Hans Böckler Stiftung
Mitbestimmung · Forschung · Stipendien

MITBESTIMMUNGSPRAXIS

Nummer 3

BESCHÄFTIGTENDATENSCHUTZ: RECHTLICHER RAHMEN UND HANDLUNGS-MÖGLICHKEITEN FÜR BETRIEBSRÄTE

Peter Wedde

MF MITBESTIMMUNGS-FÖRDERUNG

Hans Böckler Stiftung
Mitbestimmung · Forschung · Stipendien

MITBESTIMMUNGSPRAXIS

Nummer 3

BESCHÄFTIGTENDATENSCHUTZ: RECHTLICHER RAHMEN UND HANDLUNGSMÖGLICHKEITEN FÜR BETRIEBSRÄTE

Peter Wedde

ZUSAMMENFASSUNG

Über das Internet vernetzte Smartphones, Tablets oder Notebooks sind allgegenwärtig. Gleiches gilt für die vielen Anwendungsprogramme, kurz „Apps“ genannt, die kostenlos oder zu geringen Preisen im Internet angeboten werden. Dass in den verschiedenartigen Anwendungen zugleich eine Fülle von personenbezogenen Daten anfällt, stört die meisten Nutzer nicht. Dies gilt auch für intensiver werdende Verhaltens- und Leistungskontrollen im beruflichen Kontext.

Werden in technischen Systemen personenbezogene Daten verarbeitet, muss beurteilt werden, ob mögliche Kontrollen zulässig sind. Mangels spezieller gesetzlicher Regeln zum Beschäftigtendatenschutz erfolgt dies insbesondere nach den allgemeinen gesetzlichen Vorschriften, die das Bundesdatenschutzgesetz enthält. Darüber hinaus leiten sich aus allgemeinen Regelungen des Gesetzes wie etwa den Vorgaben zur Datenvermeidung, Datensparsamkeit oder zur Datenlöschung eindeutige Begrenzungen der Verarbeitungsbefugnisse der Arbeitgeber ab.

Problematisch ist, dass Beschäftigte, die im Berufsleben Datenschutzverstöße ihres Arbeitgebers erkennen, ein rechtskonformes Verhalten persönlich einfordern müssen und dies ggf. über die Aufsichtsbehörden durchsetzen müssen. Vor diesem Hintergrund sind Betriebsräte gefordert, auf Basis ihrer Mitwirkungs- und Mitbestimmungsrechte einen wirksamen Beschäftigtendatenschutz sicherzustellen. Eine herausragende Bedeutung kommt ihrem Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG zu. Das Mitbestimmungsrecht ist unabhängig davon, ob Kontrollen vom Arbeitgeber gewollt sind. Bei der Ausübung dieses Mitbestimmungsrechtes müssen Betriebsräte wie Arbeitgeber darauf hinwirken, das Persönlichkeitsrecht der Beschäftigten zu schützen.

Datenschutzrechtlich geprägte Regelungsgegenstände in einschlägigen Betriebsvereinbarungen sind beispielsweise abschließende Festlegungen geplanter Verarbeitungszwecke, Darlegungspflichten zu den Rechtsgrundlagen von Verarbeitung oder Übermittlung, Festlegungen zu individuellen Einwilligungen oder Vorgaben zur Datenvermeidung und Datensparsamkeit.

INHALT

1 EINLEITUNG

Die vielfältigen Anwendungen und Entwicklungstrends der Informationstechnik (IT) sind aus dem privaten wie aus dem beruflichen Umfeld nicht mehr wegzudenken. Ihr Kennzeichen sind die inzwischen allgegenwärtigen Smartphones und Tablets. Diese kleinen Geräte stellen für eine zunehmende Zahl von Menschen eine zentrale Kommunikationsplattform dar. Sie werden längst nicht mehr nur für Telefongespräche, sondern als zentrale Informationsdrehscheibe für Versand und Empfang von individuellen Mitteilungen, für den Zugang zum Internet sowie für Aktivitäten in sozialen Netzwerken verwendet. Das bei den verschiedenartigen Anwendungen zugleich eine Fülle von personenbezogenen Daten anfällt, scheint die begeisterten Smartphone-Nutzer zumeist nicht zu stören.

Der Siegeszug dieser handlichen und schicken Geräte hängt eng mit einer Fülle kleiner Programme zusammen, die Nutzern dort als „Apps" zur Verfügung stehen und die es im Netz zu praktisch allen Themen und für alle Anwendungsfälle gibt. Das Kürzel „App" steht für das englische Wort „Application" und entspricht im Deutschen der „Anwendung". Mit Apps lassen sich vielfältige Aufgaben erledigen. Im privaten Bereich gehört hierzu die Fernsteuerung häuslicher Geräte ebenso wie der Empfang von Audio- und Videostreams oder die Überwachung schlafender Kleinkinder. Neuester Trend in der App-Welt ist die Verbindung von Smartphones mit sogenannten Fitness-Armbändern. Folge ist, dass individuelle Gesundheitsdaten nicht nur auf den eigenen Geräten, sondern auch zentral im Internet gespeichert und ausgewertet werden können.

Im beruflichen Bereich führen Smartphones, Tablets und Apps zu fast noch tiefergreifenden Veränderungen und Umwälzungen als im Privatleben. Dabei werden die gleichen Geräte genutzt wie im privaten Bereich. Dies führt dazu, dass Beschäftigte dienstliche Geräte grundsätzlich für private Internetzugriffe nutzen können, wenn die Arbeitgeber dies erlauben. Eine zunehmende Zahl von Beschäftigten macht es umgekehrt und verwendet private Geräte für dienstliche Aufgaben. Diese Form der Nutzung im beruflichen Umfeld wird unter dem Begriff „Bring Your Own Device" (BYOD)[1] diskutiert.

Den Beschäftigten, die noch mit konventionellen Personalcomputern oder Notebooks arbeiten, werden die Funktionalitäten der auf Smartphones und Tablets verwendeten Apps mittels spezieller Software zur Verfügung gestellt. Dies führt dazu, dass die verschiedenen Gerätetypen mehr und mehr „zusammenwachsen".

Einer rasanten Veränderung unterliegt derzeit auch die hinter den Geräten stehende Technik: Die für die Arbeit notwendigen Daten werden in vielen Fällen nicht mehr auf den Endgeräten der Nutzer oder auf betrieblichen Servern gespeichert, sondern irgendwo auf der Welt in sogenannten „Clouds". Wörtlich übersetzt handelt es sich hierbei um „Wolken", tatsächlich aber um Server von Dienstleistungsanbietern. Für Nutzer beinhalten Cloud-Konzepte insbesondere die Möglichkeit, von überall und mittels verschiedener Endgeräte auf die Daten zugreifen zu können.

Clouds sind inzwischen nicht nur universelle Speichermedien für Firmendaten, sondern auch eine Quelle für Software aller Art. Firmenkunden und Privatnutzern werden die verschiedensten Programme aus der Cloud im Rahmen von Abo- oder Lizenzmodellen als Software as a Service (SaaS) angeboten. Beispielsweise steht mit Windows 365 eine Cloud-Alternative zum vielgenutzten Microsoft-Office-Paket, das individuell auf jedem Endgerät installiert werden muss, zur Verfügung. Office 365 beinhaltet in Abhängigkeit von der eingekauften Nutzungslizenz zudem weitere Anwendungen wie etwa Yammer, Skype for Business oder Delve.

SaaS aus der Cloud bietet zudem den Vorteil, dass keine bestimmte Softwareversion mehr angeschafft werden muss, die schnell veraltet. Stattdessen stehen immer aktuelle und fehlerbereinigte Versionen zur Verfügung, die zudem inhaltlich ständig weiterentwickelt werden. Das macht aufwendige Neuinstallationen auf jedem Gerät entbehrlich. Für Nutzer verbindet sich diese Entwicklung allerdings mit der Notwendigkeit, ständig auf Programmänderungen „gefasst" sein zu müssen. Eine vertraute Softwareoberfläche kann sich da überraschend von heute auf morgen verändern.

Moderne IT-Anwendungen ermöglichen gerade auch unter Rückgriff auf Cloud-Computing eine umfassende Vernetzung innerhalb des Unternehmens und mit Kunden, Lieferanten und Geschäftspartnern.

WEITERFÜHRENDE LITERATUR

Greve, Silke (2016): Cloud Computing. Reihe Praxiswissen Betriebsvereinbarungen. Hans-Böckler-Stiftung (Hg.). Düsseldorf. Download: http://www.boeckler.de/5248.htm?produkt=HBS-006383

Um in diesem vernetzten Umfeld eine schnelle reibungslose Kommunikation zu ermöglichen, finden sich in einer zunehmenden Zahl von Unternehmen Software-Anwendungen aus dem Bereich der Unified Communication[2]. Diese Art der Software ermöglicht es Beschäftigten etwa, Datenbestände ge-

1 Ausführlich Brandt, in: Computer und Arbeit 10/2011, S. 8 ff.; Sinn, in: Computer und Arbeit 10/2011, S. 4 ff.

2 Wedde, in: Computer und Arbeit 4/2015, S. 4 ff.

meinsam zu verwalten und zu bearbeiten. Über eine zentrale Software-Oberfläche lassen sich darüber hinaus kurzfristig beispielsweise auch gemeinsame Arbeiten an Dokumenten organisieren oder Telefon- bzw. Videokonferenzen. Die verwendeten Softwareoberflächen ähneln vielfach denen, die von sozialen Netzwerken bekannt sind. Weiterhin können Beschäftigte auf diesen Oberflächen Informationen per Chat oder mittels Posts austauschen. Die Software ermöglicht es zudem, Arbeitsaufgaben zu verteilen und zu koordinieren sowie deren Erledigung zu überwachen. Unified Communications führt damit letztlich dazu, dass im betrieblichen Zusammenhang praktisch alles mit allem zusammenhängt.

Die Ausbreitung derartiger Programmoberflächen wird dadurch begünstigt und beschleunigt, dass dieselben Endgeräte für private wie für berufliche Aufgaben genutzt werden können. Hieraus folgen neue Anforderungen für den Datenschutz. Grundsätzlich könnten die unterschiedlichen Sphären zwar technisch abgegrenzt werden, etwa durch den Einsatz von Mobile Device Management (MDM)-Software.[3]

WEITERFÜHRENDE LITERATUR

Thannheiser, Achim (2015): Mobile Device Management - Mobile Endgeräte verwalten und mehr. Reihe Betriebs- und Dienstvereinbarungen / Kurzauswertungen. Hans-Böckler-Stiftung (Hg.). Düsseldorf. Download: http://www.boeckler.de/6299.htm?produkt=HBS-006125

In der Praxis werden einzelne Anwendungen aber oft vermischt. Dies kann in der Konsequenz dazu führen, dass Arbeitgebern auch Informationen aus dem privaten Bereich zugänglich werden.

1.1 Mehr Verhaltens- und Leistungskontrollen?

Die IT-Welt beinhaltet viele neue, faszinierende und im Arbeitsalltag hilfreiche Möglichkeiten. Dies bewerten Beschäftigte oft positiv. Mit den einzelnen Anwendungen und insbesondere mit den meisten Apps verbinden sich indes personenbezogene Aussagen, die automatisch gespeichert werden und die dazu verwendet werden können, bekannte Verhaltens- und Leistungskontrollen zu verfeinern und neue zu realisieren.

Eine Kontrolle des Verhaltens und der Leistung von Arbeitnehmern ist aus arbeits- wie aus datenschutzrechtlicher Sicht nicht grundlegend unzulässig. Die Überwachung von Beschäftigten durch Arbeitgeber kann rechtlich beispielsweise dann legitim sein, wenn es darum geht, Daten zu gewinnen, die zur Durchführung und Abwicklung von Arbeitsverhältnissen benötigt werden. Hierzu gehören beispielsweise Informationen über den Beginn und das Ende der individuellen Arbeitszeit im Rahmen von Gleitzeitregelungen oder die detaillierte Erfassung der Arbeit von Kundendienstmitarbeitern für die Erstellung von Rechnungen.

Problematischer wird es, wenn vorliegende Informationen von Arbeitgebern nicht mehr nur zur Erfüllung arbeitsrechtlich legitimer Zwecke genutzt werden, sondern mit dem Ziel, Beschäftigte weitgehend, umfassend, dauerhaft oder flächendeckend zu kontrollieren. Derartige Überwachungsmaßnahmen im Arbeitsverhältnis sind schon deshalb problematisch, weil Beschäftigte sich diesen (anders als im privaten Bereich) nicht entziehen können. Hinzu kommt, dass eine dauerhafte Überwachung das Verhalten des Einzelnen negativ beeinflusst. Dies hat insbesondere das Bundesarbeitsgericht (BAG) mehrfach festgestellt. So heißt es beispielsweise in einem Beschluss aus dem Jahr 2004:

> *„Durch die Videoüberwachung wird […] in schwerwiegender Weise in das allgemeine Persönlichkeitsrecht der Arbeitnehmer eingegriffen. Diese werden einem ständigen Überwachungsdruck ausgesetzt. Sie müssen stets damit rechnen, gerade gefilmt zu werden. Zwar sind die Videokameras sichtbar angebracht; wann sie in Betrieb sind, ist aber für Arbeitnehmer nicht erkennbar. Da der Einigungsstellenspruch Videoaufzeichnungen von 50 Stunden pro Woche auch ohne Vorliegen eines Verdachts gestattet, haben die Arbeitnehmer während ihrer gesamten Arbeitszeit davon auszugehen, dass ihre Verhaltensweisen möglicherweise gerade aufgezeichnet werden und später anhand der Aufzeichnung rekonstruiert und kontrolliert werden können. Dementsprechend müssen sie sich bei jeder ihrer Bewegungen kontrolliert fühlen. Ihre Gestik und Mimik, bewusste oder unbewusste Gebärden, der Gesichtsausdruck bei der Arbeit oder bei der Kommunikation mit Vorgesetzten und Kollegen unterliegen stets der Möglichkeit dokumentierender Beobachtung. Damit entsteht ein Druck, sich möglichst unauffällig zu benehmen, setzen sich doch die Arbeitnehmer anderenfalls der Gefahr aus, später wegen etwa abweichender Verhaltensweisen Gegenstand von Kritik, Spott oder gar Sanktionen zu werden.“*[4]

WEITERFÜHRENDE LITERATUR

Böker, Karl-Hermann (2009): Videoüberwachung. Reihe Betriebs- und Dienstvereinbarungen / Kurzauswertungen. Hans-Böckler-Stiftung (Hg.). Düsseldorf. Download: http://www.boeckler.de/6299.htm?produkt=HBS-004576

3 Ausführlich Flake, in: Computer und Arbeit 10/2014, S. 11 ff.; Steinwender, in: Computer und Arbeit 9/2013, S. 5 ff.

4 BAG vom 29.06.2004 – 1 ABR 21/03, Neue Zeitschrift für Arbeitsrecht (NZA) 2004, S. 1278 unter B II 1 der Gründe.

Weil sich umfassende oder permanente Verhaltens- und Leistungskontrollen im Arbeitsverhältnis negativ auf das verfassungsrechtlich herausragend geschützte Persönlichkeitsrecht der Arbeitnehmer auswirken, setzt die Rechtsprechung ihnen Grenzen: Eingriff und Einschränkungen des allgemeinen Persönlichkeitsrechts von Arbeitnehmern dürfen als Ergebnis einer Abwägung mit schutzwürdigen Belangen von Arbeitgebern nur ausnahmsweise gerechtfertigt sein. Ob eine zulässige Ausnahme vorliegt, ist im Rahmen einer Güterabwägung zwischen den Persönlichkeitsrechten der Beschäftigten und den schutzwürdigen Belangen der Arbeitgeber zu ermitteln. Zur Feststellung, ob Einschränkungen des Persönlichkeitsrechts im konkreten Fall zulässig sind, muss eine Verhältnismäßigkeitsprüfung durchgeführt werden. Dabei ist zu prüfen, ob Kontrollmaßnahmen geeignet sind, den erstrebten Erfolg zu erreichen.[5] Erforderlich sind bestimmte Kontrollmaßnahmen zudem nur, wenn Arbeitgebern kein anderes, gleichwirksames Mittel zur Verfügung steht, das die Persönlichkeitsrechte weniger tangiert oder einschränkt.[6]

a. Gesetzliche Grenzen

Die Grenzen für den zulässigen Umgang mit Beschäftigtendaten im Arbeitsverhältnis, die das BAG formuliert, leiten sich aus einschlägigen gesetzlichen Normen ab, die für den Umgang mit personenbezogenen Daten bestehen. Mangels spezialgesetzlicher Regelungen zum Beschäftigtendatenschutz kommt in diesem Zusammenhang insbesondere den allgemeinen Vorschriften eine besondere Bedeutung zu, die das Bundesdatenschutzgesetz (BDSG) enthält. Daneben leiten sich Regeln und Grenzen für den Beschäftigtendatenschutz aus zahlreichen weiteren allgemeinen Einzelgesetzen ab. Beispielsweise finden sich Verarbeitungsbegrenzungen, die auch für den Umgang mit Beschäftigtendaten von Bedeutung sind, verstreut in Regelungen wie etwa dem Telekommunikationsgesetz (TKG) oder dem Telemediengesetz (TMG). Hinzu kommen im arbeits- und sozialrechtlichen Bereich Vorschriften wie etwa in § 19 Gendiagnostikgesetz zum Verlangen von Arbeitgebern nach gentechnischen Untersuchungen oder in § 84 Abs. 2 Sozialgesetzbuch IX zur Ausgestaltung des betrieblichen Eingliederungsmanagements. Diese Situation wird auch durch das Inkrafttreten der neuen europäischen Datenschutz-Grundverordnung (DSGVO)[7] am 25. Mai 2018 nichts grundlegend verändert, soweit nicht als Folge dieser dann europaweit zwingend geltenden Datenschutzregelung nationale Regeln angepasst werden müssen.[8]

b. Individuelle Durchsetzung von Datenschutzrechten

Ein Grundproblem, das sich mit dem Thema „Datenschutz und Arbeitsverhältnis“ verbindet, besteht darin, dass die Beschäftigten ein gesetzeskonformes Verhalten ihres Arbeitgebers im Umgang mit ihren personenbezogenen Daten im Konfliktfall individualrechtlich selbst einfordern und durchsetzen müssen. Kommt ein Arbeitgeber etwa seinen gesetzlichen Pflichten zur Datenlöschung nicht nach, bleibt Arbeitnehmern zur Durchsetzung ihrer Löschungsrechte neben der Einschaltung des betrieblichen Datenschutzbeauftragten oder der zuständigen staatlichen Aufsichtsbehörde nur der Gang zum Arbeitsgericht. Ein solches Vorgehen beinhaltet für sie jedoch ein hohes Risiko: Die Information der staatlichen Aufsichtsbehörden über mögliche Datenschutzverstöße des Arbeitgebers bewerten Arbeitsgerichte unter bestimmten Umständen als arbeitsrechtlichen Pflichtverstoß des Arbeitnehmers, der zur Abmahnung oder Kündigung führen kann. Ein Erfolg vor dem Arbeitsgericht führt zudem in der Praxis oft dazu, dass Arbeitgeber anschließend das Arbeitsverhältnis unter anderen Vorwänden kündigen. In der Praxis läuft der bestehende gesetzliche Schutz der Beschäftigtendaten damit vielfach leer.

c. Anforderungen an Betriebsräte

Vor diesem Hintergrund sind Betriebsräte gefordert, sowohl die Einhaltung der geltenden Vorschriften für den Bereich des Beschäftigtendatenschutzes als auch den Schutz der Persönlichkeitsrechte der Beschäftigten durch aktive Wahrnehmung ihrer Mitwirkungs- und Mitbestimmungsrechte sicherzustellen.

WEITERFÜHRENDE LITERATUR

Böker, Karl-Hermann/Demuth, Ute (2012): IKT- Rahmenvereinbarungen. Reihe Betriebs- und Dienstvereinbarungen. Hans-Böckler-Stiftung (Hg.). Frankfurt am Main. Download: http://www.boeckler.de/6299.htm?produkt=HBS-005399

Ihnen ist es zwar verwehrt, individualrechtliche Ansprüche von Beschäftigten auf Datenschutz stellvertretend geltend zu machen. Sie können aber stattdessen auf Basis der gesetzlichen Möglichkeiten, die ihnen das Betriebsverfassungsgesetz (BetrVG) einräumt, vom Arbeitgeber Ausgestaltungen von IT-Systemen verlangen, die einen umfassenden Schutz der Rechte der Beschäftigten sicherstellen.

5 BAG vom 19.01.1999 – 1 AZR 499/98, NZA 1999, S. 546.
6 BAG vom 29.06.2004 – 1 ABR 21/03, NZA 2004, S. 1278.
7 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung - DSGVO), Amtsblatt der Europäischen Union vom 4.5.2016, L 119/1 ff..
8 Vgl. Wedde, in: Computer und Arbeit 3/2016, S. 12 ff.

Wie die gesetzlichen Handlungsmöglichkeiten der Betriebsräte aussehen und wie diese optimal zum Schutz der Persönlichkeitsrechte von Beschäftigten eingesetzt werden können, wird in den folgenden Kapiteln beschrieben. Im Mittelpunkt von Kapitel II steht dabei der allgemeine datenschutzrechtliche Rahmen, der für Arbeitsverhältnisse besteht. Hieran schließt sich in Kapitel III eine Beschreibung einschlägiger Mitwirkungs- und Mitbestimmungsmöglichkeiten an, die das BetrVG bezogen auf den Beschäftigtendatenschutz zur Verfügung stellt. Abgerundet wird die Darstellung durch Hinweise für die Ausgestaltung von Betriebsvereinbarungen in Kapitel IV.

2 DER RECHTLICHE RAHMEN

2.1 Handlungsmöglichkeiten

Datenschutzrecht ist ein Grundrecht. Diese Feststellung leitet sich aus dem sogenannten Volkszählungsurteil des Bundesverfassungsgerichts (BVerfG) aus dem Jahr 1983 ab. Dort heißt es im 1. Leitsatz des Gerichts:

> *„Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des GG Art 2 Abs 1 in Verbindung mit GG Art 1 Abs 1 umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."*[9]

Mit diesem Urteil hat das höchste deutsche Gericht ein Grundrecht auf informationelle Selbstbestimmung begründet, das nicht nur im Verhältnis zwischen Bürgern und Staat gilt, sondern aufgrund der Drittwirkung von Grundrechten auch für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch private Stellen einen Rahmen vorgibt.

Die Vorgaben und Feststellungen des BVerfG zum Recht auf informationelle Selbstbestimmung haben das Bundesdatenschutzgesetz (BDSG) in der heute vorliegenden Form geprägt.[10] Was bisher allerdings fehlt, ist eine geschlossene gesetzliche Regelung zum Beschäftigtendatenschutz. Ein 2011 eingebrachter Gesetzesentwurf[11] zu diesem Thema wurde von der damaligen Bundesregierung vor einer abschließenden parlamentarischen Entscheidung zurückgezogen. Auch im Angesicht der DSGVO und mit Blick auf die dort in Artikel 88 enthaltene Öffnungsklausel für den Bereich des Beschäftigtendatenschutzes gibt es derzeit keine einschlägigen gesetzgeberischen Aktivitäten. Somit bleibt abzuwarten, in welcher Form der Regelungsgehalt des aktuell geltenden § 32 BDSG in die ab Mai 2018 bestehende neue gesetzliche Situation überführt wird.

Aufgrund des Fehlens einschlägiger gesetzlicher Regelungen zum Beschäftigtendatenschutz bleibt damit nur der Rückgriff auf aktuell geltende allgemeine Datenschutzregeln, die insbesondere das BDSG enthält. In der folgenden Darstellung werden in Fußnoten zu den einschlägigen Vorschriften des BDSG die entsprechenden Regelungen der DSGVO genannt.

2.2 Beschäftigtendatenschutz nach dem BDSG

Aufgrund des Fehlens einer speziellen gesetzlichen Regelung zum Beschäftigtendatenschutz kommen die allgemeinen Regelungen zum Datenschutz zur Anwendung, die bezogen auf nicht-öffentliche Arbeitgeber sowie für Beschäftigte der Bundesverwaltung im BDSG zu finden sind. Für die bei öffentlichen Arbeitgebern aus den Bundesländern tätigen Arbeitnehmer sind die im Detail vom BDSG abweichenden Regelungen der jeweiligen Landesdatenschutzgesetze einschlägig. Diese Landesregelungen bleiben an dieser Stelle unberücksichtigt.

a. Personenbezogene Daten

Das BDSG enthält zwingende Vorgaben für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten. Dies sind nach der Definition in § 3 Abs. 1 BDSG[12] Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Von der gesetzlichen Definition werden alle Informationen erfasst, die sich direkt oder indirekt auf bestimmte Menschen beziehen lassen. Unmittelbar personenbezogen sind etwa Name, Vorname sowie deren Verwendung in einer „sprechenden E-Mail-Adresse". Zu den personenbeziehbaren Daten gehört beispielsweise das Kennzeichen des eigenen Autos, die Telefonnummer, die Personalnummer oder die Nummer des Personalausweises.

b. Verbotsgesetz mit Erlaubnisvorbehalt

Nach § 4 Abs. 1 BDSG[13] dürfen personenbezogene Daten nur erhoben, verarbeitet und genutzt werden, wenn das BDSG selbst oder eine andere Rechtsvorschrift dies erlauben oder anordnen. Das BDSG ist deshalb ein Verbotsgesetz mit Erlaubnisvorbehalt. Fehlt die geforderte gesetzliche Erlaubnisnorm, kommt als weitere Grundlage für die Er-

9 BVerfG vom 15.12.1983 – 1 BvR 209/83, Neue Juristische Wochenschrift (NJW) 1984, S. 419.
10 Zur Entwicklungsgeschichte des Gesetzes Weichert, in: Däubler/Klebe/Wedde/Weichert (2016): Bundesdatenschutzgesetz, 5. Aufl., Frankfurt (im Folgenden: DKWW), Einleitung Rn. 5 ff.
11 BT-Drs. 17/4230.
12 Vgl. Artikel 4 Ziff. 1 DSGVO
13 Vgl. Artikel 6 Abs. 1 Buchstabe b) DSGVO.

hebung, Verarbeitung und Nutzung eine persönliche Einwilligung der Betroffenen gemäß § 4a BDSG[14] in Betracht.

Sollen Daten von Beschäftigten erhoben, verarbeitet und genutzt werden, muss der Arbeitgeber darlegen, auf welcher Rechtsgrundlage dies geschieht. Einschlägige gesetzliche Erlaubnisnormen, die für den Bereich von Beschäftigungsverhältnissen relevant sind, finden sich etwa in Gesetzen aus dem Bereich des Steuerrechts oder des Sozialversicherungsrechts. Im arbeitsrechtlichen Bereich sind Erlaubnistatbestände beispielsweise enthalten im Arbeitszeitgesetz (etwa in den §§ 3 und 4 zur Erhebung von Arbeits- oder Ruhezeiten) oder im Entgeltfortzahlungsgesetz (etwa in § 4 Abs. 1 zur Höhe der Entgeltfortzahlung im Krankheitsfall).

Fehlt eine gesetzliche Erlaubnisnorm, kann eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach § 4 Abs. 1 BDSG auch durch eine „andere Rechtsvorschrift" legitimiert werden.[15] Hierzu gehören beispielsweise die normativen Teile von Tarifverträgen und Betriebs- bzw. Dienstvereinbarungen.[16]

c. Individuelle Einwilligung

Das Fehlen der nach § 4 Abs. 1 BDSG notwendigen Erlaubnisgrundlage kann durch eine Einwilligung der Personen ersetzt werden, um deren personenbezogene Daten es geht. Eine solche Einwilligung ist nach § 4a Abs. 1 BDSG[17] nur wirksam, wenn sie auf der freien Entscheidung der bzw. des Betroffenen beruht. Sie muss also freiwillig erteilt werden. In der Einwilligungserklärung ist auf den vorgesehenen Zweck der Verwendung der personenbezogenen Daten zu verweisen. Einwilligungen nach § 4a Abs. 1 BDSG müssen im Regelfall schriftlich erteilt werden. Mündliche Einwilligungen sind nur ausnahmsweise wirksam, wie etwa bei der telefonischen Sperrung einer verlorenen Kreditkarte.
Bezogen auf Beschäftigungsverhältnisse bestehen grundlegende Zweifel an der notwendigen Freiwilligkeit einer Einwilligung.[18] Die Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten lässt sich mit einer Einwilligung deshalb nur dann legitimieren, wenn die Freiwilligkeit zweifelsfrei feststeht. Dies kann etwa bei der Zustimmung zur Datenverarbeitung im Zusammenhang mit einer betrieblichen Altersversorgung der Fall sein. Bestehen Zweifel an der Freiwilligkeit, muss diese vom Arbeitgeber, der sich auf die Erklärung von Beschäftigten beruft, bewiesen werden.[19]

d. Datenvermeidung und Datensparsamkeit

Ist die Erhebung, Verarbeitung und Nutzung personenbezogener Beschäftigtendaten gemäß § 4 Abs. 1 BDSG zulässig, müssen Arbeitgeber weitere Vorgaben beachten, die das Gesetz enthält. Hierzu gehört nach § 3a BDSG[20] beispielsweise die Datenvermeidung und Datensparsamkeit. Die Vorschrift verpflichtet Arbeitgeber, nach Möglichkeit ganz auf die Verwendung personenbezogener Daten zu verzichten. Ist ein Verzicht nicht möglich, muss sich die Erhebung, Verarbeitung und Nutzung auf die unbedingt notwendigen Informationen beschränken. Zudem müssen bestehende Möglichkeiten zur Anonymisierung und Pseudonymisierung genutzt werden, sofern dies nicht unverhältnismäßig ist.

Für Betriebsräte resultiert aus dieser allgemeinen datenschutzrechtlichen Vorgabe, dass sie vom Arbeitgeber bezogen auf personenbezogene Beschäftigtendaten eine Darlegung dazu verlangen können, warum die Verwendung einzelner personenbezogener Informationen im konkreten Fall notwendig und unumgänglich ist. Wird ein entsprechender Nachweis erbracht, können Betriebsräte mit Blick auf § 3a BDSG zudem die Verarbeitung in anonymer oder pseudonymer Form verlangen. Insbesondere der Pseudonymisierung[21] kommt in zunehmend komplexer werdenden Verarbeitungsumgebungen eine besondere Bedeutung zu: Macht sie es doch Arbeitgebern einerseits möglich, notwendige Informationen auf aggregierter Ebene zu gewinnen; andererseits schützt sie die Beschäftigtendaten vor unberechtigten und umfangreichen Zugriffen.

e. Direkterhebung

Arbeitgeber sind durch die Vorgaben in den §§ 4 Abs. 2 und 28 Abs. 1 Satz 2 BDSG[22] verpflichtet, erforderliche personenbezogene Daten direkt bei ihren Beschäftigten zu erheben. Dieses Verfahren wird bezogen auf allgemeine Rahmendaten wie etwa Qualifikation, Anschriften, Bankkonten oder berufliche Aus- und Weiterbildung der Regelfall sein. Die Pflicht zur Direkterhebung beinhaltet für Beschäftigte den Vorteil, dass sie wissen, über welche Informationen ihr Arbeitgeber verfügt.

Von einer Direkterhebung kann gemäß § 4 Abs. 2 BDSG ausnahmsweise abgewichen werden, wenn eine Rechtsvorschrift die Erhebung, Verarbeitung und Nutzung von Daten vorsieht oder zwingend voraussetzt. Weiterhin ist ein Abweichen möglich, wenn die zu erfüllende Verwaltungsaufgabe oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich machen oder wenn die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde. Das Abweichen von der Direkterhebung steht allerdings unter dem gesetzlichen

14 Vgl. Artikel 7 DSGVO.
15 Vgl. Artikel 6 Abs. 1 Buchstaben b) und c) DSGVO.
16 Sassenberg/Bamberg, in: Datenschutz und Datensicherheit 2006, S. 226; Weichert, in: DKWW, § 4 Rn. 2.
17 Vgl. Artikel 7 DSGVO.
18 Grundlegend Däubler, in: DKWW, § 4a Rn 23.
19 Wedde, in: Datenschutz und Datensicherheit 2004, S. 169.
20 Vgl. Artikel 5 Abs. 1. Buchstabe b) DSGVO.
21 Vgl. Artikel 6 Abs. 4 Buchstabe e) und 25 Abs. 1 DSGVO.
22 Vgl. Artikel 5 Abs. 1, 6 Abs. 1 und 13 DSGVO.

Vorbehalt, dass überwiegende schutzwürdige Interessen der Betroffenen hierdurch nicht beeinträchtigt werden dürfen.

Erfolgt eine Speicherung von personenbezogenen Daten nicht mittels Direkterhebung und damit ohne Kenntnis der betroffenen Beschäftigten, müssen sie nach § 33 Abs. 1 BDSG[23] vom Arbeitgeber hierüber nachträglich informiert werden. Den Beschäftigten muss dabei die Art der Daten sowie die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung mitgeteilt werden. Dies bedeutet etwa, dass Bewerber von ihrem potenziellen Arbeitgeber darüber in Kenntnis gesetzt werden müssen, wenn diese ergänzend zu den vorgelegten Bewerbungsunterlagen Informationen aus dem Internet eingeholt haben.

f. Zweck und Zweckbindung

Schon bei der Erhebung müssen die Zwecke der geplanten Verarbeitung festgelegt werden. Dies folgt aus § 4 Abs. 3 Nr. 2 BDSG bzw. aus § 28 Abs. 1 Satz 2 BDSG[24]. Entsprechendes gilt, wenn die Verwendung von personenbezogenen Daten auf der Grundlage einer freiwilligen Einwilligung nach § 4a Abs. 1 BDSG erfolgt. In diesen Fällen muss in der Einwilligungserklärung gemäß Satz 2 dieser Vorschrift auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung hingewiesen werden.

Die Festlegung der genannten Zwecke bindet die weitere Verarbeitung und Nutzung. Zweckänderungen sind zwar in bestimmten Fällen möglich. Sie stehen aber unter dem Vorbehalt, dass schutzwürdige Interessen der Betroffenen hierdurch nicht unangemessen verletzt werden (vgl. etwa § 28 Abs. 2 Nr. 2 BDSG[25]). Diese Zweckfestlegung hat beispielsweise zur Folge, dass Arbeitgeber die personenbezogenen Daten eines zu Abrechnungszwecken eingeführten elektronischen Ausweissystems nicht zur Erstellung individualisierbarer Krankheitsstatistiken verwenden dürfen.

g. Löschung und Sperrung

Für die Praxis bedeutsam ist auch § 35 Abs. 2 BDSG[26]. Nach dieser Vorschrift sind personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig ist. Dies ist etwa der Fall, wenn die Zwecke, die der Verarbeitung zugrunde lagen, erfüllt wurden bzw. sich erledigt haben. Gleiches gilt, wenn in einer Betriebsvereinbarung maximale Vorhaltefristen enthalten sind. Sind diese abgelaufen, müssen die entsprechenden personenbezogenen Daten gelöscht werden. Abweichungen von diesem Grundsatz kann es geben, wenn Arbeitgeber nachweisen, dass sie über eine datenschutzrechtliche Legitimation verfügen, die die weitere Speicherung zulässt. An Stelle einer Löschung tritt dann nach § 35 Abs. 3 BDSG[27] eine Sperrung der Verarbeitung und Nutzung für andere Zwecke.

h. Datenübermittlung

Sollen Daten an andere Konzernunternehmen oder an außerhalb des Betriebs oder des Unternehmens stehende Stellen übermittelt werden, müssen seitens des Arbeitgebers die notwendigen Legitimationen für eine Datenübermittlung gemäß § 11 BDSG[28] im Rahmen eines Auftragsvertrags gegeben sein. Darüber hinaus kommt eine Funktionsübertragung in Betracht.[29]

Aufträge zwischen Arbeitgebern und Auftragnehmern außerhalb von Unternehmen müssen schriftlich vereinbart werden. Betriebsräten sind die entsprechenden Vertragswerke im Rahmen ihres allgemeinen gesetzlichen Informationsanspruchs nach § 80 Abs. 2 BetrVG vom Arbeitgeber vorzulegen. Fehlen schriftliche Vereinbarungen, muss eine Datenübermittlung an andere Stellen unterbleiben.

2.3 § 32 BDSG – Erlaubnisnorm für die Verwendung von Beschäftigtendaten

Bezogen auf Beschäftigungsverhältnisse enthält das BDSG mit § 32 eine zentrale Erlaubnisnorm für die Erhebung, Verarbeitung und Nutzung der hier erforderlichen personenbezogenen Daten. Diese Vorschrift wurde als Folge großer Datenschutzskandale vom Gesetzgeber im Jahr 2009 in das Gesetz eingefügt.[30] Die Vorschrift ist ein erster Schritt hin zu einer grundlegenden Regelung des Beschäftigtendatenschutzes.

a. Erforderlichkeit der Datenerhebung

Nach § 32 Abs. 1 Satz 1 BDSG dürfen Arbeitgeber personenbezogene Daten von Bewerbern oder Beschäftigten erheben, verarbeiten und nutzen, wenn dies für die Begründung eines Beschäftigungsverhältnisses, für dessen Durchführung oder für dessen Beendigung erforderlich ist. Die Verarbeitungsbefugnis von Arbeitgebern beschränkt sich auf solche Daten, die für die Anbahnung, Durchführung oder Beendigung des Beschäftigungsverhältnisses zwingend erforderlich sind. Dies muss der Arbeitgeber gegenüber Betriebsräten auch unter Beachtung von § 3a BDSG nachweisen. Ist der Nachweis nicht möglich, muss die Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten unterbleiben. Die Regelungen in § 32 BDSG kommen nach dem Wortlaut der Norm auf „Beschäftigte“ zur Anwen-

23 Vgl. Artikel 14 DSGVO.
24 Vgl. Artikel 5 Abs. 1 Buchstabe b) DSGVO.
25 Vgl. Artikel 6 Abs. 1 Buchstabe f) DSGVO.
26 Vgl. Artikel 17 DSGVO.
27 Vgl. Artikel 18 DSGVO.
28 Vgl. Artikel 28 DSGVO.
29 Vgl. zur Abgrenzung zwischen Auftragsdatenverarbeitung und Funktionsübertragung Wedde, in: DKWW, § 11 Rn. 14 ff.
30 BT-Drs. 16/1357; zum Gesetzgebungsverfahren Roßnagel, in: NJW 2009, S. 2716; Weichert, in: DKWW, Einleitung Rn. 68.

dung. Hierzu gehören nach der Legaldefinition in § 3 Abs. 11 BDSG neben Arbeitnehmern auch Auszubildende, Rehabilitanten, in Werkstätten für behinderte Menschen oder nach dem Jugendfreiwilligendienstegesetz Beschäftigte, „arbeitnehmerähnliche Personen", Bewerber und ehemalige Beschäftigte, Beamte, Richter und Soldaten.

Ob die gemäß § 32 Abs. 1 Satz 1 BDSG für die Erhebung, Verarbeitung und Nutzung aller Beschäftigten notwendige Erforderlichkeit gegeben ist, ist nach der Rechtsprechung auf der Grundlage einer Verhältnismäßigkeitsprüfung festzustellen.[31] Verhältnismäßig ist eine Maßnahme, wenn sie

> *„[…] geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen ist, um den angestrebten Zweck zu erreichen".*[32]

Die Erforderlichkeit setzt grundsätzlich voraus, dass eine Verwendung von personenbezogenen Daten legitimen Zielen der Arbeitgeber dient.[33] Dies schließt beispielsweise eine Verarbeitung von Gesundheitsdaten der Arbeitnehmer aus, wenn es hierfür keine explizite gesetzliche Grundlage gibt.

Im Ergebnis einer Verhältnismäßigkeitsprüfung sind die Erhebungen, Verarbeitungen und Nutzungen als geeignet zu qualifizieren, die dazu dienen, legitime Verarbeitungszwecke umzusetzen. Als erforderlich ist der Umgang mit personenbezogenen Daten in diesem Zusammenhang nur zu bewerten, wenn Arbeitgebern als Alternative zur geplanten Erhebung, Verarbeitung und Nutzung kein anderes, gleich wirksames und die Persönlichkeitsrechte weniger einschränkendes Mittel zur Verfügung steht. Angemessen ist eine Maßnahme, wenn ihr keine überwiegenden Grundrechte der hiervon Betroffenen gegenüberstehen.[34]

Mit Blick darauf, dass Arbeitgeber die Form der Erhebung, Verarbeitung und Nutzung wählen müssen, die sich mit dem geringsten Eingriff in Persönlichkeitsrechte verbindet, ist der Begriff der Erforderlichkeit eng auszulegen. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Beschäftigten ist insbesondere dann als nicht erforderlich zu qualifizieren, wenn dem Arbeitgeber „mildere" Alternativen zur Verfügung stehen. Hierzu gehört beispielsweise die Möglichkeit, personenbezogene Daten statt im Klartext in pseudonymisierter Form zu verarbeiten (§ 3a BDSG).

Nicht als erforderlich zu qualifizieren sind Abweichungen vom festgelegten Verarbeitungszweck, sofern diese nicht durch das BDSG ausdrücklich legitimiert werden. Gegen die Erforderlichkeit heimlicher Formen der Datenerhebung spricht im Regelfall der sich hiermit verbindende unzulässige Eingriff in das Persönlichkeitsrecht der Beschäftigten.

Im Regelfall nicht als erforderlich und damit unzulässig sind Datenerhebungen, Verarbeitungen und Nutzungen von Informationen, die aus dem privaten Bereich der Beschäftigten stammen. Eine Ausnahme gibt es nur für solche Daten, die etwa für die Anbahnung, Durchführung oder Beendigung von Beschäftigungsverhältnissen erforderlich sind wie etwa die private Anschrift oder eine Kontonummer für die Gehaltszahlungen.

Die Erforderlichkeit gemäß § 32 Abs. 1 Satz 1 BDSG für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Beschäftigten kann sich in den verschiedenen Verarbeitungsphasen verändern. In der Bewerbungsphase beschränkt sich die Erhebungsbefugnis von potenziellen Arbeitgebern auf solche Informationen, an deren Kenntnis er bezogen auf einen möglichen Vertragsabschluss ein berechtigtes, billigenswertes und schutzwürdiges Interesse hat.[35] Zulässig sind im Rahmen von Bewerbungsverfahren beispielsweise Datenerhebungen zur beruflichen Fähigkeit und Erfahrung, zur bisherigen Vergütung sowie ggf. zur vorhandenen Fahrerlaubnis oder zu einschlägigen Vorstrafen.[36] Unzulässig sind hingegen Fragen zum Privatleben oder zu diskriminierungsverdächtigen Tatsachen. Zu Letzteren gehören mit Blick auf § 1 Allgemeines Gleichbehandlungsgesetz (AGG) etwa Fragen nach der ethnischen Herkunft, nach Schwangerschaften oder Kindern, nach Weltanschauung oder gewerkschaftlichem Engagement. Im Regelfall ausgeschlossen sind weiterhin Fragen nach Religionszugehörigkeit oder nach sexueller Ausrichtung. Ausnahmen gelten bezüglich der Religionszugehörigkeit für bestimmte kirchliche Träger. Dies folgt aus § 9 AGG.[37]

Kommt es zum Abschluss eines Arbeitsvertrages, sind nach § 32 Abs. 1 Satz 1 BDSG Informationen erforderlich, die ein Arbeitgeber für die Durchführung des Beschäftigungsverhältnisses benötigt. Hierzu gehören beispielsweise Angaben zur Bankverbindung bzw. zur privaten Anschrift ebenso wie die aus steuerlichen Gründen notwendige Mitteilung der Religionszugehörigkeit.[38] Datenerhebungen in der Durchführungsphase des Beschäftigungsverhältnisses stehen unter dem Vorbehalt, dass nur solche Informationen erhoben, verarbeitet und genutzt werden dürfen, die zwingend erforderlich sind und für die es im Ergebnis einer Abwägung keine Alternativen gibt.

---

31 BAG vom 26.08.2008 – 1 ABR 16/07, NZA 2008, S. 1187.
32 BAG vom 29.06.2004 – 1 ABR 21/03, NZA 2004, S. 1278.
33 Forst, in: Auernhammer u. a. (Hg.) (2014): Bundesdatenschutzgesetz und Nebengesetze, 4. Aufl., Köln, § 32 Rn. 53.
34 BAG vom 26.08.2008 – 1 ABR 16/07, NZA 2008, S. 1187.
35 Vgl. zur Rechtsprechung etwa BAG vom 13.06.2002 – 2 AZR 234/01, NZA 2003, S. 265; grundlegend vom 05.12.1997 – 1 AZR 594/56, AP Nr. 2 zu § 123 BGB; vgl. auch Däubler, in: DKWW, § 32 Rn. 16.
36 Däubler, in: DKWW, § 32 Rn. 16 ff.
37 Ausführlich Wedde, in: Däubler/Bertzbach (Hg.) (2013): Allgemeines Gleichbehandlungsgesetz, 3. Aufl., Baden-Baden, § 9 Rn. 14 ff.
38 Vgl. ausführlich Däubler, in: DKWW, § 32 Rn. 73 ff.

Nach Ende des Beschäftigungsverhältnisses bestimmt sich die Befugnis des Arbeitgebers zur Verarbeitung und Nutzung vorhandener Daten auf solche Informationen, die er für die Abwicklung des Vertragsverhältnisses benötigt. Neben steuerrelevanten Informationen, die nach den einschlägigen Regelungen teilweise bis zu zehn Jahren gespeichert werden müssen, kommen hier beispielsweise Zahlungspflichten aus dem Bereich der betrieblichen Altersversorgung in Betracht. Zu beachten ist, dass gespeicherte Daten nur für die Zwecke genutzt werden dürfen, aus denen sich eine Befugnis zur weiteren Verarbeitung ableitet. Für alle anderen Zwecke sind diese Daten im Regelfall gemäß § 35 Abs. 3 BDSG zu sperren.

b. Aufdeckung von Straftaten

§ 32 Abs. 1 Satz 2 BDSG enthält einen Erlaubnistatbestand für den Sonderfall der Aufdeckung von Straftaten. Nach dieser Regelung dürfen personenbezogene Daten eines Beschäftigten zu diesem Zweck nur dann verwendet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass im Beschäftigungsverhältnis eine Straftat begangen wurde. Die Zulässigkeit der Erhebung, Verarbeitung und Nutzung steht aber auch in diesen Fällen unter dem Vorbehalt, dass der Rückgriff auf personenbezogene Daten hierfür erforderlich ist und dass schutzwürdige Interessen diesem nicht entgegenstehen. Auf die Erhebung, Verarbeitung und Nutzung muss insbesondere dann verzichtet werden, wenn Art und Ausmaß im Hinblick auf den Anlass unverhältnismäßig sind.

Der in § 32 Abs. 1 Satz 2 BDSG genannte Tatbestand stellt eine absolute Ausnahme dar. Hierauf deutet bereits die im Text der Vorschrift enthaltene Vorgabe hin, dass zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen müssen, dass eine Straftat vorliegt. Datenverarbeitungen sind in diesen Fällen nur zulässig, wenn dem Arbeitgeber keine anderen Möglichkeiten zur Aufdeckung von Straftaten im Betrieb zur Verfügung stehen. Es wird sich im Regelfall um den Verdacht auf das Vorliegen einer schweren Straftat handeln müssen.[39] Die Vorschrift legitimiert zudem keine präventiven Maßnahmen, die unabhängig von einem konkreten Verdacht getroffen werden sollen.[40] Betroffene Beschäftigte müssen über geplante Erhebungen, Verarbeitungen und Nutzungen auf der Grundlage von § 32 Abs. 1 Satz 2 BDSG so früh wie möglich informiert werden, damit sie ihre Rechte wahrnehmen können. Damit kann die Datenverarbeitung im Regelfall nicht heimlich durchgeführt werden. Ausnahmen von dieser frühzeitigen Informationspflicht des Arbeitgebers können nur dann gelten, wenn durch eine entsprechende Mitteilung die gewollte Aufklärung unmöglich gemacht wird. In diesem Fall muss die Information zum frühestmöglichen Zeitpunkt nachgeholt werden.

Neben den betroffenen Beschäftigten ist auch der zuständige Betriebsrat auf der Grundlage von § 80 Abs. 2 BetrVG vom Arbeitgeber ebenfalls so früh wie möglich zu informieren. Sollen die entsprechenden Daten elektronisch verarbeitet werden, löst dies die Mitbestimmungsrechte des Betriebsrats gemäß § 87 Abs. 1 Nr. 6 BetrVG aus.

Unter Beachtung dieser normativen Vorgaben können beispielsweise heimliche Datenerhebungen nur unter besonderen Umständen angemessen sein, beispielsweise ein mit dem Betriebsrat vereinbarter und zeitlich befristeter Kameraeinsatz zur Aufdeckung von Diebstählen in bestimmten Bereichen.

c. Beschäftigtendatenverarbeitung in nicht-automatisierten Dateien

Die vorstehenden Grundsätze gelten gemäß § 32 Abs. 2 BetrVG nicht nur für die elektronische Verarbeitung von personenbezogenen Daten, sondern auch für die Erhebung, Verarbeitung und Nutzung in anderer Form. Damit kommen die einschlägigen datenschutzrechtlichen Vorgaben und Beschränkungen etwa auch auf schriftliche Unterlagen des Arbeitgebers oder einzelner Vorgesetzter zur Anwendung. Ausgenommen bleiben allenfalls private Aufzeichnungen von Vorgesetzten oder anderen Beschäftigten, wenn diese nicht für berufliche Zwecke genutzt werden (etwa ein privates Tagebuch). Dies folgt aus § 27 Abs. 1 Satz 2 BDSG. Nach dieser Vorschrift kommt das Gesetz nicht zur Anwendung, wenn die Erhebung, Verarbeitung und Nutzung von Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. Diese Ausnahme gilt nicht, wenn entsprechende Aufzeichnungen im beruflichen Kontext verwendet werden.

3 MITWIRKUNG UND MITBESTIMMUNG

Das BetrVG ist Grundlage für die Beteiligungs- und Mitwirkungs- und Mitbestimmungsrechte von Betriebsräten und damit auch für die Regelung neuer IT-Systeme. Vergleichbare Vorschriften finden sich im Bereich des öffentlichen Dienstes für Personaldaten in den einschlägigen Personalvertretungsgesetzen.

3.1 Gesetzliche Grundlage

Bezogen auf IT-Systeme verbindet sich mit dem BetrVG das Problem, dass dieses aus dem Jahr 1972 stammende Gesetz zuletzt vor 14 Jahren im Jahr 2001 umfassend geändert wurde. Dies hat zur Folge, dass der normative Standard des BetrVG inzwischen deutlich hinter der rasant verlaufenden

39 Ähnlich Thüsing, in: NZA 2009, S. 868.
40 Ausführlich Wedde, in: DKWW, § 32 Rn. 128 ff.

technischen Entwicklung zurückgeblieben ist. Dennoch ist das BetrVG für Betriebsräte ein sinnvolles und wirksames Handwerkszeug, das insbesondere dazu genutzt werden kann, Arbeitnehmer vor ausufernden und teilweise unzulässigen Verhaltens- und Leistungskontrollen sowie vor ungesetzlichen Erhebungen, Verarbeitungen und Nutzungen ihrer personenbezogenen Daten zu schützen. Neben Informationsrechten weist das BetrVG Betriebsräten insbesondere ein starkes Mitbestimmungsrecht hinsichtlich der Regelung von technischen Einrichtungen zu, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.

3.2 Wissen ist Macht

Unter der Überschrift „Allgemeine Aufgaben" gibt § 80 Abs. 1 Nr. 1 BetrVG Betriebsräten die Aufgabe, darüber zu wachen, dass alle zugunsten von Arbeitnehmern geltenden Gesetze, Verordnungen, Tarifverträge und Betriebsvereinbarungen durchgeführt werden. Hierzu gehören auch Regelungen zum Datenschutz, wie sie insbesondere das BDSG enthält.[41] Dies versetzt Betriebsräte unabhängig davon, dass es im BetrVG kein „Mitbestimmungsrecht zum Datenschutz" gibt, in die Lage, die Einhaltung der datenschutzrechtlichen Vorgaben zu überwachen.

Wichtig ist in diesem Zusammenhang die Regelung in § 80 Abs. 2 BetrVG. Dieser zufolge sind Betriebsräte vom Arbeitgeber rechtzeitig und umfassend über all das zu unterrichten, was sie zur Durchführung ihrer Aufgaben benötigen. In diesem Rahmen können sie beispielsweise Aufklärung darüber verlangen, welche Rechtsgrundlagen es für die von ihm durchgeführte Erhebung, Verarbeitung und Nutzung personenbezogener Daten gibt.

WEITERFÜHRENDE LITERATUR

Auswertungen und Gestaltungshilfen zu EDV - IT - Datenschutz - Kommunikation sind unter http://www.boeckler.de/594.htm#bvdoku32572 zu finden.

Im Rahmen des Informationsanspruchs haben Betriebsräte gemäß § 80 Abs. 2 Satz 2 BetrVG einen Anspruch auf Zurverfügungstellung der erforderlichen Unterlagen. Dieser beinhaltet beispielsweise im IT-Bereich auch technische Spezifikationen zu den einzelnen Systemen.

Die Auswertung technischer Unterlagen und Details setzt fachliche Kompetenzen voraus, über die nicht jedes Betriebsratsmitglied verfügt. Um dennoch die gesetzlichen Aufgaben wahrnehmen zu können, sieht § 80 Abs. 2 Satz 3 BetrVG eine Beratung durch sachkundige Arbeitnehmer vor, die den Betriebsrat als Auskunftsperson unterstützen. Darüber hinaus kann der Betriebsrat gemäß § 80 Abs. 3 BetrVG zu seiner Unterstützung nach näherer Vereinbarung mit dem Arbeitgeber externe Sachverständige hinzuziehen. Dies versetzt das Gremium grundsätzlich in die Lage, sich selbst ein Bild von der technischen Situation und den hieraus folgenden datenschutzrechtlichen Notwendigkeiten oder Problemen zu verschaffen. Hinzu kommen eigene Schulungs- und Weiterbildungsansprüche, die den Betriebsratsmitgliedern bezogen auf erforderliches Wissen gemäß § 37 Abs. 6 BetrVG zustehen.

Über den gesetzlichen Rahmen für die Informationsgewinnung hinaus können in Betriebsvereinbarungen weitere Informationsmöglichkeiten zu einzelnen IT-Systemen vereinbart werden. Zwar gibt es hierfür keinen gesetzlichen Anspruch, sehr wohl aber die Möglichkeit, mit dem Arbeitgeber im Rahmen von Verhandlungen Absprachen zu treffen.

WEITERFÜHRENDE LITERATUR

Böker, Karl-Hermann/Demuth, Ute (2012): IKT- Rahmenvereinbarungen. Reihe Betriebs- und Dienstvereinbarungen. Hans-Böckler-Stiftung (Hg.). Frankfurt am Main. Download: http://www.boeckler.de/6299.

Dies alles versetzt Betriebsräte in die Lage, sich ein klares Bild von der Realität der Datenverarbeitung im Betrieb zu verschaffen sowie davon, welche personenbezogenen Daten hierbei erhoben, verarbeitet und genutzt und zu welchen Zwecken sie verwendet werden dürfen. Diese Informationsbasis schafft die Voraussetzungen dafür, IT-Systeme auf der Grundlage bestehender Mitbestimmungsrechte aktiv auszugestalten.

3.3 Gestaltung durch Mitbestimmung

Das BetrVG enthält kein Mitbestimmungsrecht, das explizit auf die Ausgestaltung und Sicherstellung des Datenschutzes und damit auf die Sicherung der Persönlichkeitsrechte der Beschäftigten ausgerichtet ist. Dies bedeutet nicht, dass es keine Mitbestimmungsrechte gibt. Einschlägige Möglichkeiten, die mittelbar auch den Bereich Datenschutzrecht beinhalten, leiten sich vielmehr aus vorhandenen gesetzlichen Tatbeständen ab.

a. Schutz vor Verhaltens- und Leistungskontrollen

Eine herausragende Bedeutung kommt in diesem Zusammenhang dem Mitbestimmungsrecht nach

41 Wedde, in: Computer und Arbeit 4/2015, S. 4 ff.

§ 87 Abs. 1 Nr. 6 BetrVG zu.[42] Dieses greift, wenn im Betrieb technische Einrichtungen eingeführt oder angewendet werden sollen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Es ist weit gefasst und unabhängig davon, ob Arbeitgeber technische Einrichtungen zur Verhaltens- und Leistungskontrolle verwenden wollen. Ausgelöst wird es bereits dadurch, dass eine technische Einrichtung eine Überwachung der Arbeitnehmer grundsätzlich ermöglicht, unabhängig davon, ob diese vom Arbeitgeber auch tatsächlich beabsichtigt ist.[43]

Auf der Grundlage dieses Mitbestimmungsrechts können Betriebsräte zwar die Einführung und den anschließenden Betrieb von IT-Systemen nicht verhindern; sie können aber vom Arbeitgeber Regelungen verlangen, die Verhaltens- und Leistungskontrollen entweder ausschließen oder auf das zwingend notwendige Maß reduzieren. Für die Regelung der Kontrolldichte und -tiefe leitet sich aus den einschlägigen Vorschriften des BDSG ein wichtiger Maßstab ab. So folgt aus § 4 Abs. 1 BDSG zulasten des Arbeitgebers die Notwendigkeit, die gesetzlichen Grundlagen zu benennen, auf deren Basis die Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten stattfindet. Darüber hinaus resultiert aus dem in § 3a BDSG normierten Gebot der Datenvermeidung und -sparsamkeit eine Verpflichtung des Arbeitgebers, dem Betriebsrat bezüglich jedes personenbezogenen Datums darzulegen, warum dies zwingend benötigt wird bzw. warum keine Verarbeitung in pseudonymisierter oder anonymer Form möglich ist.

Datenschutzrechtliche Grundsätze sind für die Ausfüllung des Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 6 BetrVG schon allein deshalb beachtlich, weil die Vermeidung von Verhaltens- und Leistungskontrollen ebenso wie der Schutz der Daten nach dem BDSG auf die Wahrung der Persönlichkeitsrechte von Arbeitnehmern zielt. Dies wird durch die Regelung in § 75 Abs. 2 BetrVG unterstrichen, nach der Arbeitgeber und Betriebsrat die freie Entfaltung der Persönlichkeit der im Betrieb Beschäftigten zu schützen und zu fördern haben. Hieraus folgt: Betriebsräte müssen entsprechende Regelungen mit dem Ziel treffen, mögliche oder notwendige Kontrollen auf das erforderliche Minimum zu reduzieren.

Welche Regelungsspielräume damit bestehen, lässt sich am Beispiel konventioneller Taschenkontrollen illustrieren: Mit Blick auf die Vorgaben des § 75 Abs. 2 BetrVG müssen Vereinbarungen zu diesem Thema vorsehen, dass mit den Kontrollen verbundene Eingriffe in die Persönlichkeitsrechte der Beschäftigten so gering wie möglich sind. Hierzu gehört es beispielsweise, die zu kontrollierenden Personen nach dem Zufallsprinzip auszuwählen, die Zugriffe auf das zwingend Notwendige zu begrenzen (etwa auf bloße Sichtkontrollen), die Kontrolle von mitgeführten Medikamenten auszuschließen sowie ggf. Alternativen zur Verfügung zu stellen: zum Beispiel Aufbewahrungsschränke vor dem betrieblichen Bereich, die Taschenkontrollen im Ergebnis überflüssig machen.

b. Arbeits- und Gesundheitsschutz

Neben den Mitbestimmungsrechten aus § 87 Abs. 1 Nr. 6 BetrVG leiten sich ergänzende Regelungsmöglichkeiten beispielsweise aus § 87 Abs. 1 Nr. 7 BetrVG ab. Nach dieser Vorschrift besteht ein Mitbestimmungsrecht, wenn Regelungen zur Verhütung von Arbeitsunfällen und Berufskrankheiten sowie zum Gesundheitsschutz im Rahmen gesetzlicher Vorschriften oder Unfallverhütungsvorschriften Arbeitgebern Gestaltungsspielräume einräumen.

WEITERFÜHRENDE LITERATUR

Auswertungen und Gestaltungshilfen zu Arbeits- und Gesundheitsschutz sind unter http://www.boeckler.de/594.htm#bvdoku32574 zu finden.

Ein solcher Gestaltungsspielraum folgt beispielsweise aus § 4 Abs. 1 Bildschirmarbeitsverordnung. Nach dieser Vorschrift haben Arbeitgeber geeignete Maßnahmen zu treffen, damit Bildschirmarbeitsplätze den Anforderungen des Anhangs zu dieser Verordnung sowie sonstigen Rechtsvorschriften entsprechen. Nach Nr. 22 dieses Anhangs darf ohne Wissen des Benutzers keine Vorrichtung zur qualitativen oder quantitativen Kontrolle verwendet werden. Hieraus folgt, dass Arbeitnehmer grundsätzlich über alle technischen Einrichtungen informiert werden müssen, mit denen sich Verhaltens- und Leistungskontrollen durchführen lassen. Dies schließt den Einsatz und den Betrieb verdeckter Kontrolleinrichtungen ohne Kenntnis der Beschäftigten und der zuständigen Betriebsräte aus.

c. Ordnung im Betrieb

Macht der Arbeitgeber allgemeine Vorgaben zum Umgang mit IT-Systemen, ist schließlich das Mitbestimmungsrecht gemäß § 87 Abs. 1 Nr. 1 BetrVG einschlägig, das bezüglich der Ordnung im Betrieb und des Verhaltens der Arbeitnehmer im Betrieb besteht. Auf dieser Grundlage können Betriebsräte ein Mitbestimmungsrecht bezüglich allgemeiner Anweisungen zum Umgang mit IT-Systemen einschließlich der Festlegung des Inhalts von sogenannten Netiquetten reklamieren.

42 Vgl. hierzu ausführlich die Kommentierung zu § 87 Abs. 1 Nr. 6 BetrVG in Däubler/Kittner/Klebe/Wedde (Hg.) (2016), BetrVG – Betriebsverfassungsgesetz, 15. Aufl., Frankfurt (im Folgenden: DKKW), § 77 Rn. 33 ff.

43 Vgl. ausführlich BAG vom 06.12.1983 – 1 ABR 43/81, NJW 1984, 1476.

d. Wirksamkeitsvoraussetzung des Mitbestimmungsverfahrens

Dem Mitbestimmungsrecht nach § 87 Abs. 1 BetrVG kommt eine besondere Bedeutung zu. Denn eine Einigung in mitbestimmungsrechtlichen Fragen ist die Wirksamkeitsvoraussetzung für die Durchführung einer vom Arbeitgeber geplanten Maßnahme. Für den Fall einer Nichteinigung in Verhandlungen sieht § 87 Abs. 2 BetrVG ausführlich den Weg zur Einigungsstelle vor. Führt ein Arbeitgeber vor Abschluss des Mitbestimmungsverfahrens eine Maßnahme einseitig durch, indem er etwa ein IT-System ohne die geforderte Betriebsvereinbarung startet, kann der Betriebsrat diese ggf. durch eine einstweilige Verfügung stoppen.

Betriebsräten steht damit insbesondere in Form von § 87 Abs. 1 Nr. 6 BetrVG auf Basis der weiteren einschlägigen Mitbestimmungstatbestände ein Instrumentarium zur Verfügung, mit dem sie vom Arbeitgeber eine Ausgestaltung von IT-Systemen fordern können, die das allgemeine Persönlichkeitsrecht und das sich hieraus ableitende Recht auf informationelle Selbstbestimmung gewährleistet.

e. Weitere Mitbestimmungsrechte

Darüber hinaus gibt es weitere einschlägige Mitbestimmungstatbestände wie etwa das nach § 94 BetrVG. Nach Abs. 1 dieser Vorschrift bedürfen Personalfragebogen der Zustimmung des Betriebsrats. Der Begriff Personalfragebogen ist in diesem Zusammenhang weit zu fassen. Neben Fragebogen, die im Zusammenhang mit Bewerbungen verwendet werden, unterfallen dem Mitbestimmungsrecht beispielsweise auch sogenannte Checklisten, die standardisiert ausgefüllt werden.[44] Kommt eine Verständigung zwischen Arbeitgeber und Betriebsrat über den Inhalt von Personalfragebogen nicht zustande, entscheidet die Einigungsstelle.

4 UMSETZUNG

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Beschäftigten durch Arbeitgeber darf nur im Rahmen des gesetzlich Zulässigen erfolgen. Fehlt eine gesetzliche Erlaubnisnorm, kann eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch eine Betriebsvereinbarung legitimiert werden. Maßstab für einschlägige Vereinbarungen und Regelungen, die Betriebsräte fordern und durchsetzen können, sind nach den aus § 75 Abs. 2 BetrVG folgenden Grundsätzen insbesondere auch die Prinzipien und Grenzen, die es zur Sicherung des Persönlichkeitsschutzes insbesondere im BDSG gibt.

4.1 Darlegungspflichten des Arbeitgebers

Mit Blick auf den Verbotscharakter des BDSG, der in § 4 Abs. 1 des Gesetzes zum Ausdruck kommt, muss der Arbeitgeber vor der Erhebung von Daten gegenüber dem Betriebsrat die gesetzliche Grundlage benennen, auf deren Basis er eine Verwendung von personenbezogenen Daten durchführen will. Die entsprechenden Darlegungen sind eine Bringschuld der Arbeitgeber.

4.2 Übermittlungen

Bedeutsam ist in diesem Zusammenhang, dass die nach § 4 Abs. 1 notwendige Zulässigkeit sich nicht nur auf die Erhebung bezieht, sondern auch auf anschließende Verarbeitungs- und Nutzungsprozesse. Dies schließt beabsichtigte Übermittlungen von Daten an Auftragnehmer oder Dritte ein. Auch bezogen auf derartige Datenübermittlungen muss der Arbeitgeber gegenüber dem Betriebsrat die notwendigen rechtlichen Grundlagen darlegen. Handelt es sich um Auftragsdatenverarbeitung, schließt dies die Vorlage eines entsprechenden Vertrages gemäß § 11 BDSG ein. Soll eine Funktionsübertragung erfolgen, muss der Arbeitgeber deren Rechtsgrundlage darlegen. Bedeutsam ist in diesem Zusammenhang, dass die Beauftragung anderer Stellen nicht zum Wegfall von bestehenden Mitbestimmungsrechten führt. Der Arbeitgeber muss ggf. in der vertraglichen Gestaltung der Auftragsbeziehungen zu anderen Stellen die Vorgaben berücksichtigen und sicherstellen, die sich aus abgeschlossenen Betriebsvereinbarungen ableiten.

4.3 Persönlichkeitsrechte

Soweit Betriebsräte durch Betriebsvereinbarungen eine eigenständige Verarbeitungsgrundlage für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten begründen wollen, müssen sie § 75 Abs. 2 BetrVG beachten. Hieraus folgt, dass sie nur Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten per Betriebsvereinbarung zulassen dürfen, die nicht unangemessen in die Persönlichkeitsrechte der Beschäftigten eingreifen. Dies grenzt für den Abschluss von Betriebsvereinbarungen den Rahmen des Zulässigen ein. Auch Einigungsstellen können im Streitfall per Spruch keine Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten zulassen, die gegen die Vorgabe in § 75 Abs. 2 BetrVG verstoßen. Dies schützt Betriebsräte davor, vom Arbeitgeber bezogen auf den Abschluss von Regelungen unangemessen unter Druck gesetzt zu werden.

4.4 Einwilligung

Gesetzliche Mitwirkungs- und Mitwirkungsrechte werden nicht dadurch außer Kraft gesetzt, dass Be-

44 Vgl. Fitting (2016): Betriebsverfassungsgesetz, 28. Aufl., München, § 94 Rn. 6 ff.

schäftigte mittels Einwilligung gemäß § 4a BDSG bestimmte Erhebungen, Verarbeitungen oder Nutzungen zugelassen haben. Schließen Betriebsräte Betriebsvereinbarungen zu IT-Systemen ab, sind individuelle Einwilligungen unwirksam, wenn die hierdurch möglichen Erhebungen, Verarbeitungen oder Nutzungen die datenschutzrechtliche Situation der Beschäftigten gegenüber den kollektivrechtlichen Regelungen verschlechtert. Dies folgt aus dem Grundsatz, dass kollektivrechtliche Schutzregelungen durch individualrechtliche Absprachen nicht verschlechtert, sondern nur verbessert werden können.[45]

4.5 Einschränkungen

Betriebsräte können bezogen auf IT-Systeme, die ihren Mitbestimmungsrechten unterfallen, verlangen, dass die Arbeitgeber das Gebot der Datenvermeidung und Datensparsamkeit in § 3a BDSG einhalten. Dies führt praktisch dazu, dass Arbeitgeber für alle personenbezogenen Daten detailliert darlegen müssen, warum ein Verzicht auf die Verwendung oder eine Verarbeitung in pseudonymisierter oder anonymisierter Form nicht möglich ist. Kann er die Erforderlichkeit der Erhebung, Verarbeitung oder Nutzung unter Verzicht auf eine Pseudonymisierung oder Anonymisierung nicht nachweisen, spricht dies gegen eine Berechtigung zur Verwendung der Daten.

4.6 Zwecke

Weitere Verarbeitungsbeschränkungen, die Betriebsräte bei der Gestaltung von Betriebsvereinbarungen beachten müssen, folgen nach den §§ 4 Abs. 3 und 28 Abs. 1 Satz 2 BDSG aus der Notwendigkeit, die Zwecke der Verarbeitung und Nutzung bereits bei der Erhebung von Daten festzulegen. Vor diesem Hintergrund können sie per Betriebsvereinbarung Erhebungen, Verarbeitungen oder Nutzungen festlegen, die sich ausschließlich an bestimmten Zwecken orientieren. So kann beispielsweise für ein Zugangskontrollsystem festgeschrieben werden, dass die anfallenden Daten ausschließlich für die Feststellung der Arbeitszeit verwendet werden. Gleichzeitig kann ausgeschlossen werden, dass hieraus etwa Erkenntnisse zur Krankheitsdauer oder zum Krankenstand abgeleitet werden.

Die gesetzlichen Vorgaben zur Zweckbestimmung geben Betriebsräten, die mittels einer Betriebsvereinbarung eine Rechtsgrundlage für die Datenerhebung, Verarbeitung und Nutzung schaffen wollen, einen hilfreichen Gestaltungsspielraum. Kann der Arbeitgeber nicht darlegen, auf welcher Rechtsgrundlage er Daten erheben, verarbeiten und nutzen will oder macht er keine Aussagen dazu, warum ein Verzicht bzw. eine Pseudonymisierung oder Anonymisierung nicht möglich ist, kann ein Betriebsrat mit Blick auf die einschlägigen datenschutzrechtlichen Vorgaben seine Zustimmung zu den IT-Systemen verweigern, mit denen entsprechende Datenverarbeitungen erfolgen sollen.

4.7 Einführung und Änderung von IT-Systemen

Aus Sicht von Betriebsräten ist es bedeutsam, dass sich die Mitbestimmung gemäß § 87 Abs. 1 Nr. 6 BetrVG immer auf bestimmte IT-Systeme bezieht. Das heißt: Jede Ersteinführung eines neuen bzw. jede Veränderung eines bestehenden IT-Systems löst das Mitbestimmungsrecht erneut aus. Dies mag für Arbeitgeber unbefriedigend sein, stellt aber aus Sicht von Betriebsräten sicher, dass die Rechte der von ihnen vertretenen Beschäftigten gewahrt werden. Vor diesem Hintergrund sollten Betriebsräte darauf Wert legen, sich ihr weit gefasstes Mitbestimmungsrecht nicht durch Regelungen in Betriebsvereinbarungen einschränken zu lassen, die Arbeitgebern weitgehende „automatische“ Änderungsbefugnisse zugestehen. Sie müssen sich die Möglichkeit erhalten, ihre uneingeschränkten Mitbestimmungsrechte einzufordern, wenn sich die Möglichkeiten für Verhaltens- und Leistungskontrollen als Folge von Veränderungen der Systeme ändern. Dies stellt besonders bezogen auf neue Formen von Software aus dem Bereich „Software as a Service“ für Betriebsräte zukünftig eine neue Herausforderung dar. Lösbar ist diese über prozessorientierte Betriebsvereinbarungen, die Haltepunkte bzw. die Möglichkeit der „Rückholbarkeit“ beinhalten.

„Automatisierte“ Änderungsbefugnisse können darüber hinaus für die Fehlerbehebung bzw. für eine notwendige Systempflege vereinbart werden, solange sichergestellt ist, dass hieraus keine neuen Funktionalitäten folgen.

4.8 Gestaltungsspielräume

Bezüglich der inhaltlichen Ausgestaltung von Betriebsvereinbarungen sind Betriebsräte schon mit Blick auf § 75 Abs. 2 BetrVG nicht völlig frei. Bei der Formulierung von Regelungen müssen vielmehr neben den Vorgaben des BDSG auch andere Regelungen Berücksichtigung und Beachtung finden, die darauf abzielen, das Persönlichkeitsrecht der Beschäftigten zu schützen und zu wahren. Neben den schon angesprochenen Regelungen in § 3a BDSG zur Datenvermeidung und Datensparsamkeit sowie zur Zweckbindung in § 4 Abs. 3 Nr. 2 BDSG bzw. in § 28 Abs. 1 Satz 2 BDSG sind in diesem Zusammenhang weitere Aspekte zu beachten wie etwa die Vorgaben zur Datenlöschung in § 35 Abs. 2 BDSG, notwendige Maßnahmen aus dem Bereich des technisch-organisatorischen Da-

45 Vgl. Berg, in DKKW, § 77 Rn. 33 ff.

tenschutzes gemäß § 9 BDSG, Informationspflichten des Arbeitgebers gemäß § 33 Abs. 1 BDSG sowie die formalen Anforderungen an die Auftragsvergabe gemäß § 11 BDSG. Im Ergebnis führen diese Vorgaben dazu, dass die Grundtatbestände des BDSG strukturell Eingang in abgeschlossene Betriebsvereinbarungen finden müssen, wenn sich Arbeitgeber und Betriebsräte nicht dem Risiko aussetzen wollen, gegen die grundlegende Vorgabe des § 75 Abs. 2 BetrVG zu verstoßen und damit die Unwirksamkeit einer Betriebsvereinbarung als Erlaubnisnorm im Sinne von § 4 Abs. 1 BetrVG riskieren wollen.

Um die Rechte der Beschäftigten zu wahren und zu sichern, können Betriebsräte in einschlägigen Betriebsvereinbarungen zur Umsetzung der Vorgaben des BDSG sowie zur Sicherung ihrer eigenen Kontrollmöglichkeiten ergänzende Regelungen verlangen. Hierzu gehört mit Blick auf das allgemeine Kontrollrecht des Betriebsrats nach § 80 Abs. 1 Nr. 1 BetrVG beispielsweise die Möglichkeit für Betriebsräte, jederzeit den gesamten Verarbeitungsprozess kontrollieren zu können. Im Zeitalter moderner IT beinhaltet dies ein „elektronisches Zugangsrecht" zu den Systemen des Arbeitgebers sowie der von diesem beauftragten Stellen. Zwar verfügen Betriebsräte vermutlich nicht über das erforderliche Know-how, um Kontrollen in technischen Bereichen durchzuführen; doch sollte in Betriebsvereinbarungen verankert werden, dass es Audit-Verfahren gibt bzw. dass Betriebsräte den fehlenden Sachverstand durch Einbindung externer Experten ersetzen können. In jedem Fall lassen sich interne Audit-Maßnahmen mit notwendigen Kontrollmaßnahmen externer Sachverständiger kombinieren.

ÜBER DIE SAMMLUNG VON BETRIEBSVEREINBARUNGEN

Die Hans-Böckler-Stiftung verfügt über die bundesweit einzige bedeutsame Sammlung betrieblicher Vereinbarungen, die zwischen Unternehmensleitungen und Belegschaftsvertretungen abgeschlossen werden. Derzeit enthält unsere Datenbank etwa 16.000 Vereinbarungen zu ausgewählten betrieblichen Gestaltungsfeldern.

Unsere breite Materialgrundlage erlaubt Analysen zu betrieblichen Gestaltungspolitiken und ermöglicht Aussagen zu Trendentwicklungen der Arbeitsbeziehungen in deutschen Betrieben. Regelmäßig werten wir betriebliche Vereinbarungen in einzelnen Gebieten aus. Leitende Fragen dieser Analysen sind: Wie haben die Akteure die wichtigsten Aspekte geregelt? Welche Anregungen geben die Vereinbarungen für die Praxis? Wie ändern sich Prozeduren und Instrumente der Mitbestimmung? Existieren ungelöste Probleme und offene Fragen? Die Analysen betrieblicher Vereinbarungen zeigen, welche Regelungsweisen und -verfahren in Betrieben bestehen. Die Auswertungen verfolgen dabei nicht das Ziel, Vereinbarungen zu bewerten, denn die Hintergründe und Strukturen in den Betrieben und Verwaltungen sind uns nicht bekannt. Ziel ist es, betriebliche Regelungspraxis abzubilden, Trends aufzuzeigen und Gestaltungshinweise zu geben.

Bei Auswertungen und Zitaten aus Vereinbarungen wird streng auf Anonymität geachtet. Die Kodierung am Ende eines Zitats bezeichnet den Standort der Vereinbarung in unserem Archiv und das Jahr des Abschlusses. Zum Originaltext der Vereinbarungen haben nur Mitarbeiterinnen und Mitarbeiter des Archivs und Autorinnen und Autoren Zugang.

Zusätzlich zu diesen Auswertungen werden vielfältige anonymisierte Auszüge aus den Vereinbarungen in der Online-Datenbank im Internetauftritt der Hans-Böckler-Stiftung zusammengestellt. Damit bieten wir anschauliche Einblicke in die Regelungspraxis, um eigene Vorgehensweisen und Formulierungen anzuregen. Darüber hinaus gehen wir in betrieblichen Fallstudien gezielt Fragen nach, wie die abgeschlossenen Vereinbarungen umgesetzt werden und wie die getroffenen Regelungen in der Praxis wirken.

Das Internetangebot ist unmittelbar zu erreichen unter www.boeckler.de/betriebsvereinbarungen

Anfragen und Rückmeldungen richten Sie bitte an betriebsvereinbarung@boeckler.de

IMPRESSUM

Ausgabe
Beschäftigtendatenschutz:
Rechtlicher Rahmen und
Handlungsmöglichkeiten für
Betriebsräte
ISSN 2366-0449

Autor
Prof. Dr. Peter Wedde
Professor für Arbeitsrecht und Recht
der Informationsgesellschaft
an der Frankfurt University
of Applied Sciences

Redaktion und Kontakt
Dr. Manuela Maschke
Hans-Böckler-Stiftung
manuela-maschke@boeckler.de
www.boeckler.de/betriebsvereinbarungen

Produktion
Setzkasten GmbH, Düsseldorf
Düsseldorf, Juni 2016