzliche Erwägungen vorangestellt werden:

Es ist klar, dass ein BeschDSG einen Ausgleich zwischen den Grundrechten der Arbeitgeber und denen der Beschäftigten vornehmen muss. Beide Seiten sind – Ausnahme ist das öffentliche Dienstecht – als „private" Grundrechtsträger und als Vertragspartner in ihrer Autonomie zu achten. Bei dem Ausgleich muss berücksichtigt werden, dass sich der Arbeitgeber strukturell in einer stärkeren Position befindet, da er durch die Verfügungsmacht über die Produktionsmittel sowie durch seine ökonomische, juristische, informationstechnische und soziale Potenz den Beschäftigten überlegen ist. Die Rechte des Arbeitgebers werden gegenüber Beschäftigten durch ein umfassendes Direktionsrecht (§ 106 Abs. 1 GewO) umgesetzt. Zum Schutz vor dem strukturell überlegenen Vertragsteil hat ein BeschDSG individuelle Rechte für den Beschäftigten vorzusehen, wobei zwischen materiellen und prozessualen Rechten unterschieden werden kann. Ergänzend – auch durch das Grundgesetz abgesichert – stehen den Arbeitnehmern betriebsverfassungsrechtlich garantierte Kollektivrechte zu, die im BeschDSG in Bezug auf den Datenschutz konkretisiert werden könnten.

Bisher ist der Beschäftigtendatenschutz in Deutschland in § 26 BDSG sowie in spezifischen weiteren Gesetzen, etwa den Sozialgesetzbüchern (SGB), dem Arbeitssicherheitsgesetz (ASiG), dem Allgemeinen Gleichstellungsgesetz (AGG) und vielen weiteren – auch untergesetzlichen – Normen geregelt. Angesichts der bestehenden Komplexität ist es weder möglich noch wünschenswert diese Normen in ein BeschDSG zu integrieren, zumal sie dann aus ihren spezifischen Zusammenhängen herausgerissen würden. Wohl aber ist es geboten die allgemeinen Regeln, also insbesondere die zu allgemein gehaltenen Inhalte des § 26, aus dem BDSG herauszulösen und ein eigenes Gesetz zu schaffen. Ein Aufblähen des BDSG wäre wenig anwendungsfreundlich. Wenn auf die DSGVO oder das BDSG verwiesen werden kann sind Regelungen im BeschDSG zu vermeiden. Sinnvoll können aber Regelungen sein, in denen die Vorgaben des allgemeinen Datenschutzrechts konkretisiert werden, etwa zu Datenschutz-Folgenabschätzungen bei der Verarbeitung von Beschäftigtendaten (Art. 35 DSGVO), zu Datenschutzbeauftragten (Art. 37, 38 DSGVO), zu Abwägungen als Rechtsgrundlage (Art. 6 Abs. 1 lit. f DSGVO), zum Auskunftsrecht Beschäftigter (Art. 15 DSGVO), zu Betriebsvereinbarungen als Rechtsgrundlage (Art. 88 DSGVO), zur Zertifizierung von Verfahren (Art. 42 DSGVO) oder zu Aufgaben der Aufsichtsbehörden (vgl. Art. 58 Abs. 6 DSGVO).

Die kollektivrechtliche Seite des Beschäftigtendatenschutzes hat bisher vor allem im Betriebsverfassungsgesetz ihre Grundlage, etwa das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG. Da eine Modernisierung des Beschäftigtendatenschutzes auch eine kollektivrechtliche Seite haben muss, ist es naheliegend parallel das BetrVG und evtl. das Tarifrecht zu ändern, etwa indem zusätzliche Mitbestimmungsrechte eingeführt oder über den Datenschutz hinaus Klagerechte eingeräumt werden. Rein datenschutzrechtliche Festlegungen sollten im BeschDSG normiert werden. Wichtig ist in jedem Fall, dass die Verknüpfung der beiden Rechtsmaterien erkennbar ist.

Es ist im Arbeitsrecht noch weit verbreitet das Datenschutzrecht als eine separate Materie anzusehen und zu behandeln. Dies resultiert beispielsweise in der immer noch anzutreffenden Ansicht, dass in Mitbestimmungsprozessen keine Datenschutzfragen zu thematisieren seien. Entsprechende Herangehensweisen sind bzw. waren im Zivilrecht generell wie speziell im Verbraucher- und im Wettbewerbsrecht zu verzeichnen.[33] Sie ignorieren, dass alle bestehenden Regelungen Bestandteil eines einheitlichen Normgefüges sind, bei dem eine künstlich abschottende Sichtweise zwangsläufig zu Inkonsistenzen und Rechtsverkürzungen führen muss.

Das Beschäftigtendatenschutzrecht wird bisher vorrangig durch die Rechtsprechung konturiert, der des Bundesarbeitsgerichts (BAG) und der Arbeitsgerichte, zunehmend auch über Urteile des Europäischen Gerichtshofs (EuGH). Diese zurückblickende Konkretisierung des Datenschutzes über Einzelfälle erhöht nur bedingt die Rechtssicherheit bei den Beteiligten. Auch muss man konstatieren, dass es für bestimmte Anwendungsfälle, wie beispielsweise zur Videoüberwachung am Arbeitsplatz, eine jahrzehntelange, verfestigende Rechtsprechung gibt, für andere Fragestellungen jedoch keine, sehr wenige oder gar widersprüchliche Entscheidungen. Insbesondere für kleine und mittlere Unternehmen sowie bei Unternehmen ohne Mitbestimmung bestehen für Arbeitgeber und Arbeitnehmer daher viele Unwägbarkeiten bei der Rechtsanwendung. Absehbare technische, ökonomische und soziale Entwicklungen können in Gerichtsurteilen – anders als durch Entscheidungen des Gesetzgebers – nicht berücksichtigt werden. Ein BeschDSG muss dem Anspruch gerecht werden materiell sowie durch klar festgelegte Verfahren die Rechtssicherheit zu erhöhen. Es muss zugleich technologieoffen sein, um für absehbare Änderungen anwendbar zu sein ohne sinnvollen Fortschritt zu hindern. Bei der Festlegung der Regeln können bei der gerichtlichen Kasuistik mit ihren Einzelfallabwägungen Anleihen gemacht werden.

Es wird kontrovers diskutiert, was „spezifischere Vorschriften" i.S.v. Art. 88 Abs. 1 DSGVO sind, die über die Öffnungsklausel sowie in Kollektivvereinbarungen erlaubt sind. Unstreitig ist dabei, dass die DSGVO einen Mindeststandard festlegt, der nicht unterschritten werden darf; die Grenzen der DSGVO sind einzuhalten. Die Diskussion, inwieweit darüber hinausgehende Abweichungen – insbesondere nach unten – zulässig sind, hat eher akademischen Charakter.[34] Das Recht zur Spezifizierung eröffnet einen Ermessensspielraum, wobei bei der Konkretisierung die spezifischen Aspekte des Beschäftigungsverhältnisses ausschlaggebend sein müssen. Es besteht die Möglichkeit zusätzliche, strengere oder einschränkende, nationale Vorschriften vorzusehen.[35] Im Folgenden sollen einige wesentliche Regelungsaspekte eines BeschDSG dargestellt und erörtert werden.

V. Wesentliche Regelungsaspekte

a. Allgemeine Regelungen

Bisher wird der Anwendungsbereich des Beschäftigtendatenschutzes durch § 26 Abs. 8 BDSG in Verbindung mit § 5 BetrVG festgelegt. Erfasst werden Arbeitnehmer einschließlich Leiharbeitnehmer[36], Auszubildende, Rehabilitanden, Beschäftigte in Behindertenwerkstätten, Personen, die Freiwilligendienste oder Zivildienst leisten, Beamte und Richter des Bundes, Soldaten und insbesondere auch die aufgrund ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnlich einzuordnenden Personen. Erfasst werden zudem Personen, die sich für ein Beschäftigungsverhältnis bewerben oder deren Beschäftigungsverhältnis beendet ist. Sinnvoll ist es die neue Kategorie der Crowdworker, also von Beschäftigten, die über das Internet Dienstleistungen für ein Unternehmen erbringen, als arbeitnehmerähnliches Beschäftigungsverhältnis zu präzisieren und von wirtschaftlich nicht abhängigen Soloselbstständigen abzugrenzen.[37]

Hinsichtlich der Wirksamkeit von Einwilligungen im Arbeitskontext macht § 26 Abs. 2 BDSG mit seiner Vermutungsregelung zur Freiwilligkeit schon heute eine präzisierende Vorgabe. Insofern sind beispielhafte Ergänzungen möglich.

b. Bewerbungssituation

Mehr und mehr Unternehmen stützen zumindest Teile ihrer Datenverarbeitung im Bewerbungsprozess auf die Einwilligung der sich Bewerbenden. Dies gilt beispielsweise für nicht im strengen Sinne erforderliche Fragen, für das Durchführen von Persönlichkeitstest und Gesundheitsuntersuchungen und für den Einsatz von digitalen Auswahlverfahren. Auch der Einsatz vermeintlicher künstlicher Intelligenz (KI), etwa durch Sprach- oder Mimikanalyse, soll häufig auf Einwilligungen basieren.[38] Ein aktuell von der EU-Kommission verfolgter Regelungsansatz sieht vor, dass besonders invasive Analyseverfahren nur eingeschränkt oder überhaupt nicht erlaubt sein sollen. Gemäß dem Kommissions-Vorschlag soll der Einsatz von KI bei der Einstellung und Auswahl von Personen, für Entscheidungen über Beförderung und Kündigung sowie für die Zuweisung, Überwachung oder Bewertung von Personen in Arbeitsvertragsverhältnissen als hochriskant (Art. 6 ff. i.V.m. Anhang III Nr. 4 Entwurf KI-Verordnung) eingestuft werden (s.u. VII.).[39]

Der Bewerbungsprozess ist bisher gesetzlich nicht näher geregelt. Die arbeitsgerichtliche Rechtsprechung erlaubt dem Arbeitgeber Fragen zu stellen, an deren Beantwortung er ein „berechtigtes, billigenswertes und schutzwürdiges Interesse" hat.[40] Eine Datenerhebung im Rahmen der Bewerbung muss – im Hinblick auf die angestrebte Stelle – „erforderlich" sein. Zudem gelten die europarechtlich determinierten, diskriminierungsrechtlichen Regelungen des AGG (§ 6 Abs. 1 S. 2 AGG). Es besteht ein „Recht auf Lüge".[41] Hinsichtlich einer Erhebung bei Dritten, etwa bei früheren Arbeitgebern oder im Internet (durch sog. Background-Checks)[42], muss – nicht zuletzt zur Vermeidung von Falschbewertungen – die Einbeziehung der Betroffenen gewährleistet sein. Im Interesse der Rechtsklarheit sollte die bisherige Rechtsprechung gesetzlich fixiert werden, auch im Interesse einer Eindeutigkeit hinsichtlich der Rechtsfolgen im Fall eines Verstoßes. Der Abgleich von Bewerbenden- und Beschäftigtendaten mit sog. Anti-Terror- oder Sanktionslisten bedarf in jedem Fall einer ausdrücklichen, für die Betroffenen transparenten Rechtsgrundlage, so dass eine Rechtsschutzmöglichkeit eröffnet wird. Auch dies ist gesetzlich klarzustellen.

Tests und Untersuchungen können als Einstellungsvoraussetzung erforderlich sein, um die körperliche und psychische Eignung für die konkret angestrebte Stelle festzustellen, etwa bei Tätigkeiten mit Drittgefährdungsmöglichkeit.[43] Solche Tests sind aber nur akzeptabel, wenn sie – was gesetzlich vorzugeben ist – von qualifiziertem Personal gemäß einem (z.B. durch Zertifizierung) validierten Verfahren durchgeführt werden. Hierzu gehört, dass – entsprechend der betriebsärztlichen Betreuung – nur die Ergebnisse der Tests und Untersuchungen, nicht aber die zumeist äußerst sensiblen erhobenen Daten dem Arbeitgeber bekannt werden.[44]

Es sollte ganz allgemein präzisiert werden, dass das durch die jeweilige Interessenslage gekennzeichnete Machtgefälle zwischen Bewerbenden und potenziellem Arbeitgeber eine freiwillige Einwilligung nicht ermöglicht, die Einwilligung als Rechtsgrundlage im Bewerbungsprozess also ausscheidet.

c. Verarbeitung während des Beschäftigungsverhältnisses

Angesichts der vielen unterschiedlichen Fallgestaltungen erscheint eine abschließende Listung der zulässigen Kontrollzwecke im Beschäftigungsverhältnis nicht möglich. Unbefriedigend ist aber auch die in § 26 Abs. 1 S. 1 BDSG enthaltene, auf Art. 88 Abs. 1 S. 1 DSGVO zurückgehende Generalklausel (s.o. III.). Es ist möglich und nötig typische konkretisierte Zwecke beispielhaft zu benennen, wodurch zugleich – bei entsprechender Dokumentation – eine Zweckdifferenzierung erreicht werden kann: Einhaltung gesetzlicher Verpflichtungen, Schutz des Eigentums und Vermögens des Arbeitgebers, Wahrung von Betriebsgeheimnissen, Optimierung von Arbeitsprozessen, Qualitätssicherung der Produktion, Aufdeckung von Straftaten und groben Pflichtverletzungen, Entgeltabrech-

nung, betriebliches Eingliederungsmanagement.[45]

Hinsichtlich der Art und der Intensität der Datenerhebung können gesetzlich relevante Kriterien benannt werden, die bei der Verhältnismäßigkeitsprüfung anzulegen sind, z.B. die zeitliche und räumliche Dimension von Kontrollen, die Sicherung von kontrollfreien Bereichen, Art und Anlass von Kontrollmaßnahmen, prozedurale Vorgaben, Transparenz gegenüber den Betroffenen. Als absolute Grenze sollte eine lückenlose technische Kontrolle am Arbeitsplatz, also eine Dauer- und Totalüberwachung, ausdrücklich ausgeschlossen werden.[46] Die Kriterien dafür, wann von einer solchen Dauer- und Totalüberwachung auszugehen ist, müssen klar definiert werden.

Zumindest für Daten, die alleine aus Gründen der Sicherstellung des ordnungsgemäßen Betriebs und zur Fehlerbehebung erhoben und weiterverarbeitet werden, sollte eine enge Zweckbindung bestehen. Dies betrifft insbesondere so genannte Protokolldaten (Logfiles), die sowohl die Administration als auch die Nutzung von Systemen automatisiert nachzeichnen. Eine Zweckänderung nach Art. 6 Abs. 4 DSGVO sollte ausdrücklich ausgeschlossen werden.

Ein außerdem regulierungsbedürftiger Sonderfall der Beschäftigtenkontrolle ist die im Homeoffice, da hier der räumliche, zeitliche und sozial-familiäre Intimbereich durch Arbeitgebervorgaben tangiert sein kann.[47] Insofern kann und muss die Einwilligung der Betroffenen von Relevanz sein.

d. Ausgewählte konkrete Kontrollanlässe und -maßnahmen

Heimliche Kontrollmaßnahmen des Arbeitgebers, die nur in begründeten Einzelfällen, also ausnahmsweise erlaubt sein können, sind von materiellen Voraussetzungen abhängig zu machen (z.B. zur Aufklärung von erheblichen Straftaten oder schweren Pflichtverletzungen).[48] Anlass für derartige Maßnahmen muss in jedem Fall ein zu dokumentierender konkreter hinreichender Verdacht sein. Im Interesse der Wahrung der Verhältnismäßigkeit ist ein eskalierendes Vorgehen zu prüfen. Die Maßnahmen bedürfen einer verfahrensmäßigen Einhegung. Diese kann darin bestehen, dass der betriebliche Datenschutzbeauftragte und der Betriebsrat einbezogen werden. Es ist klarzustellen, dass die Mitbestimmungsrechte durch einen datenschutzrechtlich normierten Erlaubnistatbestand nicht obsolet werden.

Im Rahmen des Arbeitsverhältnisses entstehen angesichts einer zunehmenden Digitalisierung im Bereich der Produktion, Kommunikation und Organisation oft zwangsläufig bzw. nebenbei beschäftigtenbezogene Daten. Hierbei kann es sich um sensitive i.S.v. Art. 9 DSGVO oder sonstige besondere schutzbedürftige Daten handeln. Deren Sekundärnutzung und die damit verbundene Zweckänderung, z.B. für Verhaltens- und Leistungskontrollen, muss auf das unbedingt erforderliche und verhältnismäßige Maß eingeschränkt werden. Sie muss in einem für die Beschäftigten transparenten und damit kalkulierbaren Verfahren erfolgen. Die Einbeziehung des Betriebsrats bei diesem Verfahren sollte gesetzlich vorgesehen werden; die konkrete Ausgestaltung in Form von Informations-, Kontroll- und Interventionsrechten kann Betriebsvereinbarungen überlassen werden (zur Mitbestimmung s.u. V.e.). Die Zweckänderung von besonders invasiv erhobenen Daten, etwa über Gefühle oder Gesundheitszustände, ist vollständig gesetzlich auszuschließen.

Arbeitgeber schalten bei ihrer Datenverarbeitung zunehmend Dritte ein, die Hard- und Software (z.B. beim Cloud-Computing) bereitstellen, aber auch weitergehende Dienstleistungen und Personal zum Einsatz bringen. Es ist gesetzlich sicherzustellen, dass hierbei der Arbeitgeber, etwa durch die Vertragsgestaltung mit dem Dienstleister, gewährleistet, dass sämtliche individuellen und kollektiven Rechte der Betroffenen bzw. des Betriebsrates wahrgenommen werden können.[49] Weiterhin muss gewährleistet werden, dass diese Dienstleister die erhobenen Daten nur für legitime und nicht für kommerzielle eigene Zwecke nutzen. Beispielsweise ist klarzustellen, dass die Nutzung von Beschäftigtendaten (Kundendaten) durch den Dienstleister zur Weiterentwicklung eines eigenen Produkts als kommerzielle Nutzung gilt und zu unterbleiben hat.

Insbesondere Arbeitgeber in Konzernverbünden strukturieren ihre Arbeitshierarchie häufig über eine sog. Matrix-Organisation. Diese dient in der Regel der gesellschaftsübergreifenden Projektarbeit und soll die disziplinarischen Zuständigkeiten auch über die Arbeitgebergrenzen hinweg innerhalb eines Mutterkonzerns sicherstellen, wozu ein berechtigtes Interesse des Arbeitgebers bestehen kann. Überschreiten die Konzernunternehmen hierbei reine Hilfsfunktionen und bestimmen dadurch Zwecke und Mittel der Datenverarbeitung, so besteht eine gemeinsame datenschutzrechtliche Verantwortung. Gesetzlich kann zumindest beispielhaft aufgeführt werden, wann in solchen Fällen ein berechtigtes Interesse des Arbeitgebers besteht und welche berechtigten Interessen von Beschäftigten der Verarbeitung entgegenstehen können. Der Arbeitgeber hat in diesen Fällen jedenfalls sicherzustellen, dass für die Beschäftigten transparent ist, welcher Konzernteil welche Aufgaben wahrnimmt. Werden hierbei Beschäftigtendaten des Arbeitgebers mit Daten anderer Konzernunternehmen verknüpft so sind, unbeschadet bestehender Mitbestimmungsrechte der Interessenvertretungen, durch explizit festzulegende und zu dokumentierende geeignete Maßnahmen die Beschäftigteninteressen sicherzustellen.

Die Verarbeitung sensitiver Daten gemäß Art. 9 DSGVO, insbesondere von Gesundheitsdaten, ist schon bisher weitgehend bereichsspezifisch geregelt.[50] In diesen Regelungen sind Anlass, Zweck, Umfang und Beteiligte der Datenverarbeitung zumeist rechtssicher festgelegt. Zudem besteht in § 26 Abs. 3 BDSG eine generalklauselhafte Regelung ohne praktische Relevanz. Da sie lediglich europarechtliche Vorgaben wiederholt, dürfte diese Regelung, ebenso wie § 26 Abs. 1 S. 1 BDSG, europarechtlich unzulässig und deshalb nicht anwendbar sein (s.o. III.). Die Notwendigkeit einer über die bereichsspezifischen Festlegungen hinausgehenden gesetzlichen Norm bedarf einer näheren Begründung, zumal Spezifizierungen des Art. 9 Abs. 2 lit. b DSGVO auch durch Kollektivvereinbarungen nach Art. 88 Abs. 1 DSGVO möglich sind. Jedenfalls sind zusätzliche Sicherungen vorzusehen.

Hinsichtlich der Eingriffsschwere ist die Verarbeitung von sensitiven Daten mit Verhaltens- und Leistungskontrollen oder mit dem Einsatz von KI-Verfahren vergleichbar. Es bietet sich an zumindest diese Art der Datenverarbeitung auch mitbestimmungspflichtig zu machen (s.u. weitergehend V.e.).

Der Einsatz von sog. künstlicher Intelligenz (KI) in Beschäftigungsverhältnissen nimmt stark zu, etwa in Bewerbungsverfahren, bei der Gefahrenvorsorge, beim Einsatz von sog. sozialen Medien oder im Rahmen der Produktion. Die Regelung des Art. 22 DSGVO, die die automatisierten Entscheidungen auch im Beschäftigungsverhältnis reguliert, greift vielmals zu kurz.[51] Im Fall einer Regulierung bedarf es zunächst einer möglichst präzisen Festlegung, welche Verfahren erfasst sein sollen. Angesichts des Umstands, dass die EU eine umfassende KI-Verordnung plant, die auch für Beschäftigungsverhältnisse gelten soll (s.o. V.b.), erscheint eine nationale materiell-rechtliche Vollregelung nicht erforderlich. Um zu vermeiden, dass sich eine entsprechende Praxis etabliert, sollte aber klargestellt werden, dass der Einsatz von KI allein auf Basis einer individuellen Einwilligung nicht statthaft ist. Eine Unterrichtungspflicht in Bezug auf KI wurde 2021 mit dem Betriebsrätemodernisierungsgesetz in den §§ 80 Abs. 3 S. 2, 90 Abs. 1 Nr. 3 BetrVG konkretisiert. Eine Mitbestimmungspflicht beim KI-Einsatz in Personalentscheidungen wurde in § 95 Abs. 2a BetrVG eingeführt.[52]

Die EU hat eine Whistleblower-Richtlinie[53] erlassen, die am 17.12.2021 in deutsches Recht hätte umgesetzt sein müssen. Nunmehr liegt ein Entwurf eines Hinweisgeberschutzgesetzes vor, der wohl hauptsächlich bei Beschäftigungsverhältnissen anzuwenden sein wird. Dieser in manchen Einzelfragen noch umstrittene Entwurf wird voraussichtlich in Bälde Gesetz.[54] Angesichts dessen scheint es nicht angebracht allgemeine Regelungen hierzu in ein BeschDSG zu integrieren. Es kann aber evtl. zusätzlich nötig sein, spezifisch arbeitsrechtliche Fragen, etwa zu einem Disziplinierungs- und Kündigungsschutz oder Aspekte zum Umfang der trotz gesetzlicher Vorgabe bestehenden Mitbestimmungsrechte bei der Ausgestaltung konkreter Hinweisgebersysteme in das Hinweisgeberschutzgesetz oder auch ins BeschDSG aufzunehmen.

e. Kollektivrechtliche Aspekte

Der Betriebsrat hat gemäß § 80 Abs. 1 Nr. 1 BetrVG die Aufgabe die Einhaltung der Arbeitnehmer schützenden Gesetze zu überwachen. Hierzu gehört die Überwachung der Beachtung des Datenschutzrechts. Dies wird in § 75 Abs. 2 S. 1 BetrVG bestärkt, wonach es dem Betriebsrat zukommt die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Diese Förderungsaufgabe kann dadurch verstärkt werden, dass dem Betriebsrat insofern gesetzlich explizit ein Initiativrecht zugestanden wird.

Durch das Betriebsrätemodernisierungsgesetz wurde in § 79a BetrVG klargestellt, dass die datenschutzrechtliche Verantwortlichkeit für die personenbezogene Verarbeitung durch den Betriebsrat beim Arbeitgeber verbleibt. Der unabhängige Betriebsrat hat mit dem Arbeitgeber zu kooperieren. Beispielhaft können die sich hieraus ergebenden Pflichten konkretisiert werden, etwa in Bezug auf die Erstellung des Verarbeitungsverzeichnisses nach Art. 30 DSGVO, die Umsetzung der Betroffenenrechte nach Art. 12 ff DSGVO oder die Erstellung eines Löschkonzepts für die beim Betriebsrat rechtmäßig verarbeiteten Daten. Hinsichtlich der Datenschutzkontrolle beim Betriebsrat ist vorstellbar, dass der Datenschutzbeauftragte hiermit ein Betriebsratsmitglied beauftragt.

Datenschutzbeauftragter und Betriebsrat verfolgen bzgl. der Verarbeitung von Beschäftigtendaten gleichgerichtete Aufgaben und Interessen. Um eine enge und gute Kooperation zu erleichtern, ist es sinnvoll, unabhängig von bestehenden Mitbestimmungsrechten nach § 99 BetrVG, die Einstellung und Abberufung von (internen wie externen) Datenschutzbeauftragten mitbestimmungspflichtig zu machen.[55] Bei der Beurteilung der gesetzlich geforderten fachlichen Kompetenz, zu der auch die Kompetenz gehört die Persönlichkeitsrechte der Beschäftigten zu wahren, ist die Erfahrung und Expertise des Betriebsrates von Bedeutung. Angesichts des erhöhten Kündigungsschutzes, den betriebliche Datenschutzbeauftragte genießen, ist es schon bei deren Bestellung von zentraler Bedeutung, dass diese Person das Vertrauen des Betriebsrats genießt und die Fähigkeit hat in datenschutzrechtlichen Konflikten im Betrieb zwischen Arbeitgeber und Arbeitnehmervertretung zu vermitteln.

Eine Erweiterung der Mitbestimmungspflicht bietet sich – in Erweiterung des § 87 Abs. 1 Nr. 6 BetrVG – generell für die Ausgestaltung und Konkretisierung des Beschäftigtendatenschutzes im Betrieb an. Es ist bisher oft unklar, inwieweit bei Verfahren, die zur Verhaltens- und Leistungskontrolle geeignet sind, Regelungen in einer Betriebsvereinbarung erlaubt und geboten sind (zu Verarbeitungszwecken, Zugriffsberechtigungen, Löschkonzepten, technisch-organisatorischen Maßnahmen, Betroffenenrechten).[56] Durch eine entsprechende Erweiterung kann diese Unsicherheit beseitigt und dem Auftrag in § 75 Abs. 2 S. 1 BetrVG eine prozessuale Grundlage gegeben werden.[57] Zudem sollte künftig gesetzlich gewährleistet werden, dass Betriebsräte bei der Erstellung einer Datenschutz-Folgenabschätzung für Beschäftigtendaten verarbeitende Systeme und Verfahren gemäß Art. 35 Abs. 9 DSGVO zwingend eingebunden werden.[58]

Der von Art. 88 DSGVO vorgesehene Abwägungsprozess kann über in Betriebsvereinbarungen fixierte angemessene Garantien gestaltet werden. Dies kann der Fall sein, wenn die Wahrung schutzwürdiger Betroffeneninteressen eine Verarbeitung zur Umsetzung berechtigter Interessen legitimieren soll (Art. 88 Abs. 1 S. 1 i.V.m. Art 6 Abs. 1 lit. f DSGVO), was auch im Fall der Verarbeitung sensitiver Daten relevant sein kann (Art. 9 Abs. 2 lit. b DSGVO). Bei Datentransfers in ein aus Datenschutzsicht unsicheres Drittland können dort geeignete Garantien geregelt werden, die z.B. ergänzend zu Standarddatenschutzklauseln oder Binding Corporate Rules (Art. 47 DSGVO) zur Anwendung kommen (Art. 46 DSGVO).

In der Praxis wird häufig darüber gestritten, ob der Betriebsrat einen Anspruch darauf hat, dass ihm die vom

verantwortlichen Arbeitgeber zu erstellenden datenschutzrechtlichen Dokumente, soweit sie die Verarbeitung von Beschäftigtendaten betreffen, gemäß § 80 Abs. 2 S. 2 BetrVG vorgelegt werden müssen. Zwecks Klarstellung der Rechtslage sollte festgehalten werden, dass dem Betriebsrat die relevanten Dokumente (u.a. Verarbeitungsverzeichnis gemäß Art. 30 DSGVO, Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO, Verträge zur Auftragsverarbeitung und zur gemeinsamen Verantwortlichkeit gemäß Art. 26, 28 DSGVO, Zertifizierungsunterlagen gemäß Art. 42 DSGVO, Verträge und Genehmigungen zur Drittauslandsübermittlung gemäß Art. 45 ff. DSGVO) bereitzustellen sind.

Die datenschutzrechtliche Expertise von Betriebsräten hat in den letzten Jahren zugenommen. In noch stärkerem Maße zugenommen hat aber die rechtliche und technische Komplexität von Informations- und Kommunikationssystemen. Diese entsteht durch erweiterte Funktionalität und Komplexität von Daten und Software, stärkere Vernetzung mit vielfältigen Schnittstellen, den Einsatz von nicht selbst betriebenen Systemen und generell durch die Einbindung externer IT-Dienstleister. Überschreiten Systeme eine bestimmte Komplexitätsschwelle, ist der Betriebsrat zur Wahrung seiner Aufgaben darauf angewiesen externen Sachverstand hinzuziehen. Die Bestimmung in § 80 Abs. 3 BetrVG zur Sicherstellung der erforderlichen sachverständigen Unterstützung sollte dadurch verbessert werden, dass die Hinzuziehung von Sachverständigen bei bestimmten Systemgestaltungen gesetzlich vermutet wird. Um den Anreiz zu erhöhen unabhängig geprüfte Verfahren einzusetzen, kann gesetzlich geregelt werden, dass im Fall einer Zertifizierung gemäß Art. 42 DSGVO die Rechtskonformität gesetzlich angenommen wird.[59]

f. Betroffenenrechte

Die Betroffenenrechte sind in den Art. 12 ff. DSGVO weitgehend abschließend reguliert. Zwar sind viele Aspekte in der Rechtsprechung und der Literatur umstritten. Eine Klärung dieser Streitfragen muss wegen des abschließenden Charakters der DSGVO jedoch weitgehend den Gerichten überlassen bleiben.[60] Eine Ausnahme hiervon besteht für Beschränkungen der Betroffenenrechte, wo über eine Öffnungsklausel Spielräume für nationale Regelungen bestehen (Art. 23 DSGVO). Insbesondere hinsichtlich des Schutzes der Rechte und Freiheiten anderer Personen (Art. 23 Abs. 1 lit. i DSGVO) bestehen arbeitsrechtliche Konkretisierungsmöglichkeiten. Es sollte klargestellt werden, dass Betriebs- und Geschäftsgeheimnisse dem individuellen Auskunftsersuchen nach Art. 15 DSGVO nicht entgegengehalten werden können.

Konkretisierungen sind auch hinsichtlich der Verfahren zur Inanspruchnahme der Betroffenenrechte vorstellbar, etwa zu Antwortfristen, zum Ablauf des Auskunftsverfahrens oder zum Technikeinsatz.

Große Unsicherheit besteht bisher hinsichtlich der Regelfristen für die Löschung personenbezogener Daten. Es gibt, etwa im Gesundheits-, im Steuer- und im Handelsrecht spezifische Regelungen, nicht aber für Standardprozesse in Beschäftigungsverhältnissen (Personalakte nach Beendigung des Beschäftigungsverhältnisses, Lohnnachweise, Zeugnisse und Bewertungen, Abmahnungen). Gesetzliche Vorgaben können hier Rechtssicherheit für alle Beteiligten schaffen. Auch sollten, möglicherweise mit Bezug auf DIN 66398, grundlegende Anforderungen an die Festlegung und Dokumentation von Regellöschfristen formuliert werden.

Besteht in einem Unternehmen ein Betriebsrat, haben die betroffenen Beschäftigten eine datenschutzrechtliche Interessenvertretung. Fehlt es hieran, so ist das Übergewicht der Arbeitgeberseite gegenüber den isolierten Beschäftigten höher. Dem kann durch kompensierende individuelle Rechte, z.B. solche, die ansonsten auch dem Betriebsrat zustehen, entgegengewirkt werden.[61]

g. Folgen rechtswidriger Datenverarbeitung und Rechtsdurchsetzung

Es ist oft streitig, inwieweit bei unzulässiger Datenerhebung und -speicherung ein Sachvortrags- oder ein Beweisverwertungsverbot im Rahmen von gerichtlichen Verfahren, etwa anlässlich einer Kündigung, besteht.[62] Hinsichtlich des gebotenen Interessenausgleichs der Beteiligten schafft eine gesetzliche Regelung mit Regelbeispielen, wofür die Rechtsprechung Anhaltspunkte liefern kann, mehr Klarheit. Zugleich lassen sich so die Anreize für eine unzulässige Datenverarbeitung verringern. Den Parteien sollte ausdrücklich in einer Betriebsvereinbarung die Möglichkeit der Vereinbarung von Verwertungsverboten eröffnet werden, auch bei der Missachtung von Mitbestimmungsrechten.

Das bestehende Abhängigkeitsverhältnis zum Arbeitgeber sowie Rechtsunsicherheiten können dazu führen, dass Beschäftigte vor einer Kontaktaufnahme mit der Aufsichtsbehörde zurückschrecken und eine gerichtliche Auseinandersetzung mit ihrem Arbeitgeber scheuen. Art. 80 DSGVO sieht vor, dass nicht nur die betroffene Person selbst, sondern Verbände im Verfahren oder Prozess auftreten können. Nach Art. 80 Abs. 1 DSGVO kann eine betroffene Person einen Verband insofern beauftragen, beispielsweise um ihr Beschwerderecht bei einer Aufsichtsbehörde auszuüben oder Ansprüche auf Information, Auskunft und Unterlassung gegen den Verantwortlichen geltend zu machen. Gemäß Art. 80 Abs. 2 DSGVO können Mitgliedstaaten ein von einem Auftrag durch Betroffene unabhängiges Verbandsklagerecht einführen – auch für Betriebsräte oder Gewerkschaften.[63] Damit kann ein Beitrag geleistet werden in Erweiterung der auf Verbraucher abzielenden europäischen Verbandsklagerichtlinie, die bis zum 25.12.2022 hätte umgesetzt werden müssen.[64] Mit kollektiven Rechtsdurchsetzungsmöglichkeiten können individuelle Rechtsverfahren vermieden und zugleich bestehende Vollzugsdefizite verringert werden. Dies erhöht die Rechtskonformität bei der Verarbeitung von Beschäftigtendaten und entlastet alle Beteiligten.

VI. Etablierung einer Beschäftigtendatenschutzkommission

Der Beirat zum Beschäftigtendatenschutz hat die Schaffung einer ständigen Beschäftigtendatenschutzkommission beim Bundesministerium für Arbeit und Soziales (BMAS) vorge-

schlagen, die Entwicklungen im Bereich des Beschäftigtendatenschutzes begleiten und abstrakte Regelungen für die Praxis konkretisieren soll. Die Beteiligung der Datenschutzaufsichtsbehörden und der Sozialpartner sollen hierbei sichergestellt werden. Das Gremium soll die Normgeber beraten und neue Instrumente in den Blick nehmen, etwa zur Entwicklung von Standards, Best-Practice-Ansätzen, Musterdokumenten, Audits und Prüfkriterien für Datenschutzzertifizierungen (vgl. Art. 42 Abs. 5 DSGVO). Ein solches Gremium kann dazu beitragen, dass angepasst an aktuelle technische Entwicklungen ein frühzeitiger Ausgleich zwischen Arbeitgeber- und Beschäftigteninteressen gesucht und gefunden wird und dass dieser Ausgleich nicht allein den Betriebsparteien und den Gerichten überlassen wird.[65]

VII. Schlussbemerkung

Die Geschichte des bisherigen Scheiterns eines Beschäftigtendatenschutzgesetzes und des Langberichts des dafür eingesetzten Beirats zeigt, dass eine Einigung zwischen Arbeitgeber- und Arbeitnehmervertretern bis heute nicht gelungen und auf kurze Sicht nicht absehbar ist. Die Arbeitgeberseite verweigert sich bisher einer zeitgemäßen Regulierung. Angesichts des hohen und zunehmenden Problempotentials darf dies nicht der Grund für die Politik sein sich den Regelungsnotwendigkeiten zu entziehen. Es ist gerade bei dieser Konstellation geboten zum Schutz der schwächeren Partei – der Beschäftigtenseite – gesetzliche Vorgaben zu machen. Dies hindert die Politik nicht den praktischen Bedürfnissen der Unternehmen hinsichtlich Rationalisierung der Datenverarbeitung und der Effektivierung von Organisation, Produktion und Verfahren durch Digitalisierung zu entsprechen. Die Politik hat in Deutschland aufgrund ihrer profunden Erfahrung im gesetzlichen Datenschutz die Möglichkeit EU-weit Standards zu setzen. Ein gutes Gesetz vermittelt der Arbeitgeberseite vielleicht die Einsicht, dass der Datenschutz der Beschäftigten letztlich auch in ihrem Interesse liegt und zu erhöhter Rechtssicherheit führt. Eine regulierte und interessenwahrende Datenverarbeitung erhöht die Zufriedenheit der Beschäftigten und dadurch deren Motivation, deren Zufriedenheit und letztlich deren Kreativität und Produktivität.

1 Dokumentiert in DANA 1/2022, 18 ff., hier 19.

2 BMAS veröffentlicht Ergebnisse des unabhängigen, interdisziplinären Beirats zum Beschäftigtendatenschutz, www.bmas.de 21.01.2022.

3 Digitalstrategie, Gemeinsam digitale Werte schöpfen, https://www.bmvi.de/SharedDocs/DE/Anlage/K/presse/063-digitalstrategie.pdf?__blob=publicationFile, S. 36 f.

4 Dazu DVD-PE 08.09.2022, Wissings Digitalstrategie ist ein wertloser Ankündigungskatalog, https://www.datenschutzverein.de/wp-content/uploads/2022/09/2022-09-Digitalstrategie.pdf; in diesem Heft, S. 248.

5 E-Mail des stellv. Pressesprechers des BMAS an die Autoren v. 27.09.2022.

6 Beirat Beschäftigtendatenschutzgesetz, DANA 3/2022, 183.

7 Abgedruckt in diesem Heft, S. 228.

8 Schulzki-Haddouti, Streit um Beschäftigten-Datenschutzgesetz, www.heise.de 13.05.2022, Kurzlink: https://heise.de/-7089189.

9 Steinmüller/Lutterbeck/Mallmann/Kolbe/Schneider, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministers des Innern, 1971, BT-Drs. VI/3826, S. 134 f., 155 ff.

10 BVerfG 15.12.1983 – 1 BvR 209/83 u.a., NJW 1984, 419 ff.

11 BVerfG 23.10.2006 – 1 BvR 2027/02, Rn. 33-36, JZ 2007, 577.

12 Damals noch: Arbeitnehmerdatenschutzgesetz.

13 Nachweise für die vielfachen Bestrebungen bei Seifert in Simitis, BDSG, 8. Aufl. 2016, § 32, Rn. 1.

14 Gesetz zur Änderung datenschutzrechtlicher Vorschriften v. 14.08.2009, BGBl. I S. 2814.

15 Art. 27 ff. GRCh: u.a. Rechte auf rechtzeitige Unterrichtung und Anhörung, auf kollektive Interessenverteidigung, auf gesunde, sichere und würdige Arbeitsbedingungen; dazu Weichert/Schuler, Besondere Probleme im Beschäftigtendatenschutz und Empfehlungen für ein Beschäftigtendatenschutzgesetz, 18.12.2020, www.netzwerk-datenschutzexpertise.de, S. 7 f.; Weichert NZA 2020, 1599.

16 Zu nennen ist insbesondere die freie Telekommunikation (Art. 10 GG, Art. 7 GRCh) und – wegen der zunehmenden Homeoffice-Tätigkeit – der Schutz der Wohnung (Art. 13 GG, Art. 7 GRCh).

17 Recht auf Eigentum, Berufsfreiheit, Unternehmensfreiheit, Art. 12, 14 GG, Art. 15-17 GRCh).

18 Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 2017, Teil 9 Rn. 6 (S. 134 f.).

19 Weichert/Schuler (En. 15), S. 5 f.

20 Statt vieler siehe Entwurf des DGB sowie Aufsatz von Wedde in diesem Heft, S. 224.

21 Rüdesheim AiB 2021, 30 ff.

22 Kelber/Blufarb ZRP 4/2022 Editorial. Datenschutzkonferenz, 04.05.2022, Die Zeit für ein Beschäftigtendatenschutzgesetz ist „Jetzt"! https://www.datenschutzkonferenz-online.de/media/en/Entschliessung_Forderungen_zum_Beschaeftigtendatenschutz.pdf.

23 Z.B Datenethikkommission, zit. in Weichert/Schuler (En. 15) S. 6 f.

24 G.v. 14.06.2021, BGBl. I S. 1762.

25 Rüdesheim AuR 2021, 345 f.; Kuß/Langenheim CR 2022, 235 ff.

26 VG Wiesbaden 21.12.2020 – 23 K 1360 / 20 WI.PV.

27 EuGH 07.02.1973 – C-39/72, Rn. 17; EuGH 10.10.1973 – C-34/73, Rn. 10, 11; Weichert in Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 2. Aufl., 2020, Einleitung Rn. 35a; Selmayr/Ehmann in Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Einführung Rn. 80.

28 EuGH-Generalanwalt Sanchez-Bordona 22.09.2022 – C-34/21, Rn. 58 ff.

29 EuGH-Generalanwalt Sanchez-Bordona 22.09.2022 – C-34/21, Rn. 69-75.

30 Schlussanträge des Generalanwalts v. 22.09.2022 – C-34/21.

31 Weichert/Schuler (En. 15); S. 10 ff.

32 Dazu schon – mit teilweise noch weitergehenden Vorschlägen – Weichert/Schuler (En. 15).

33 Weichert in Däubler/Wedde/Weichert/Sommer (En. 27), Einleitung UKlaG Rn. 3a ff., 9 ff.

34 BAG 27.05.1986 – 1 ABR 48/84, NJW 1987, 674 = MDR 1987, 83 = NZA 1986, 643 = BB 1986, 1087, 2333 = DB 1986, 2080, Rn. 97; Rüdesheim AuR 2021, 344; Klebe in Däubler/Klebe/Wedde, BetrVG, 18. Aufl., 2022, § 87 Rn. 195 m.w.N.

35 EuGH 28.04.2022 – C-319/20, NJW 2022, 1740 = NVwZ 2022, 945 = GRUR 2022, 920 = EuZW 2022, 522 = K&R 2022, 422 = afp 2022, 224, Rn. 57; EU-Generalanwalt

Sanchez-Bordona 22.09.2021 – C-34/21, Rn. 46.

36 Insofern muss festgelegt werden, dass deren Datenschutzrechte auch gegenüber dem ausleihenden Unternehmen gelten.

37 Däubler, Gläserne Belegschaften, 9. Aufl. 2021, Rn. 183d.

38 Greif/Kollmann ZAS 2021, 61 ff.; Hoffmann NZA 2022, 19 ff.

39 ErwGr 36 Entwurf KI-Verordnung

40 BAG 07.09.1995 – 8 AZR 828/93, NZA 1996, 637 = BB 1996, 217 = BB 1995, 1961 = DB 1996, 634.

41 Ständige Rechtsprechung seit BAG 05.12.1957 – 1 AZR 594/56, NJW 1958, 516 = MDR 1958, 372 = DB 1958, 227, 228, 282.

42 Däubler (En. 37), Rn. 211a.

43 So Vorgaben gemäß ArbSchG, ArbMedVV, SGB VII.

44 Schuler/Weichert, Die Datenverarbeitung des Betriebsarztes, www.netzwerk-datenschutzexpertise.de 22.09.2020, S. 8.

45 Däubler (En. 37), Rn. 394 ff.

46 BAG 27.03.2003 – 2 AZR 51/02, NJW 2003, 3436 = MDR 2004, 39 = NZA 2003, 1193 = BB 2003, 2578 = DB 2003, 2230 = JR 2004, 132.

47 Wedde AiB 2021, 24 f.; Leissler/Terharen ZAS 2022, 99 ff.; Müller, Homeoffice in der arbeitsrechtlichen Praxis, 2019.

48 EGMR (Große Kammer) 17.10.2019 - 1874/13, 8567/13, NJW 2020, 141 = NZA 2019, 1697 = AuR 2020, 131 (López Ribalda ua / Spanien).

49 Schuler/Weichert (En. 15), S. 14 f.

50 U.a. in SGB V, VII und IX, EFZG, ASiG, ArbSchG, ArbMedVV, IfSG, im Beamtenrecht; § 19 ff. GenDG.

51 Zu den allgemeinen datenschutzrechtlichen Anforderungen Datenschutzkonferenz, Hambacher Erklärung zur Künstlichen Intelligenz v. 03.04.2019.

52 Klebe CuA 10/2021, 16f.; Ruchhöft CuA 7-8/2021, 20 ff.; siehe auch Schröder/Höfers, Praxishandbuch Künstliche Intelligenz, 2022.

53 Richtlinie (EU) 2019/1937 v. 23.10.2019.

54 Dzida NZA 8/2022 Editorial; Gerdemann ZRP 2022, 98 ff.; Tölle ZRP 2022, 156 ff.

55 Rüdesheim AuR 2021, 347; Weichert/Schuler (En. 15) S. 25.

56 Dafür z.B. Holthusen RdA 2021, 28 ff.

57 Rüdesheim AuR 2021, 346 f.

58 Weichert/Schuler (En. 15) S. 20 f., 25 f.

59 Weichert/Schuler (En. 15), S. 21.

60 Zur Auskunft gemäß Art. 15 DSGVO Lembke/Fischels NZA 2022, 513 ff.

61 Weichert/Schuler (En. 15) S. 18 f.

62 Erfinger RdA 2021, 9 ff.; Rüdesheim AuR 2021, 347 f.

63 Rüdesheim AuR 2021, 348.

64 Oltmans NZA 16/2022 Editorial; Walter/Fischer K&R 2022, 32 ff.; Weichert/Schuler (En. 15) S. 26 f.

65 Weichert/Schuler (En. 15), S. 24.

Peter Wedde

Beschäftigtendatenschutz aus gewerkschaftlicher Sicht

Die Datenschutz-Grundverordnung (DSGVO) verzichtet darauf einheitliche europaweit gültige Regelungen zum Beschäftigtendatenschutz vorzugeben. Art. 88 DSGVO trägt zwar die Überschrift „Datenverarbeitung im Beschäftigungskontext“, beschränkt sich aber inhaltlich insbesondere darauf den Mitgliedsstaaten die Verantwortung für die Schaffung spezifischer gesetzlicher Regelungen zuzuweisen. Als mögliche Regelungsinhalte werden in Art. 88 Abs. 1 DSGVO Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags, des Managements, der Planung und der Organisation der Arbeit genannt, zudem zur Gleichheit und Diversität oder zur Gesundheit und Sicherheit am Arbeitsplatz sowie zum Schutz des Eigentums von Arbeitgebern und Kunden. Art. 88 Abs. 2 DSGVO gibt vor, dass Regelungen in den Mitgliedsstaaten insbesondere angemessene Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen umfassen sollen. Als spezifische Regelungsthemen werden die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb von Konzernstrukturen und Überwachungssysteme am Arbeitsplatz benannt.

In Deutschland wurde die durch die DSGVO eröffnete Möglichkeit zur Schaffung eines Beschäftigtendatenschutzgesetzes bisher nicht genutzt. Ein im Sommer 2020 vom Bundesminister für Arbeit und Soziales eingesetzter interdisziplinärer Expertenbeirat hat zwar anlässlich der Übergabe seines Berichts festgestellt, dass zentrale Elemente des Beschäftigtendatenschutzes einer wirksamen und rechtssicheren gesetzlichen Festlegung bedürfen.[1] Bundesarbeitsminister Hubertus Heil hat anschließend darauf hingewiesen, dass die neue Koalition in der aktuellen Legislatur Regelungen zum Beschäftigtendatenschutz schaffen will, um Rechtsklarheit für Arbeitgeber und Beschäftigte zu erreichen und die Persönlichkeitsrechte der Beschäftigten effektiv zu schützen.[2] Über den Arbeitsstand zu diesem Thema ist aber in der Öffentlichkeit bisher nichts bekannt. Damit setzt sich auf der politischen Ebene die „unendliche Geschichte“ fort, die sich bezüglich der Schaffung eines gesetzlichen Beschäftigtendatenschutzes in den letzten Jahrzehnten abgespielt hat.[3]

In der Arbeitswelt wurde und wird die Erforderlichkeit einer in sich geschlossenen Regelung zum Beschäftigtendatenschutz unterschiedlich eingeschätzt. Von Arbeitgeberseite wird ein solches Gesetz vielfach mit dem Argument abgelehnt, dass das geltende Datenschutzrecht ausreiche. Gewerkschaften, Betriebs- sowie Personalräte