Innovationen im neuen Datenschutzrecht?

Stichtag 25. Mai 2018 DSGVO und neues BDSG treten gleichzeitig in Kraft. Ihr genauer Inhalt kann nicht in einem einzigen CuA-Beitrag dargestellt werden; die „workload“ wäre zu groß.[1] Im Folgenden soll es daher insbesondere um Dinge gehen, die neu sind im neuen Recht. Vielleicht ergeben sich ja zusätzliche Möglichkeiten für die betriebliche Interessenvertretung...

von **WOLFGANG DÄUBLER**

Zunächst zum Gewohnten: Auch nach der DSGVO gilt weiter das, was die Juristen „Verbot mit Erlaubnisvorbehalt“ nennen. Jede Datenverarbeitung – von der Erhebung über die Nutzung bis zur Löschung – bedarf einer Rechtsgrundlage. Fehlt diese, handelt es sich um einen rechtswidrigen Vorgang, für den nunmehr erhebliche Sanktionen vorgesehen sind.

Beispiel: Der Gruppenleiter findet es vernünftig, wenn er sich auf seinem privaten PC eine Datei mit dem schönen Titel „Menschliche Beobachtungen“ anlegt. Dort vermerkt er nicht nur Fehltage einzelner Gruppenmitglieder, sondern auch Beobachtungen über ihr Verhalten („Der A hat am 8.10. schon wieder gepennt“). Für eine solche Privatinitiative gibt es keine Rechtsgrundlage.

Was als Rechtsgrundlage in Betracht kommt, bestimmt sich nach Art. 6 DSGVO. Soweit Beschäftigte betroffen sind, gilt § 26 Abs. 1 BDSG: Er ist aufgrund der Öffnungsklausel in Art. 88 DSGVO erlassen worden und orientiert sich am bisherigen § 32 Abs. 1 BDSG-alt. Auch die übrigen Bestimmungen des BDSG-neu stützen sich auf solche Ermächtigungen oder füllen Lücken der DSGVO. Wer die Rechtslage erkennen will, muss beide gemeinsam betrachten.

Vertrag

Häufigste Rechtsgrundlage ist ein Vertrag, dessen Durchführung die Verarbeitung von Daten erfordert. Die Personalabteilung muss ersichtlich zur Abwicklung des Arbeitsverhältnisses über bestimmte Angaben verfügen – über wie viele ist damit nicht gesagt, das bestimmt sich nach dem Notwendigen. Gegen Betriebsausweise ist nichts einzuwenden, doch ist darauf zu

[1] Zu verweisen ist deshalb auf Däubler, Gläserne Belegschaften, 7. Aufl., Frankfurt/Main (Bund-Verlag) 2017, wo die neue Rechtslage einschließlich des BDSG umfassend dargestellt ist. Allein die DSGVO ist erläutert in den Kommentaren von Auernhammer, Ehmann/Selmayr, Gola, Kühling/Buchner und Paal/Pauly, alle 2017. Zur DSGVO s. auch Däubler, CuA 3/2016, S. 13 ff. und Weichert, CuA 3/2017, S. 8 ff.

achten, welche Daten dort festgehalten sind und bei welchen Gelegenheiten von ihnen Gebrauch gemacht wird.

Unterstellt, der Betriebsausweis kann in der Kantine als Zahlungsmittel verwendet werden; was man ausgegeben hat, wird am Ende des Monats vom Gehalt abgezogen. Das ist praktisch, aber es lässt Einblicke in die Ess- und Trinkgewohnheiten zu. Wer immer nur vegane Gerichte isst, ist für den (interessanten) Aufenthalt in Argentinien nicht unbedingt geeignet, weil das Rindersteak dort zum „Normalstandard" gehört. Auch könnte der Arbeitgeber mit Hilfe der Kantinendaten ermitteln, ob bestimmte Personen regelmäßig kurz vor oder kurz nach dem Betriebsratsvorsitzenden bezahlt haben; so könnte man zumindest „erraten", wer zum Freundeskreis zählt.

Datenschutzkonforme Technik

Gegen zu viele Daten und Datenverknüpfungen hilft der in Art. 25 Abs. 1 DSGVO niedergelegte Grundsatz des „Datenschutzes durch Technikgestaltung", häufig mit dem englischen Ausdruck „Privacy by design" bezeichnet. Die Technik wird von vorne herein so eingerichtet, dass bestimmte Daten gar nicht anfallen.

Im Kantinenfall kann man Karten einführen, die man am Automaten gegen Bargeld auflädt. Sie enthalten keinerlei personenbezogene Daten und werden als Zahlungsmittel verwendet.

Bisher hat man sich darüber viel zu wenige Gedanken gemacht. Das sollte sich nunmehr ändern. Die „Datenminimierung" (wie man auch sagt) ist in Art. 5 Abs. 1 Buchstabe c DSGVO ausdrücklich festgelegt. § 26 Abs. 5 BDSG-neu bestimmt zusätzlich, es seien „geeignete Maßnahmen" zu ergreifen, um sicherzustellen, dass u. a. dieser Grundsatz eingehalten wird. Für einen klugen Unternehmer empfiehlt es sich, bei der Auswahl von Geräten den „datenschutzfreundlichen" den Vorzug zu geben. Fehlt im Einzelfall die Klugheit oder das Problembewusstsein, kann der Betriebsrat ein wenig nachhelfen.

Gibt es auf dem Markt keine solchen Geräte, kommt „Plan B" zur Anwendung: Art. 25 Abs. 2 DSGVO spricht von „datenschutzfreundlichen Voreinstellungen", auf Englisch „privacy by default" genannt. Das bedeutet: das Gerät kann zwar außerordentlich viel erfassen, bestimmte seiner Merkmale werden aber von vorne herein nicht aktiviert.

Der Standort des Handys lässt sich zwar an sich feststellen, doch wird ausgeschlossen, dass von dieser technischen Möglichkeit Gebrauch gemacht wird.

Auch das ist nicht nur ein Appell, sondern eine bindende Verpflichtung. Auf die Sanktionen, die bei einer Verletzung drohen, ist noch zurückzukommen.

Einwilligung

Neben Verträgen ist die Einwilligung der betroffenen Person die wichtigste Basis für die Datenverarbeitung. Ein Verbraucher ist beispielsweise damit einverstanden, regelmäßig Werbung der Firma X zu bekommen. Nach Art. 6 Abs. 1 Buchstabe a DSGVO muss sie sich auf „einen oder mehrere bestimmte Zwecke" beziehen. Eine Pauschaleinwilligung ist deshalb von vorne herein wirkungslos.

Die Erklärung: „Facebook darf mit meinen Daten machen, was es will" ist rechtlich ohne Bedeutung.

Weiter muss die Einwilligung „freiwillig" sein – das wird schon aus ihrer Definition in Art. 4 Nr. 11 DSGVO deutlich. Daran fehlt es, wenn ein Vertragsschluss davon abhängig gemacht wird, dass auch solche Daten preisgegeben werden, die für den Abschluss und die Durchführung des Vertrages gar nicht erforderlich sind. Man spricht insoweit von einem „Koppelungsverbot", das sich in Art. 7 Abs. 4 DSGVO findet.

Bei der Einstellung soll ein Amazon-Beschäftigter unterschreiben, er sei damit einverstanden, jederzeit Werbemails aus der „Amazon-Familie" zu erhalten. Unzulässig, weil für die Durchführung des Arbeitsvertrags nicht erforderlich.

Wie steht es mit der Freiwilligkeit in sozialen Abhängigkeitsverhältnissen oder genauer: immer dann, wenn der Einzelne auf den Vertragsabschluss angewiesen ist? Die Berufsunfähigkeitsversicherung soll nach den Allgemeinen Geschäftsbedingungen nur zustande kommen, wenn der Versicherte für die Zukunft alle Ärzte von der Schweigepflicht entbindet, die Aussagen über seinen Gesundheitszustand machen können. Hier musste erst das Bundesverfassungsgericht für Klarheit sorgen und die Klausel für unwirksam erklären.[2] Eine so weitgehende Preisgabe von sehr sensiblen Daten war für die Zwecke des Vertrages nicht erforderlich.

Erteilt der Arbeitnehmer seine Einwilligung, in einem Werbefilm des Arbeitgebers abgebildet zu werden, so muss man die typische Juristen-Antwort geben: „Es kommt darauf an". Machen einige mit, andere nicht, ohne dass ihnen dies irgendjemand übel nimmt, so ist die Freiwilligkeit gegeben.[3] Wird umgekehrt von der Personalabteilung gesagt: „Wer da nicht mitmacht, darf nicht mit besonderem Entgegenkommen der Firma

[2] BVerfG 23.10.2006 – 1 BvR 2027/02, JZ 2007, 576; BVerfG 17.7.2013 – 1 BvR 3167/08 – RDV 2014, 34 = ZD 2014, 84.
[3] So im Fall BAG Urteil v. 11.12.2014 – 8 AZR 1010/13, NZA 2015, 604.

rechnen, wenn er mal ein Anliegen hat“, wäre die Freiwilligkeit zu verneinen. Dasselbe gilt, wenn das nicht gesagt wird, der Einzelne aber mit entsprechenden Reaktionen rechnet. § 26 Abs. 2 BDSG n. F. gibt einige zusätzliche Anhaltspunkte, wann mit Freiwilligkeit zu rechnen ist. Einzelheiten sind an anderer Stelle ausgeführt.[4]

Erfüllung rechtlicher Pflichten

Art. 6 Abs. 1 Buchstabe c DSGVO hält es weiter für gerechtfertigt, wenn Daten in Erfüllung rechtlicher Pflichten in bestimmter Weise verarbeitet werden. Es ist daher weiter zulässig, Daten an die Sozialversicherungsträger oder an das Finanzamt zu übermitteln, soweit dies für die Abführung von Sozialbeiträgen und von Lohnsteuer erforderlich ist. Auch die Informationspflicht des Arbeitgebers gegenüber dem Betriebsrat nach § 80 Abs. 2 BetrVG ist hier einzuordnen. Insoweit öffnet sich die DSGVO dem nationalen Recht.

Kein Verstoß gegen Treu und Glauben

Macht der Verantwortliche von einer Möglichkeit Gebrauch, die in Art. 6 Abs. 1 DSGVO oder in § 26 Abs. 1 BDSG-neu genannt ist, so muss er den Grundsätzen des Art. 5 DSGVO Rechnung tragen. Außer der schon genannten „Datenminimierung“ gehört dazu beispielsweise der Grundsatz, dass Daten nicht unter Verstoß gegen Treu und Glauben erhoben werden dürfen. Ein solcher Verstoß liegt etwa bei heimlicher Erhebung vor – sieht man einmal von den seltenen Fällen ab, dass gegen einen Beschäftigten der durch Tatsachen begründete Verdacht besteht, er habe im Betrieb eine strafbare Handlung begangen, der nur durch heimliche Observation ausgeräumt oder bestätigt werden kann.[5]

Der Arbeitgeber hatte ohne Wissen des Arbeitnehmers einen sog. Keylogger eingesetzt, der sämtliche Tastatureingaben kontrollierte und regelmäßig Screenshots fertigte. Das BAG erklärte dies schon nach geltendem Recht für unzulässig[6] – in Zukunft könnte es sich dabei auf das Verbot der Datenerhebung gegen Treu und Glauben (Art. 5 Abs. 1 Buchst. a DSGVO in Verbindung mit § 26 Abs. 5 BDSG) stützen.

Datentransparenz

Weiter muss nach Art. 5 Abs. 1 Buchstabe a DSGVO die Transparenz gewahrt sein. Das bedeutet, dass der Betroffene wissen muss, was mit seinen Daten geschieht. Nach Art. 12 Abs. 1 DSGVO muss er in „präziser, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ informiert werden. Was dies konkret – auch für

[4] Däubler, Gläserne Belegschaften, § 4 IV 1 (Rn. 150 ff.).
[5] In diesen Fällen greift § 26 Abs. 1 Satz 2 BDSG-neu ein.
[6] BAG Urteil v. 27.7.2017 – 2 AZR 681/16 - Pressemitteilung

Betriebsvereinbarungen – bedeutet, ist noch nicht voll ausgelotet. Ein der Praxis entnommenes Beispiel vermag dies zu verdeutlichen.

Eine US-Firma bietet dem Arbeitgeber ein Software-Modul an, das Personalentscheidungen erleichtern soll. Es beruht auf der Auswertung einer riesigen Datenmenge und nennt beispielsweise Indizien, wann sich ein Beschäftigter mit Veränderungsabsichten trägt. Bemerkenswert ist, dass dort auch der „Erfahrungssatz" enthalten ist, wer fünf Jahre lang nicht befördert wurde, habe kein Entwicklungspotential mehr; der Arbeitgeber sei deshalb gut beraten, sich von ihm zu trennen. Eine solche „Empfehlung" darf nach Art. 22 DSGVO nicht einfach automatisch nachvollzogen werden; vielmehr muss immer noch ein menschlicher Entscheidungsträger dazwischen geschaltet werden. Nur: Dieser muss dann behaupten, dass „die Maschine" unrecht habe und der Fall des Arbeitnehmers ganz anders liege. Das setzt die Bereitschaft zu eigener Argumentation voraus, die auf Widerspruch stoßen kann. Ist es da nicht viel weniger riskant, einfach das „Urteil" des Systems zu übernehmen?

Hier stellt sich die Frage, ob der Rückgriff auf „Big Data" – Erkenntnisse noch mit dem Transparenzprinzip vereinbar ist. Bisher hat sie – soweit ich sehe – keine Rolle gespielt, aber unter dem neuen Recht wird es anders sein. Big Data hat in der Personalabteilung nichts zu suchen – nur wenn man sich von vorne herein auf diesen Grundsatz stützt, hat man eine Chance, dass er auch von den Gerichten anerkannt wird.

Dokumentationspflichten

Der Verantwortliche muss dokumentieren, welche Daten er zu welchem Zweck verarbeitet. Dies ergibt sich aus Art. 5 Abs. 2, für Unternehmen mit 250 und mehr Beschäftigten aber auch aus Art. 30 DSGVO, der den Verantwortlichen ähnlich wie bisher § 4g Abs. 2 BDSG zur Erstellung eines Dateiverzeichnisses verpflichtet. Dort muss für jede Datei vermerkt sein, zu welchen Zwecke eine Verarbeitung erfolgt. In ähnlicher Weise verlangt Art. 24 Abs. 1 DSGVO (ohne Ausklammerung der kleineren Unternehmen) Maßnahmen, die sicherstellen und „den Nachweis erbringen" sollen, dass die Verarbeitung in Übereinstimmung mit der DSGVO erfolgte. Fehlt die Dokumentation, kann dies beträchtliche Folgen haben.

Im Unternehmen X gibt es für die Beschäftigten Ausweise, die den Zugang zum Betriebsgelände ermöglichen und mit deren Hilfe gleichzeitig die Kommens- und Gehenszeiten festgehalten werden. Letzteres ist wegen der Gleitzeit notwendig. Dem A wird vorgeworfen, während der Kernarbeitszeit häufig nicht da gewesen zu sein. Er macht geltend, bei der Benutzung der Ausweise sei es ausschließlich um die Zugangskontrolle gegangen. Kann X nicht beweisen, dass mit der Datenerfassung auch die Arbeitszeit kontrolliert werden sollte – es ist gar kein Zweck oder nur „Zugangskontrolle" dokumentiert – so ist A fein heraus: X kann nicht beweisen, in legaler Weise Kommens- und Gehenszeiten erhoben zu haben, und deshalb dürfen die Computeraufzeichnungen auch nicht gegen A verwendet werden.

Datenschutz-Folgenabschätzung

Neu im Datenschutzrecht ist die in Art. 35 DSGVO verbindlich festgelegte Datenschutz-Folgenabschätzung. Sie soll Risiken der Datenverarbeitung herausarbeiten und dazu anleiten, diese zu minimieren oder auszuschließen. Wann sie notwendig ist, wird in Art. 35 Abs. 1 DSGVO nur relativ allgemein umschrieben.[7] Es müsse sich – so heißt es - voraussichtlich ein „hohes Risiko" für die Rechte und Freiheiten natürlicher Personen ergeben. Dieses könne sich insbesondere aus der Verwendung neuer Technologien sowie durch die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung ergeben. Dies wird wiederum in Art. 35 Abs. 3 DSGVO beispielhaft konkretisiert. Genannt wird der Fall einer umfangreichen Verarbeitung sensitiver Daten im Sinne des Art. 9 DSGVO, was beispielsweise im Krankenhaus oder bei Sicherheitsbehörden der Fall ist. Weiter wird die systematische und umfangreiche Überwachung öffentlich zugänglicher Bereiche genannt. Schließlich geht es um die „systematische und umfassende" Bewertung persönlicher Aspekte von Menschen, die sich auf automatisierte Verarbeitung einschließlich des Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient.

Als „Profiling" definiert Art. 4 Nr. 4 DSGVO „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Personen zu analysieren oder vorherzusagen." Nach einem solchen Profiling weiß der Große Bruder fast alles und kann sogar das Verhalten seiner „Untertanen" voraussagen. Dies ist nicht etwa verboten, sondern in Art. 22 DSGVO nur davon abhängig gemacht, dass ein menschlicher Entscheider eingeschaltet wird. Eine betriebliche Interessenvertretung wird alles unternehmen müssen, um ein solches Profiling zu verhindern.

Vieles spricht dafür, die Personalverwaltung als einen Bereich mit hohen Risiken anzusehen und eine Datenschutz-Folgenabschätzung durchzuführen. Ihre Durchführung und ihr Ergebnis ist dem Betriebsrat nach § 80 Abs. 2 BetrVG als betriebliche Angelegenheit zur Kenntnis zu bringen. Er kann darauf hinwirken, dass die dort vorgesehenen Maßnahmen auch wirklich ergriffen werden. Dies klingt höchst harmlos – doch wenn die Aufsichtsbehörde von Defiziten erfährt, kann das weitreichende Folgen haben.

[7] Hierzu und zum Folgenden Kiesche CuA 2/2017 S. 31, 32

Schadensersatz bei Datenschutzverstößen

Bisher spielt der Schadensersatz im Datenschutzrecht kaum eine Rolle. Ein nachweisbarer (!) materieller Schaden entsteht in aller Regel nicht, wenn Daten in unbefugte Hände gelangen. Ein Ausgleich für immaterielle Schäden ist außerhalb des öffentlichen Dienstes nur geschuldet, wenn eine „schwere" Persönlichkeitsrechtsverletzung vorliegt. Diese wurde von der Rechtsprechung verneint, wenn die bei der Bestellung einer Bahncard angefallenen Daten gegen den ausdrücklichen Willen des Betroffenen an ein US-Unternehmen übermittelt wurden.[8] Wird ein ausgeschiedener Mitarbeiter zu Werbezwecken weiter als „dazugehörig" bezeichnet, so bekommt er zwar einen Ersatz, doch fiel dieser mit 660 Euro recht bescheiden aus.[9] Hauptanwendungsfall waren bislang unerlaubte Videoaufnahmen über eine längere Zeit hinweg. Dabei schwankte die Höhe des Schadensersatzes von Fall zu Fall. So hat etwa das ArbG Iserlohn die »Rekordsumme« von 25.000 Euro zugesprochen,[10] während sich das LAG Rheinland-Pfalz in einem ebenfalls gravierenden Fall von Überwachung mit 650 Euro begnügte.[11]

Art. 82 DSGVO schafft hier neue Maßstäbe. Zum einen setzt die Haftung für immaterielle Schäden keine „schwere" Persönlichkeitsverletzung mehr voraus. Vielmehr reicht ein einfacher Verstoß gegen Datenschutzrecht. Dies könnte dazu führen, dass die bisherigen Sätze bei den „einfachen" Verstößen zugrunde gelegt werden, während man bei den gravierenden Fällen zu sehr viel höheren Beträgen kommt. Zum zweiten reicht für die Haftung auf Schadensersatz, dass ein Verstoß gegen die DSGVO oder das sie ergänzende nationale Recht[12] vorliegt; Verschulden wird nicht vorausgesetzt. Der Verantwortliche kann nach Art. 82 DSGVO lediglich den Nachweis führen, dass er „in keinerlei Hinsicht" für den Umstand verantwortlich war, durch den der Schaden eingetreten ist. Es kommt also nicht auf das Verschulden an, sondern darauf, ob er keinerlei Einfluss auf das schädigende Geschehen hatte. Dies ist bei vorsätzlichen Eingriffen Dritter denkbar, nicht aber dann, wenn ein Angestellter einen Fehler machte oder bewusst seine Pflichten verletzte.

---

[8] AmtsG Kassel 3.11.1998 – 424 C 1260/98, CR 1999, 749 = DSB Heft 1/2000 S. 16 = DuD 1999, 599.

[9] LG Düsseldorf 10.4.2013 – 2a O 235/12, RDV 2013, 318

[10] ArbG Iserlohn 4.6.2008 – 3 Ca 2636/07, juris

[11] Urteil v. 23.5.2013 – 2 Sa 540/12, ZD 2014, 41. Beide Entscheidungen auch bei Schulze/Schreck AiB 4/2014 S. 50.

[12] Däubler, Gläserne Belegschaften, § 12 X 2 (Rn. 625g)

In einem Chat-Forum wird aus der Personalakte des A zitiert und außerdem erwähnt, dort befinde sich ein ärztliches Zeugnis der Psychiatrischen Klinik X. Wie die Information dorthin gekommen ist, lässt sich nicht klären. Haftung des Arbeitgebers auf Schadensersatz gegeben, da er nicht ausschließen kann, dass einer seiner Beschäftigten dem anonymen Chatter die Information gegeben hat. Anders dann, wenn ausschließlich ein Hacker am Werk war und dies trotz ausreichender Cybersecurity nicht zu verhindern war.

Aufsichtsbehörde und Sanktionen

Die Aufsichtsbehörde für den Datenschutz ist durch die DSGVO aufgewertet worden. Dies zeigt schon der beeindruckende Katalog ihrer Aufgaben nach Art. 57 DSGVO, aber auch die Tatsache, dass sie nach Art. 52 Abs. 4 DSGVO mit den nötigen personellen, technischen und finanziellen Ressourcen ausgestattet werden muss. Sie hat zahlreiche Untersuchungs- und Abhilfebefugnisse, wobei das letztere harmloser klingt als es ist: Die Abhilfe kann nach Art. 58 Abs. 2 DSGVO auch darin bestehen, dass eine Datenverarbeitung vorübergehend oder auf Dauer verboten wird.

Dies kann insbesondere gegenüber Unternehmen von Bedeutung sein, die keine Niederlassung in der EU haben, aber der DSGVO nach ihrem Art. 3 Abs. 2 deshalb unterstehen, weil sie – in der Regel über das Internet – den in der EU befindlichen Menschen Waren oder Dienstleistungen anbieten oder weil sie, etwa im Wege des webtracking, ihr Verhalten beobachten. Zwar müssen diese Unternehmen nach Art. 27 DSGVO einen Vertreter in der EU bestellen, doch bleibt es gleichwohl problematisch, ihnen bei Verstößen ein Bußgeld aufzuerlegen und dieses beizutreiben. Hier hilft ein Verbot, die bisherigen Aktivitäten fortzusetzen, wenn das EU-Datenschutzrecht nicht beachtet wird.

Viel mehr Aufmerksamkeit hat die Befugnis der Aufsichtsbehörden nach Art. 83 DSGVO erfahren, bei Verstößen gegen zahlreiche Bestimmungen der Verordnung Bußgelder zu verhängen. Diese können bis zu 20 Mio. Euro oder 4 % des weltweit erzielten Umsatzes betragen, sofern dieser Betrag der höhere ist. Auf zahlreichen Direktionsetagen hat dies Furcht und Schrecken verbreitet. Natürlich würde es gegen das Verhältnismäßigkeitsprinzip verstoßen, würde die Weitergabe einer Personalakte an einen Unbefugten mit 5 Mio. Euro Bußgeld belegt, doch lässt sich nicht abschätzen, in welcher Weise die Behörden von ihren Befugnissen Gebrauch machen werden. Dies stärkt faktisch die Position aller Datenschützer einschließlich des Betriebsrats: Ein umfassender Datenschutz vermindert das Risiko des Arbeitgebers, schlimmen Sanktionen ausgesetzt zu sein. Vorschlägen des Betriebsrats zu folgen, kann so im wohlverstandenen Interesse des Unternehmens liegen.