Arbeitsrecht im Betrieb

SONDERAUSGABE
August 2018
D 3591

EXTRA

AiB | FACHZEITSCHRIFT FÜR DEN BETRIEBSRAT

NEUER DATENSCHUTZ

So können Betriebsräte die Weichen stellen

dtb – Datenschutz- und Technologieberatung

BUND VERLAG

Eva-Maria Stoppkotte
Redaktion Arbeitsrecht im Betrieb

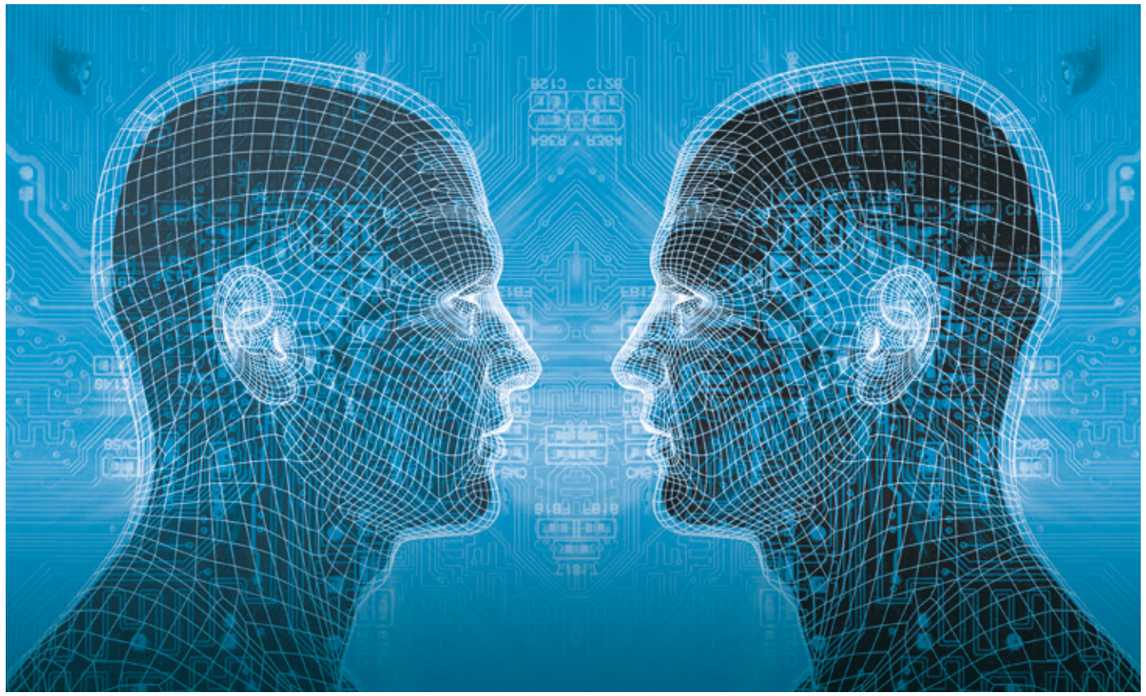
Matthias Wilke
Datenschutz- und Technologieberatung (dtb), Kassel

Mattias Ruchhöft
Technologieberater und Fachautor beim Bund-Verlag

Faires Spiel

Die DSGVO ist »ein ganz dummes Eigentor«, meint der US-Investor Peter Thiel. Sie sei ein Eingeständnis, dass Europa in der Internet-Industrie verloren habe. Das ist diskussionswürdig, denn die DSGVO zielt darauf ab, die Menschenrechte in einer digitalen Welt zu schützen. Sie wurde geschaffen, weil häufig mit unseren Daten hinter unserem Rücken Schindluder getrieben wurde. Ein Beispiel dazu: Wenn ich auf dem Bahnportal eine Fahrkarte buche und anschließend über ein Hotelportal ein Zimmer, wird dieses teurer angeboten, da die Cookies die Verknüpfung dieser Daten ermöglicht. Da wurden höchstpersönliche Daten weitergegeben und zur Währung, ohne dass ich als Datengeber darüber informiert wurde. Das geht so nicht mehr! Jetzt muss fair gespielt werden und dazu können Betriebs- und Personalräte mit ihren Überwachungs- und Mitbestimmungsrechten gehörig beitragen. Dennoch sind Datenschutz und neue Technologien vereinbar, zumal sich die elementaren Grundlagen des Datenschutzes hier in Deutschland nicht geändert haben. Wenn ich personenbezogene Daten zu einem legitimen Zweck verarbeite und dies dem Datengeber dokumentiere, darf ich das auch nach dem 25.5.2018 machen.

Viel Spaß bei der Lektüre wünschen



NEUER DATENSCHUTZ

Jetzt die Weichen stellen

Im Beschäftigungsverhältnis fallen viele personenbezogene Daten an. Auch diese sind durch die neuen Regelungen unter stärkeren Schutz gestellt. Ein erhöhtes Engagement von Betriebs- und Personalräten für den Datenschutz lohnt sich.

AiB extra August | 2018

INHALTSVERZEICHNIS

RUBRIKEN

Der neue Beschäftigtendatenschutz

DATENSCHUTZRECHT *§ 26 BDSG 2018 regelt ab sofort den Beschäftigtendatenschutz. Damit ist es jetzt für Interessenvertretungen das »Grundgesetz des Beschäftigtendatenschutzes«. Nun sind die Betriebsparteien gefordert: Sie müssen die Bestimmungen in konkrete Vereinbarungen überführen.*

VON **MATTHIAS WILKE**

AiB extra August|2018 Der neue Beschäftigtendatenschutz MATTHIAS WILKE

Seit dem 25.5.2018 gibt es ein neues Datenschutzrecht. Die Verordnung (EU) 2016/679 (nachfolgend DSGVO) gilt ab dem Stichtag unmittelbar. Gleichzeitig tritt das BDSG 2018 in Kraft und ergänzt die DSGVO in wichtigen Fragen, für die es in der DSGVO eine Öffnungsklausel gibt, so zum Beispiel Art. 88 DSGVO für den Datenschutz am Arbeitsplatz. Es stellt sich die Frage, welche Konsequenzen und Änderungen im Beschäftigtendatenschutz von der DSGVO und dem BDSG 2018 zu erwarten sind. Es bleibt zudem abzuwarten, wie die Bundesländer ihre Datenschutz- und Krankenhausgesetze der DSGVO anpassen. Richtig wären kurze, einheitliche Gesetze, die das Nötige regeln. Es sollten keine unterschiedlichen gesetzlichen Auslegungen der DSGVO in den Bundesländern geben.

Bewertung des BDSG 2018

Das BDSG 2018 ist differenziert zu bewerten. Der Gesetzgeber hat es in der letzten Legislaturperiode geschafft, das BDSG in der alten Fassung den Vorgaben der DSGVO anzupassen. Ergebnis ist ein neues BDSG, das am 25.5.2018 in Kraft getreten ist. Allerdings ist das BDSG 2018 deshalb so komplex, weil der Gesetzgeber neben der Anpassung an die DSGVO ab § 45 in Teil 3 des Gesetzes in weiteren 40 Paragrafen die Justiz- und Polizeirichtlinie (Datenschutz-Richtlinie für Polizei und Strafjustiz – EU-Richtlinie 2016/680) umgesetzt hat. Von daher sind Aufbau und Inhalte des BDSG 2018 für Rechtsanwender wie zum Beispiel Betriebsparteien recht schwierig nachzuvollziehen.

Zum Verhältnis von DSGVO und BDSG 2018

DSGVO und BDSG 2018 sind ab 25.5.2018 nebeneinander anzuwenden. Das BDSG 2018 ergänzt nicht nur die DSGVO aufgrund von Öffnungsklauseln. Es weicht teilweise – wohl unzulässig – von ihr ab, so beispielsweise bei der Videoüberwachung in § 4 BDSG 2018. Die DSGVO steht in der Normenhierarchie über dem BDSG 2018 und ist vorrangig anzuwenden.

Es bleibt unklar, ob das BDSG 2018 in einigen Bestimmungen der DSGVO als unmittelbar geltendes Recht widerspricht und deshalb diese Bestimmungen nicht angewendet werden dürfen. Der Gesetzgeber hat im Gesetzgebungsprozess des BDSG 2018 zuletzt auf

DARUM GEHT ES

1. Seit dem 25.5.2018 gilt ein neues Datenschutzrecht. Gleichzeitig tritt das BDSG 2018 in Kraft und ergänzt die DSGVO in wichtigen Fragen.

2. Aufgrund der Öffnungsklausel in Art. 88 DSGVO gibt es jetzt § 26 BDSG 2018 als neues »Grundgesetz des Beschäftigtendatenschutzes«.

3. Trotz Kritik von Datenschützern sind die Neuerungen klar und verständlich und regeln den Beschäftigtendatenschutz ganzheitlich.

Am 14.4.2016 hat das Europäische Parlament die DSGVO verabschiedet. Die DSGVO gilt verbindlich für alle Mitgliedstaaten ab dem 25.5.2018.

berechtigte Kritik reagiert und offensichtliche Verstöße gerade bei der Regelung der Betroffenenrechte (§§ 32–37 BDSG 2018) korrigiert. Für den Grundrechtsschutz auf europäischer Ebene ist der EuGH zuständig. Es ist zu erwarten, dass er seine Rechtsprechung zum Recht auf Datenschutz und damit zum Beschäftigtendatenschutz in den nächsten Jahren fortführen wird. Klagen zum BDSG 2018 oder zur Umsetzung und Auslegung der DSGVO in Deutschland werden kommen, weil noch viele Rechtsfragen ungelöst sind und erst gerichtlich entschieden werden müssen.

Beschäftigtendatenschutz auf europäischer und nationaler Ebene

Obwohl es wünschenswert wäre, ist nicht davon auszugehen, dass auf europäischer Ebene die EU-Kommission in den nächsten Jahren eine Verordnung oder eine Richtlinie zum Beschäftigtendatenschutz durchsetzen will oder kann. Der deutsche Gesetzgeber wird keinen Versuch starten, ein Gesetz zum Beschäftigtendatenschutz erneut durchzusetzen. Ein solches Gesetz wird offenkundig in absehbarer Zeit nicht kommen. Ein Versuch der Bundesregierung in 2013 scheiterte auf ganzer Linie und die letzte Fassung des geplanten Gesetzes hätte den Beschäftigten massiv geschadet. Interessenvertretungen werden in den nächsten Jahren die DSGVO und § 26 BDSG 2018 anwenden und umsetzen müssen. Dabei können sie auf die Rechtsprechung des Bundesarbeitsgerichts zu § 32 BDSG a.F. seit 2013 setzen.[1]

Von daher ist Art. 88 DSGVO, der die Öffnungsklausel zum Beschäftigtendatenschutz für den nationalen Gesetzgeber darstellt, zumindest für die nächsten Jahre für den nationalen Beschäftigtendatenschutz von größter Bedeutung. Aufgrund der Öffnungsklausel in Art. 88 DSGVO gibt es jetzt § 26 BDSG 2018 als neues »Grundgesetz des Beschäftigtendatenschutzes«.

§ 26 BDSG 2018 regelt jetzt den Beschäftigtendatenschutz

§ 26 BDSG 2018 regelt die »Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses« mit insgesamt acht Absätzen. Der Gesetzgeber führt damit § 32 BDSG a.F. fort, mit dem der Beschäftigtendatenschutz in 2009 erstmals geregelt wurde. § 32 BDSG a.F. konnte sich in der Praxis trotz anfänglicher Kritik von Arbeitsrechtlern durchsetzen. Viele grundsätzliche Bestimmungen der DSGVO bleiben unberührt, so zu den Begriffen (Art. 4 DSGVO), den Datenschutzgrundsätzen (Art. 5 Abs. 1 a – f DSGVO), der Rechtmäßigkeit (Art. 6 Abs. 1 DSGVO), des erforderlichen Datenschutz-Managements und der Nachweisbarkeit der Umsetzung (Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO). In wesentlichen Punkten des Beschäftigtendatenschutzes ist durch § 26 BDSG 2018 alles beim Alten geblieben. Der bisherige § 32 BDSG a.F. wird weitgehend fortgeführt.[2] Die Vorschriften des § 32 in Verbindung mit § 28 Abs. 6–8 BDSG a.F. sind in § 26 BDSG 2018 durch Klarstellungen und Ergänzungen präzisiert worden.

Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

Nachfolgend sollen die Regelungen des BDSG 2018 kurz dargestellt werden.

▸ Zwecke der Datenverarbeitung

Für die »einfachen« personenbezogenen Daten wird § 32 Abs. 1 Satz 1 BDSG a.F. übernommen. Neu ist der Rechtfertigungsgrund der Erfüllung einer gesetzlichen oder kollektivrechtlichen Pflicht. Dieser ist für Betriebsräte besonders wichtig, wenn sie erforderliche Beschäftigtendaten für ihre Aufgaben nach dem BetrVG verarbeiten müssen:

»*Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.*«

▸ Sensible personenbezogene Daten

Die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten auch im Beschäftigungskontext wird in § 22, § 26 Abs. 3 Satz 1 BDSG 2018 geregelt.[3] Zu den besonders zu schützenden Daten gehören

- Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,
- Daten, die genetischer, biometrischer Art sind und die Identifizierung eines Beschäftigten ermöglichen,
- Daten, die die Gesundheit des Beschäftigten betreffen und
- Daten, die Aussagen zum Sexualleben sowie zur sexuellen Orientierung enthalten.[4]

▸ Rechte der Betriebs-/Personalräte

Die Rechte der Beschäftigtenvertretungen bleiben nach § 26 Abs. 6 BDSG 2018 weiterhin wie in § 32 Abs. 3 BDSG a.F. unberührt. Der Gesetzgeber hat jedoch Fragen, die sich bei der Verarbeitung und Nutzung von Beschäftigtendaten durch die Interessenvertretung stellen, leider offengelassen und nicht geregelt.[5]

▸ Kollektivvereinbarungen haben ein enormes Potenzial

Die bislang auch in der Rechtsprechung anerkannte Befugnis der Betriebsparteien, Kollektivvereinbarungen abzuschließen, die den Datenschutz im Beschäftigungskontext regeln, wird neben Art. 88 Abs. 2 DSGVO und ErwGr 155 jetzt in § 26 Abs. 4 BDSG 2018 bestätigt. Die DSGVO und das BDSG 2018 lassen die Verarbeitung von Beschäftigtendaten durch Kollektivvereinbarungen (Betriebs-/Dienstvereinbarungen und Tarifverträge) als Rechtfertigungsgrund zu. Sie sind nach Dr. Stefan Brink ein zunehmend wichtiger Baustein des Beschäftigtendatenschutzes, der jetzt EU-weit angewendet werden kann.[6]

Eine Betriebs-/Dienstvereinbarung kann damit, wie bisher, nach § 4 Abs. 1 BDSG a.F. als »andere Rechtsvorschrift« die Verarbeitung von Beschäftigtendaten erlauben. Es gibt in der DSGVO keine Übergangsregelung für »Alt-Betriebsvereinbarungen«. In der betrieblichen Praxis werden Betriebs- und Dienstvereinbarungen (Einzel- und Gesamtbetriebsvereinbarungen) aktuell den Standards der DSGVO angepasst. Durch die Regelung in § 26 Abs. 4 BDSG 2018 können die Alt-Betriebsvereinbarungen zum Datenschutz fortgelten. Kollektivvereinbarungen dürfen nicht hinter den Anforderungen der DSGVO (Art. 88 Abs. 1

1 Siehe hierzu auch den Aufsatz von Brink im Heft.

2 Siehe BR-Drs. 110/17 v. 2.2017, 96.
3 Siehe hierzu den Beitrag von Buchner/Sperlich im Heft.
4 Düwell/Brink, Beschäftigtendatenschutz nach der Umsetzung der Datenschutz-Grundverordnung – Viele Änderungen und wenig Neues, NZA 2017, 1083 f. (auch abgedruckt in NZA-Sonderausgabe Arbeitnehmerdatenschutz März 2018, 15).
5 Siehe hierzu den Beitrag von Köppen im Heft.
6 Brink, Einleitung NZA-Sonderausgabe Arbeitnehmerdatenschutz, März 2018, 8.

und 2 DSGVO) zurückfallen. Sie müssen vor allem nach Art. 88 Abs. 2 DSGVO angemessene und besondere Maßnahmen zur Wahrung der Rechte der betroffenen Beschäftigten umfassen. Hierzu gehören etwa besondere Aufklärungs- und Sensibilisierungsmaßnahmen im Betrieb, regelmäßige Auskünfte über die Ergebnisse der Kontrollmaßnahmen oder Informationen zu den Möglichkeiten moderner Datenverarbeitung im Rahmen einer Mitarbeiterversammlung.

Die Betriebsparteien sollten vorrangig Maßnahmen zur Erhöhung der Transparenz der Datenverarbeitungen vorsehen und über die Betroffenenrechte der Beschäftigten (Art. 12–17 DSGVO) klar und verständlich informieren. Hinreichend klare Zwecke der Verarbeitung von Beschäftigtendaten sind festzulegen. Maßnahmen zur Sicherung der Zweckbindung im Beschäftigungskontext sind einzubeziehen. Der nationale Gesetzgeber gibt konkrete Maßnahmen zum Schutze von besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO in § 22 Abs. 2 BDSG 2018 vor.

- Betriebsvereinbarungen der neuen Rechtslage anpassen?

Über die Notwendigkeit und den Umfang der erforderlichen Änderungen von bestehenden Betriebsvereinbarungen gibt es allerdings Streit.[7] Brink, Landesdatenschutzbeauftragter in Baden-Württemberg, führt dazu aus:

»*DSGVO-Tipp: Die gestiegenen Anforderungen machen für die meisten Betriebsvereinbarungen eine Anpassung erforderlich. Wie Arbeitgeber und Betriebsrat dieser Herausforderung begegnen, sei es durch Anpassung jeder einzelnen Betriebsvereinbarung oder dem Abschluss einer Rahmenbetriebsvereinbarung, die für bereits abgeschlossene aber auch für künftig abzuschließende Betriebsvereinbarung Anwendung findet, bleibt den Betriebsparteien überlassen. Fest steht, dass der Handlungsbedarf dringend erkannt werden sollte. Nur die wenigsten Betriebsvereinbarungen werden beispielsweise die Zwecke der Verarbeitung konkret und bestimmt genug benennen oder die hohen Anforderungen in Sachen Transparenz erfüllen. Aber auch bei der Bestimmung angemessener und besonderer Schutzmaßnahmen im Sinne von Art. 88 Abs. 2 DSGVO wird auf die Betriebsparteien einiges an Arbeit zukommen. Hiervor sollten sie jedoch nicht zurückschrecken, sondern die Möglichkeit nutzen!*«

Er weist darauf hin, dass die Beratung zu Betriebsvereinbarungen inzwischen bei seiner Aufsichtsbehörde am stärksten nachgefragt wird. Nach Brink hat diese Form des betriebsgerechten Datenschutzes enormes Potenzial. [8]

- Anwendungsbereich des § 26 BDSG 2018

Die Regelungen des § 26 BDSG 2018 zum Beschäftigtendatenschutz beziehen sich nach Abs. 7 weiterhin, wie bislang in § 32 Abs. 2 BDSG a.F., auch auf Datenverarbeitungen, die nicht in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Diese Regelung des Gesetzgebers ist zulässig, weil der Anwendungsbereich der DSGVO offenkundig nicht betroffen ist.

- Straftaten im Beschäftigungsverhältnis

Die rechtliche Bestimmung zur Aufklärung von Straftaten im Beschäftigungsverhältnis unter Wahrung der Verhältnismäßigkeit ist unverändert von § 32 Abs. 1 Satz 2 BDSG a.F. in § 26 Abs. 1 Satz 2 BDSG 2018 übernommen worden. Richtig regelt die Bestimmung nur die Aufdeckung von Straftaten im Beschäftigungsverhältnis, nicht jedoch »untergesetzliche Regelverstöße« wie zum Beispiel grobe Pflichtverletzungen. Die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten zur Aufdeckung von Straftaten setzt nach der Rechtsprechung des BAG nur einen »einfachen« Anfangsverdacht voraus.[9]

- Einwilligungen im Beschäftigungskontext

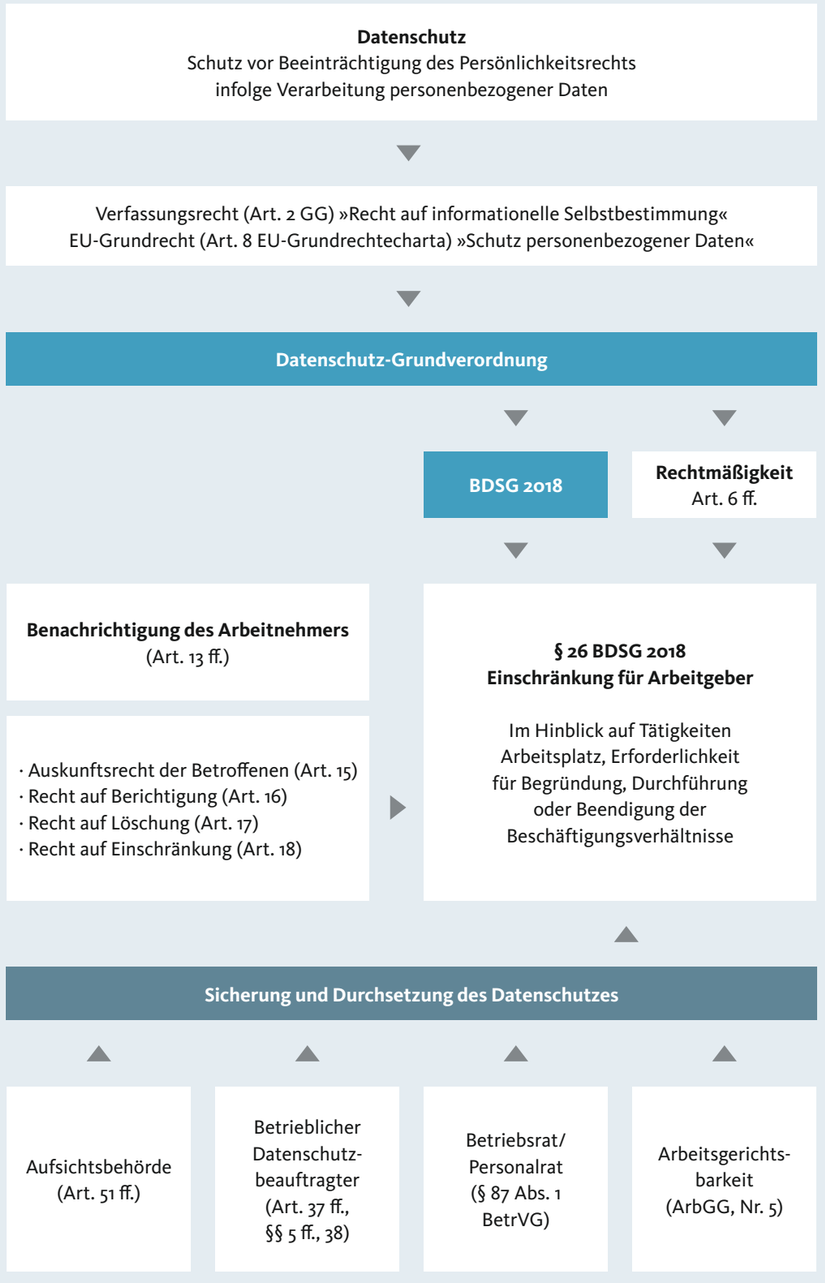
Der Gesetzgeber erwähnt jetzt in § 26 Abs. 2 BDSG 2018 Einwilligungen von Beschäftigten ausdrücklich als Verarbeitungsgrundlage. Der Erwägungsgrund (ErwGr) 155 betont ebenfalls die Zulässigkeit der Einwilligung als Rechtfertigungsgrund. Dabei wird die Freiwilligkeit der Einwilligung nach Art. 4 Nr. 11 DSGVO betont. Bezogen auf den Beschäftigungskontext war bislang die freie und informierte Einwilligung hoch umstritten, so besonders bei den Aufsichtsbehörden. Gerade mit Blick auf die Freiwilligkeit der Einwilligung in Kenntnis der Sachlage werden auch

7 Siehe hierzu den Beitrag von Kiesche/Berger/Wilke im Heft.

8 Brink, in: NZA-Sonderausgabe Arbeitnehmerdatenschutz, S. 7–8; grundlegend LfDI Baden-Württemberg; Der Ratgeber Beschäftigtendatenschutz: Zwischen wirtschaftlicher und persönlicher Abhängigkeit und informationeller Selbstbestimmung, 2. Aufl. März 2018.

9 Düwell/Brink, a.a.O., 1084.

ÜBERSICHT



Quelle: Michael Kittner, Arbeits- und Sozialordnung, 43.Aufl., Übersicht 43: Datenschutz

zukünftig genaue Feststellungen vom Verantwortlichen sowie bei Kontrollen von den zuständigen Aufsichtsbehörden zu treffen sein.[10] Die eingeschränkte Geltung der Einwilligung im Beschäftigungskontext in § 26 Abs. 2 BDSG 2018 aufgrund des Machtungleichgewichts zwischen Arbeitnehmer und Arbeitgeber ist nach wie vor zu beachten. Einwilligungen können einerseits gesetzlich vorgegeben sein, andererseits können sie im Beschäftigungsverhältnis eingeholt werden, wenn sie gleichermaßen Vorteile für die Beschäftigten und den Arbeitgeber bringen.

§ 26 Abs. 3 BDSG 2018 hat grundsätzlich das Schriftformgebot für die Wirksamkeit der Einwilligungserklärung aufgenommen. Allerdings ist ein Abweichen von der Schriftform zulässig, wenn »wegen besonderer Umstände eine andere Form angemessen ist«. Diese Besonderheiten können sich aus dem konkreten Beschäftigungsverhältnis zum Beispiel bei Telearbeit ergeben.[11]

▸ Beschäftigtenbegriff im Datenschutz erweitert

Die datenschutzrechtliche Definition der Beschäftigten in § 26 Abs. 8 (§ 3 Abs. 11 BDSG a.F.) stellt klar, dass der Betriebsrat auch für den Datenschutz der Bewerber tätig werden kann. Erstmals werden zudem die Leiharbeitnehmer in den Begriff einbezogen und das auch im Hinblick auf den Entleiherbetrieb.

▸ Der betriebliche Datenschutzbeauftragte

Das BDSG 2018 schreibt in Fortführung von § 4f BDSG a.F. auch seit dem 25.5.2018 vor, dass bei mehr als neun Beschäftigten, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, ein betrieblicher Datenschutzbeauftragter zu bestellen ist. Die derzeitigen Standards in Deutschland für die Bestellung und den Schutz der Datenschutzbeauftragten sind somit beibehalten worden (§ 38 BDSG 2018 in Verbindung mit § 6 BDSG 2018).[12]

▸ Kritikwürdige Bestimmungen im BDSG 2018

Im BDSG 2018 gibt es weiterhin etliche Leerstellen im Beschäftigtendatenschutz. Es fehlen ein eindeutiges Verbot heimlicher Kontrollen und ausreichende gesetzliche Vorgaben zum Fragerecht des Arbeitgebers, zur Videoüberwachung von Beschäftigten in öffentlich nicht zugänglichen Räumen, Verwendung von biometrischen Daten oder zur Ortung bzw. Erstellung von Bewegungsprofilen von Beschäftigten. Ebenso werden Cloud Computing, Social Media Monitoring und Big Data nicht angemessen geregelt.

Kein großer Wurf, aber klar und verständlich

§ 26 BDSG 2018 ist zu Recht nicht als der große Wurf zum Beschäftigtendatenschutz bezeichnet worden. Ein umfassendes Gesetz zum Beschäftigtendatenschutz bleibt zwar wünschenswert, ist aber nicht realistisch. Insofern ist jetzt § 26 BDSG 2018 für Beschäftigtenvertretungen das »Grundgesetz des Beschäftigtendatenschutzes«. Die Betriebsparteien müssen die Bestimmungen in Betriebsvereinbarungen konkretisieren.

Neben der berechtigten Kritik von Datenschützern ist positiv festzuhalten: Die Bestimmungen und Neuerungen des § 26 BDSG sind klar und verständlich, regeln den Beschäftigtendatenschutz ganzheitlich unter Einbezug der sensiblen Daten und wahren mit konkreten Verweisen den Anwendungsvorrang der DSGVO. Zudem bleibt die Rechtsprechung des BAG zum Beschäftigtendatenschutz, vor allem zum § 32 BDSG a.F., aller Wahrscheinlichkeit nach erhalten. Die Beibehaltung des bisherigen nationalen Standards zum betrieblichen Datenschutzbeauftragten ist zu begrüßen. Die Datenverarbeitung durch Interessenvertretungen erhält zumindest eine wichtige neue Rechtsgrundlage in § 26 Abs. 1 Satz 1 BDSG 2018. Betriebsräte können Beschäftigtendaten verarbeiten, wenn sie erforderlich zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einer Kollektivvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten sind.

Im Zusammenspiel DSGVO, Betriebsvereinbarungen und § 26 BDSG 2018 lässt sich der Beschäftigtendatenschutz von engagierten Datenschützern in Unternehmen und Behörden voranbringen. ◁

Matthias Wilke, Geschäftsführer Datenschutz- und Technologieberatung (dtb), Kassel.
info@dtb-kassel.de

10 A.a.O.
11 A.a.O., 1085.
12 Siehe hierzu den Beitrag von Kiesche im Heft.

Neue Rolle für Datenschutzbeauftragte

GESTÄRKTER DATENSCHUTZBEAUFTRAGTER *Die DSGVO weist dem betrieblichen Datenschutzbeauftragten neue Aufgaben zu. Er wird zur Anlauf- und Beratungsstelle für Betriebsräte, betroffene Beschäftigte, Aufsichtsbehörden und Kunden.*

VON **EBERHARD KIESCHE**

Der betriebliche Datenschutzbeauftragte ist nach Art. 37–39 Datenschutz-Grundverordnung (nachfolgend DSGVO) in festgelegten Fällen europaweit vorgeschrieben. Zudem sieht Art. 37 Abs. 4 Satz 1 DSGVO eine Öffnungsklausel vor, die es den nationalen Gesetzgebern ermöglicht, Benennungsvoraussetzungen für den Datenschutzbeauftragten festzulegen (so jetzt im § 38 Abs. 1 Satz 1 und 2 BDSG 2018).[1] Danach besteht für nicht-öffentliche Stellen, das heißt, auch für Unternehmen in der Privatwirtschaft, eine Benennungspflicht, sofern sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigen. Dieser Beitrag erörtert die Rolle des Datenschutzbeauftragten nach der DSGVO, wesentliche Neuerungen und gibt mögliche Antworten auf strittige Fragen, die sich in der betrieblichen Praxis stellen.[2]

Europaweite verpflichtende Benennung

Insgesamt nimmt die Bedeutung des betrieblichen/behördlichen Datenschutzbeauftragten (nachfolgend bDSB) in Europa zu. Neu ist die europaweite verpflichtende Benennung eines bDSB in öffentlichen Stellen und auch in der Privatwirtschaft. Die Grundregeln zum bDSB finden sich in Art. 37–39 DSGVO. In Art. 37 Abs. 1 DSGVO werden risikoorientiert Voraussetzungen festgelegt, wann ein bDSB zu benennen ist.[3] Durch §§ 5, 6, 7, 38 Bundesdatenschutzgesetz (BDSG) 2018 wird der bisherige nationale Standard ohne wesentliche Änderungen für den bDSB beibehalten. Betriebliche Datenschutzbeauftragte müssen mit dem 25.5.2018 nicht neu bestellt werden. Der bDSB ist ein besonders wichtiges Element eines Datenschutz-Managementsystems, das jetzt aufgrund der DSGVO (Art. 33 und ErwGr 87) eingeführt werden muss.[4]

Juristische Personen als externe Datenschutzbeauftragte?

Der Verantwortliche ist nach Art. 4 Nr. 7 DSGVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Grundsätzlich kann der Verantwortliche auch nach Art. 37 Abs. 6 DSGVO wählen, ob er einen internen oder einen externen Datenschutzbeauftragten benennt. Strittig ist die Frage, ob eine juristische Person als externer Datenschutzbeauftragter arbeiten darf.[5] Die Art. 29-Datenschutzgruppe sieht in ihren Leitlinien zum Datenschutzbeauftragten (WP 243 rev.01) diese Möglichkeit vor. Es ist zu empfehlen, in der juristischen Person (Datenschutzgruppe) einen Anwalt als namentlichen Ansprechpartner zu benennen.

Der Datenschutzbeauftragte erhält nun eine Garantenfunktion

Insgesamt ergeben sich durch die DSGVO zusätzliche und veränderte Aufgaben für den

DARUM GEHT ES

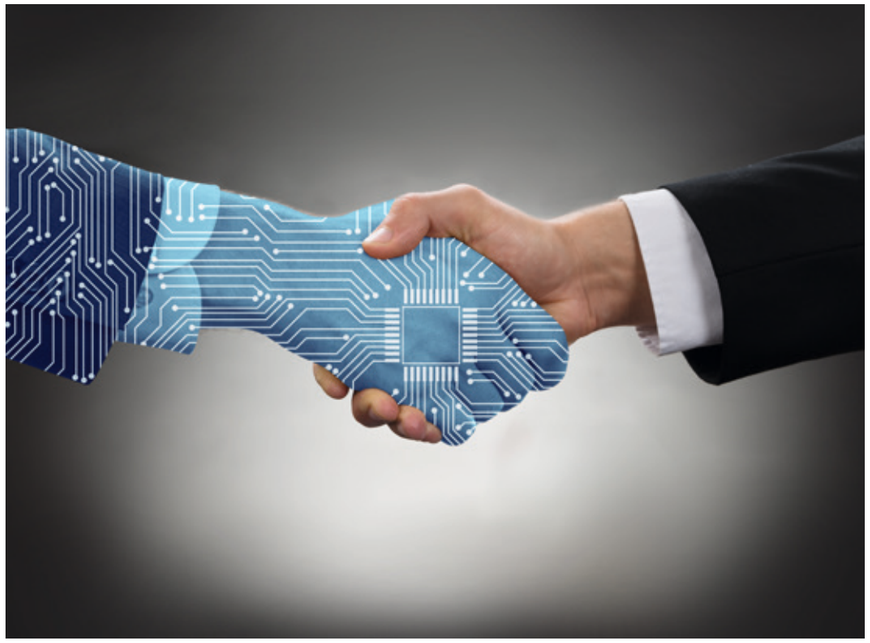
1. Die Bedeutung des betrieblichen Datenschutzbeauftragten (bDSB) nimmt durch die Regelungen der DSGVO zu.

2. An die Stelle der Vorabkontrolle tritt die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO.

3. Betriebsräte dürfen den bDSB nicht kontrollieren, da dieser weisungsfrei arbeitet. Die Pflicht des bDSG zur Kooperation mit dem Betriebsrat besteht aber weiterhin.

1 Zum Verständnis Kranig/Ehmann, Erste Hilfe zur Umsetzung der Datenschutz-Grundverordnung, München 2017, 32 ff.
2 Umfassend und zu empfehlen Jaspers/Reif, Kommentierung zu Art. 37–39 DSGVO, in: Schwartmann, Jaspers, Thüsing/Kugelmann, DS-GVO/BDSG, Heidelberg 2018, 831 ff.
3 Ausführlich hierzu Niklas/Faas, Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung, in: NZA-Sonderausgabe Arbeitnehmerdatenschutz, 53, 54 (NZA 2017, 1091).
4 Siehe Einleitung, NZA-Sonderausgabe Arbeitnehmerdatenschutz, 7; Reif, in Gola, DS-GVO, Art. 33, Rn. 40–41; umfassend Schierbaum, Gestärkte Datenschützer, CuA 1/2018, 14–19.
5 Hierzu Jaspers/Reif, a.a.O., Art. 37 Rn. 45.

Der betriebliche Datenschutzbeauftragte ist auch an Datenschutzstrategien des Unternehmens oder an der Datenschutz-Folgenabschätzung beteiligt.



bDSB. Art. 39 Abs. 1 a–e DSGVO führt nicht abschließend fünf Aufgaben an. An die Stelle der Vorabkontrolle tritt die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO. Der fachkundige bDSB wird für alle beteiligten Akteure im betrieblichen Datenschutz eine Anlauf- und Beratungsstelle.

Vor allem ändert sich die Gesamtaufgabe des bDSB. Sein Hinwirken auf die Einhaltung der Datenschutzvorschriften in § 4g BDSG a.F. wird ab 25.5.2018 durch eine umfassende Überwachungs- bzw. Compliancefunktion nach Art. 39 Abs. 1b DSGVO abgelöst. Er muss überwachen, dass die Vorschriften der DSGVO und anderer Datenschutzgesetze eingehalten werden. Die konkrete Überwachungsfunktion bezieht sich unter anderem auf interne Datenschutzstrategien. Damit wird er de facto zum Compliance-Manager.[6] Sein Ziel muss es sein, kontinuierlich Datenverstöße und Unregelmäßigkeiten zu erkennen und zu verhindern. Die neue Rolle hat Auswirkungen auf die (zivil- und strafrechtliche) Haftung des bDSB. Er kann sich grundsätzlich durch Unterlassen seiner Pflichten aufgrund von § 13 Strafgesetzbuch (StGB) strafbar machen. Das setzt voraus, dass der bDSB vorsätzlich handelt.[7]

Stellung des internen bDSB und Haftung

Der bDSB ist im Falle der Nichteinhaltung der DSGVO durch den Verantwortlichen selber nicht verantwortlich. Er sollte jedoch Stellen- oder Funktionsbeschreibungen oder ein Delegationsschreiben, in dem ihm die Handlungsverantwortung für die Erledigung echter Datenschutzpflichten des Verantwortlichen übertragen wird, eindeutig zurückweisen. Für die Einhaltung der datenschutzrechtlichen Bestimmungen ist der Verantwortliche bzw. der Auftragsverarbeiter verantwortlich. Der bDSB bleibt eigenständig, hat aber keine über die Aufgaben in Art. 39 DSGVO hinausgehende Entscheidungsbefugnis in der Linienfunktion. Eine derartige Verantwortung würde der unabhängigen Stellung des bDSB widersprechen.[8]

Der bDSB führt somit keine Maßnahmen des Datenschutzes durch, sondern berät, bewertet und überwacht ausschließlich. Er ist zum Beispiel in der Frage der Datenschutzstrategien des Unternehmens (Policies) oder bei der Durchführung der Datenschutz-Folgenabschätzung nach Art. 35, 36 DSGVO beteiligt.

Folgt der Verantwortliche seinen Ratschlägen nicht, zum Beispiel bei der Meldung von Datenschutzverletzungen nach Art. 33, 34 DSGVO, sollte der bDSB seine abweichende Stellungnahme dokumentieren. Das Führen eines Verarbeitungsverzeichnisses nach Art. 30 DSGVO[9] oder die Durchführung von Datenschutzschulungen kann ihm vom Verantwortlichen zusätzlich übertragen werden. Diese zusätzlichen Aufgaben dürfen aber nicht seine Aufgabenerfüllung nach Art. 39 DSGVO beeinträchtigen und nicht zu einem Interessenkonflikt führen.

Unterstützungspflicht

Auch weiterhin muss der Verantwortliche, zum Beispiel das Unternehmen oder die Behörde, den bDSB nach Art. 39 Abs. 2 DSGVO und § 6 Abs. 2 BDSG 2018 für öffentliche Stellen umfassend mit den erforderlichen Ressourcen für die Erfüllung seiner Aufgaben unterstützen. Ihm ist frühzeitig Zugang zu allen Informationen und Verarbeitungen personenbezogener Daten zu gewähren.

Die Pflicht zur Unterstützung betrifft etwa geeignete IT-Ausstattung, Räume, Büroeinrichtungen, Fachliteratur, Fortbildungen (Art. 38 Abs. 2 DSGVO) zum Erhalt des Fachwissens und ausreichende finanzielle und personelle Mittel. Dem bDSB muss vor allem ein ausreichendes Zeitbudget zugestanden werden, das abhängig ist von Faktoren wie zum Beispiel der Anzahl der Datenverarbeitungsvorgänge und der Schutzbedürftigkeit der Daten. Es ist dringend zu empfehlen, dass zumindest in größeren Unternehmen, Unternehmensgruppen und Behörden Datenschutzkoordinatoren, die den bDSB unterstützen, benannt werden. Weiterhin sollten Datenschutzbeauftragte regelmäßigen Zugang zu Treffen des mittleren und oberen Managements erhalten. Es ist weiterhin anzuraten, falls Auftragsverarbeitung nach Art. 28 DSGVO besteht, mit dem Datenschutzbeauftragten des Auftragsverarbeiters zusammenzuarbeiten.

Kontaktdaten des bDSB müssen publiziert werden

Die Kontaktdaten des bDSB beim Verantwortlichen oder beim Auftragsverarbeiter müssen intern und extern zum Beispiel nach Art. 13 Abs. 1, Art. 30 Abs. 1 und Art. 33 Abs. 3b DSGVO publiziert werden. An die Aufsichtsbehörde sind gemäß Art. 37 Abs. 7 DSGVO die Kontaktdaten weiterzugeben. Es empfiehlt sich, den bDSB namentlich zu nennen. Der bDSB muss über eine Hotline oder abhörsichere Anrufbeantworter persönlich erreichbar sein. Sichere Kommunikationskanäle für die Vertraulichkeit seiner Arbeit nach Art. 38 Abs. 5 DSGVO und § 6 Abs. 5, § 38 Abs. 2 BDSG 2018 sind demnach unerlässlich. Alle Beschäftigten sind über die Benennung eines Datenschutzbeauftragten zu informieren.

Gemeinsamer Datenschutzbeauftragter für eine Unternehmensgruppe

Nach Art. 37 Abs. 2 DSGVO (§ 5 Abs. 2 BDSG 2018 für öffentliche Stellen) ist es jetzt ausdrücklich zulässig, als Unternehmensgruppe (Art. 4 Nr. 19 DSGVO) bzw. Konzern in einem Akt einen gemeinsamen Datenschutzbeauftragten zu benennen. Voraussetzung ist jedoch eine leichte sprachliche und örtliche Erreichbarkeit sowohl für die betroffenen Personen als auch für die zuständigen Aufsichtsbehörden von jeder Niederlassung aus (Art. 4 Nr. 16 DSGVO).[10]

Der zentrale Datenschutzbeauftragte muss mit den betroffenen Personen wirksam kommunizieren und mit den zuständigen Datenschutzaufsichtsbehörden effektiv zusammenarbeiten können. Das setzt voraus, dass er in der von den Betroffenen und den Aufsichtsbehörden verwendeten Sprache kommunizieren kann. Ein französischer zentraler Datenschutzbeauftragter in einem Konzern mit weit auseinanderliegenden Standorten, der als direkter Ansprechpartner für Beschäftigte in Deutschland dienen soll, wäre wohl nicht mehr »leicht erreichbar«.

Für die »leichte Erreichbarkeit« muss der Verantwortliche als Grundvoraussetzung die Kontaktdaten des bDSB veröffentlichen, vor allem gegenüber den Aufsichtsbehörden, Beschäftigten und Kunden. Leichte Erreichbarkeit setzt zudem voraus, dass der zentrale Datenschutzbeauftragte in Konzern-Einzelgesellschaften von Koordinatoren unterstützt wird und eine umfassende Qualifikation vorweisen kann.

Der Datenschutzbeauftragte zwischen Verantwortlichen und Aufsichtsbehörde

Der Datenschutzbeauftragte hat nach Art. 36 Abs. 3d, 39 Abs. 1e DSGVO die Funktion, für die zuständige Aufsichtsbehörde eine Anlaufstelle zur Kontaktherstellung zu sein. Er hat mit der zuständigen Aufsichtsbehörde in Datenschutzfragen zusammenzuarbeiten. Er

6 Siehe auch Niklas/Faas, a.a.O., 57.
7 A.a.O., 59, insbesondere das Fazit; besonders lesenswert Jaspers/Reif, a.a.O., Art. 39 Rn. 25 – 27.
8 Niklas/Faas, a.a.O., 58 f.
9 Gossen/Schramm, Das Verarbeitungsverzeichnis der DS-GVO. Ein effektives Instrument zur Umsetzung der neuen unionsrechtlichen Vorgaben, ZD 2017, 7.
10 Niklas/Faas, a.a.O., 55; Klug, in: Gola, DS-GVO, Art. 37 Rn. 17, 18; Jaspers/Reif, a.a.O., Art. 37 Rn. 31 – 33.

AiB extra August|2018 Neue Rolle für Datenschutzbeauftragte EBERHARD KIESCHE

AUS DEM GESETZ

Normen aus der DSGVO und dem BDSG 2018

Art. 37 DSGVO Benennung eines Datenschutzbeauftragten
(1) Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn
a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln,
b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.
(2) Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.
(3) Falls es sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder öffentliche Stelle handelt, kann für mehrere solcher Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden.
(4) Für in anderen als den in Absatz 1 genannten Fällen können der Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, einen Datenschutzbeauftragten benennen; falls dies nach dem Recht der Union oder der Mitgliedstaaten vorgeschrieben ist, müssen sie einen solchen benennen. Der Datenschutzbeauftragte kann für derartige Verbände und andere Vereinigungen, die Verantwortliche oder Auftragsverarbeiter vertreten, handeln.
(5) Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.
(6) Der Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.
(7) Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

§ 5 BDSG 2018 Benennung
(1) Öffentliche Stellen benennen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten. Dies gilt auch für öffentliche Stellen nach § 2 Absatz 5, die am Wettbewerb teilnehmen.
(2) Für mehrere öffentliche Stellen kann unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe eine gemeinsame Datenschutzbeauftragte oder ein gemeinsamer Datenschutzbeauftragter benannt werden.
(3) Die oder der Datenschutzbeauftragte wird auf der Grundlage ihrer oder seiner beruflichen Qualifikation und insbesondere ihres oder seines Fachwissens benannt, das sie oder er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage ihrer oder seiner Fähigkeit zur Erfüllung der in § 7 genannten Aufgaben.
(4) Die oder der Datenschutzbeauftragte kann Beschäftigte oder Beschäftigter der öffentlichen Stelle sein oder ihre oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.
(5) Die öffentliche Stelle veröffentlicht die Kontaktdaten der oder des Datenschutzbeauftragten und teilt diese Daten der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mit.

§ 38 BDSG 2018 Datenschutzbeauftragte nichtöffentlicher Stellen
(1) Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.
(2) § 6 Absatz 4, 5 Satz 2 und Absatz 6 finden Anwendung, § 6 Absatz 4 jedoch nur, wenn die Benennung einer oder eines Datenschutzbeauftragten verpflichtend ist.

kann dabei in Loyalitätskonflikten gegenüber der Leitung des Unternehmens geraten, zum Beispiel in der Unterrichtung und Beratung über die Datenschutz-Folgenabschätzung nach Art. 35, 36 DSGVO oder bei Beschwerden von betroffenen Personen als »Anwalt der Betroffenen«. Wichtig ist, dass die Beratung des bDSB durch die Aufsichtsbehörden nach Art. 57 Abs. 3 DSGVO unentgeltlich für das Unternehmen ist, ebenso wie für die betroffenen Personen, die Beschwerde bei der Aufsichtsbehörde einlegen. Insofern empfiehlt es sich für Verantwortliche und Auftragsverarbeiter, gegebenenfalls nach Art. 37 Abs. 4 Satz 1 DSGVO freiwillig einen Datenschutzbeauftragten zu benennen. Auch für einen solchen Datenschutzbeauftragten gelten die Vorgaben der Art. 37 – 39 DSGVO insgesamt.

Unbeschränkte Befugnisse für den bDSB: Den Betriebsrat kontrollieren?

Die Frage stellt sich, ob nach Art. 39 DSGVO der bDSB ab 25.5.2018 im Rahmen seiner Kontrollpflicht den Betriebsrat kontrollieren darf und das entsprechende Verbot bzw. die gültige Rechtsprechung des BAG von 1997[11] damit wegfällt. Die Überwachungsfunktion des bDSB nach Art. 39 Abs. 1 DSGVO ist offensichtlich nicht eingeschränkt.

Allerdings ist nach dem BDSG 2018 und der DSGVO (Erwägungsgrund (ErwGr) 197) die vollständige Unabhängigkeit des bDSB in der Praxis nicht gegeben. Er ist der Unternehmensleitung zuzuordnen, auch wenn er bei der Ausübung seiner Aufgaben und Pflichten nach Art. 38 Abs. 3 Satz 1 DSGVO weisungsfrei handeln soll. Die einzig wirklich unabhängige Kontrollinstanz ist der Betriebsrat.[12] Das tragende Prinzip der Betriebsverfassung (die Unabhängigkeit des Betriebsrats vom Arbeitgeber) würde mit der Kontrollbefugnis des bDSB gegenüber dem Betriebsrat aufgehoben werden. Eine gegenseitige Kontrollmöglichkeit ist wohl auch nach dem 25.5.2018 nicht vorgesehen.[13] Die Pflicht zur Kooperation des bDSB mit den Beschäftigtenvertretungen ist weiterhin gegeben.[14]

Können Betriebsräte weiterhin betriebliche Datenschutzbeauftragte sein?

Nach Art. 38 Abs. 6 Satz 2 DSGVO und § 7 Abs. 2 BDSG 2018 wird »Zuverlässigkeit« gefordert. Andere Aufgaben und Pflichten bei einem Teilzeit-bDSB dürfen nicht zu Interessenkonflikten führen. Insofern kann jetzt zweifelhaft sein, ob Betriebsräte weiterhin noch das Amt eines Datenschutzbeauftragten ausüben können. Interessenkonflikte sind wohl grundsätzlich nicht auszuschließen, so dass die bisherige Rechtsprechung des 10. Senats Bundesarbeitsgericht (BAG) in Frage gestellt werden kann.[15] Bisher hat das BAG zu Recht eine generelle Vermutung der Unzuverlässigkeit der Betriebsräte aufgrund einer bloßen Mitgliedschaft für die Aufgabe des bDSB abgelehnt.

Betriebsrat als Verantwortlicher oder Teil des Verantwortlichen?

Die Beantwortung der Frage, ob der bDSB den Betriebsrat kontrollieren kann, hängt auch davon ab, ob der Betriebsrat als Teil des Verant-

11 BAG 11.11.1997 – 1 ABR 21/97.
12 Däubler, Gläserne Belegschaften. Das Handbuch zum Beschäftigtendatenschutz, 7. Auflage, Frankfurt 2017, Rn. 635, 685 ff.
13 Andere Auffassung Jaspers/Reif, a.a.O., Art. 39 Rn. 15.
14 Simitis-Simitis, Bundesdatenschutzgesetz, 8. Aufl., § 4g Rn. 8;
15 BAG 23.3.2011 – 10 AZR 562/09; siehe hierzu Jaspers/Reif, a.a.O., Art. 38 Rn. 29.

Wichtigste Aufgabe des betrieblichen Datenschutzbeauftragten ist die Überwachung, dass die Datenschutz-Grundverordnung und andere Datenschutzgesetze eingehalten werden.

wortlichen oder als eigenständiger Verantwortlicher zu qualifizieren ist. Das BAG hat bislang wiederholt bestätigt, dass der Betriebsrat Teil der verantwortlichen Stelle ist.[16] Es hat eine Weitergabe von personenbezogenen Daten der Beschäftigten durch den Arbeitgeber an den Betriebsrat als Nutzung durch den Arbeitgeber bewertet, nicht als Datenübermittlung. Diese Frage wird in naher Zukunft von den Gerichten erneut zu entscheiden sein.[17] Eindeutig ist der Betriebsrat nach Art. 4 Nr. 10 DSGVO nicht Dritter. Jetzt ist offen, ob nach der DSGVO der Betriebsrat nun Teil des Verantwortlichen oder selber Verantwortlicher (Art. 4 Nr. 7 DSGVO) ist oder mit dem Arbeitgeber eine gemeinsame Verantwortung teilt.[18]

Betriebsräte überwachen die Einhaltung von BDSG 2018 und DSGVO

Der bDSB und der Betriebsrat kontrollieren sich nicht gegenseitig. Sie sorgen unter dem Gebot der Zusammenarbeit für die Einhaltung des Datenschutzes im Unternehmen. Betriebsräte dürfen und müssen jedoch überwachen, ob die Datenschutzgesetze zugunsten der Beschäftigten eingehalten werden.

Dazu gehören zum Beispiel die Anforderungen der DSGVO insgesamt, die Aufgabenerfüllung und die Rahmenbedingungen bzw. die erforderlichen Ressourcen für die Arbeit des bDSB. Der Betriebsrat sollte sich beispielsweise den Jahresplan/Jahresbericht für die Arbeit des bDSB vorlegen lassen und mit ihm den Beschäftigtendatenschutz in gemeinsamen Sitzungen erörtern.

Die Aufsichtsbehörde kann tätig werden

Wenn die Zuverlässigkeit des bDSB nicht gegeben ist, weil seine sonstigen Aufgaben ihn in einen Interessenkonflikt bringen, kann die zuständige Aufsichtsbehörde den bDSB abberufen. Das gilt auch dann, wenn der bDSB die für seine Aufgaben erforderliche Fachkunde[19] nicht besitzt. Die Datenschutzaufsichtsbehörden sollen den bDSB unterstützen und beraten (§ 40 Abs. 6 Satz 1 und 2 BDSG 2018).

Die wachsende Bedeutung und Verantwortung des bDSB

Mit der DSGVO erhält der bDSB neue Aufgaben und vor allem eine Überwachungsfunktion. Er muss überwachen, dass die DSGVO und andere Datenschutzgesetze eingehalten werden. Er wird somit zu einer echten Anlauf- und Beratungsstelle für betroffene Kunden, Beschäftigte, Aufsichtsbehörden und Beschäftigtenvertretungen. Angesichts der Herausforderungen für den (Beschäftigten-)Datenschutz durch das neue Recht und die Digitalisierung der Wirtschaft sollten die Kontrollinstanzen des Datenschutzes kooperieren und bereits bestehende Formen der Zusammenarbeit erheblich verstärken. Eine Untätigkeit des bDSB oder mangelnde Aufgabenerfüllung sollte angesichts der Bußgelder nach Art. 83 DSGVO nicht mehr vorkommen. ◁

Dr. Eberhard Kiesche,
Berater, Arbeitnehmerorientierte Beratung (AoB), Bremen.

16 Zum Beispiel BAG 18.7.2012 – 7 ABR 23/11.
17 Zum Beispiel Gola-Gola, DS-GVO, Art. 4 Rn. 55.
18 Düwell/Brink, Viele Änderungen und wenig Neues, in NZA-Sonderausgabe Arbeitnehmerdatenschutz, S. 19.
19 Siehe das Anforderungsprofil für bDSB des Düsseldorfer Kreises vom 24./25.11.2010.

Wer hat den Hut auf?

ZUSTÄNDIGKEITSBEREICH *Das Zusammenspiel zwischen Einzelbetriebsrat, Gesamtbetriebsrat und Konzernbetriebsrat ist nicht immer konfliktfrei. Gesetzgeber und Rechtsprechung tragen hier nur bedingt zur Klärung bei. Delegierung, Dezentralisierung und administrative Unterstützung bieten »Hilfslösungen«.*

VON **WOLFGANG DÄUBLER**

Die Beteiligung des Betriebsrats bezieht sich nicht selten auf Fragen, die sich nicht auf den Betrieb als arbeitstechnische Einheit beziehen. Vielmehr geht es um Angelegenheiten, über die auf Unternehmens- oder Konzernebene entschieden wird. Wer soll bei der Verwaltung einer Unterstützungskasse mitbestimmen, die unternehmens- oder konzerneinheitliche Leistungen vorsieht? Wer soll über das im ganzen Unternehmen oder im ganzen Konzern eingesetzte SAP-System mitentscheiden? Dass man in beiden Fällen eine Arbeitnehmervertretung auf Unternehmens- wie auf Konzernebene braucht, liegt auf der Hand. Im Grundsatz ist es also völlig berechtigt, dass es einen Gesamt- und einen Konzernbetriebsrat gibt. Fraglich ist allein, wie die Zuständigkeiten im Einzelnen bestimmt werden. Gibt man dem Gesamtbetriebsrat zu weite Befugnisse, können Basisaktivitäten abgeblockt werden. Bestimmt man seine Zuständigkeit zu eng, muss man sehr viele Einzelbetriebsräte unter einen Hut bringen.

Die gesetzliche Regelung

In Bezug auf die Zuständigkeiten von Betriebsrat und Gesamtbetriebsrat (GBR) hat der Gesetzgeber in § 50 Abs. 1 BetrVG keine sehr klare Lösung getroffen. Eine Kompetenz des GBR besteht dann, wenn

- es um Angelegenheiten geht, die das Gesamtunternehmen oder mehrere Betriebe betreffen und wenn
- sie nicht durch die einzelnen Betriebsräte innerhalb ihrer Betriebe geregelt werden können.

Während sich die erste Bedingung meist leicht feststellen lässt – es genügt schon, dass zwei Betriebe betroffen sind –, hat die zweite einiges Kopfzerbrechen bereitet. Bei wörtlicher Auslegung hätte der Gesamtbetriebsrat gar keinen Aufgabenbereich, ist doch ein abgestimmtes Vorgehen aller Einzelbetriebsräte immer möglich. Da dies nicht gewollt sein kann, stehen Rechtsprechung und herrschende Lehre auf dem Standpunkt, für eine betriebsübergreifende Regelung müsse ein zwingendes Erfordernis sprechen; bloße Zweckmäßigkeit genüge nicht.[1] In gleicher Weise wird auch die Zuständigkeit des Konzernbetriebsrats (KBR) von der des GBR und des Einzelbetriebsrats abgegrenzt.

Der Schematismus des BAG

Über das zwingende Erfordernis kann man sicherlich unterschiedlicher Auffassung sein, doch schafft eine andere Aussage des BAG in der Praxis sehr viel mehr Probleme: Sobald eine Zuständigkeit des GBR in Bezug auf einen Teil einer Angelegenheit bestehe, falle diese insgesamt in die Kompetenz des GBR. Es bestehe – so das BAG[2] – ein Grundsatz der Zuständigkeitstrennung. Damit sei eine Beschränkung des GBR auf eine Rahmenkompetenz nicht vereinbar. Im Zusammenhang mit der unternehmensweiten Einführung einer technischen Einrichtung anerkannte das BAG zwar, »dass es häufig Detailfragen (gibt), die für mehrere Betriebe unterschiedlich geregelt werden könnten«, doch müsse es schon wegen der schwierigen Abgrenzungsprobleme bei der strikten Zuständigkeitstrennung und damit bei der Regelungskompetenz des GBR

DARUM GEHT ES

1. Zwischen Betriebsratsgremien innerhalb eines Unternehmens kommt es immer wieder zu Auseinandersetzungen bei der Zuständigkeit.

2. Das BetrVG und das Bundesarbeitsgericht liefern keine Musterlösungen für ein generelles Vorgehen.

3. Beschränkung auf Sachfragen und Delegierung von Aufgaben können zur Klärung beitragen.

1 BAG, NZA 1999, 947; BAG, NZA 2002, 688; BAG, NZA 2002, 988; BAG, NZA 2005, 234, 235; aus der Lit. s. den Überblick bei Fitting, BetrVG, 28. Aufl. 2016, § 50 Rn. 20 ff.
2 BAG, NZA 2007,399.

bleiben. Bei einem technischen System müssen somit auch die Zugriffsmöglichkeiten im Einzelbetrieb vom GBR mitgeregelt werden. Den Beteiligten ist es auch nicht möglich, einzelne Befugnisse auf die untere Ebene zu delegieren.[3]

Diese Position vermag nicht zu befriedigen. Schon vom Gesetzeswortlaut her ist sie alles andere als überzeugend: § 50 Abs. 1 BetrVG bezieht die Zuständigkeit des GBR auf »Angelegenheiten«, nicht auf »Mitbestimmungsrechte«. Können denn verschiedene »Angelegenheiten« nicht auch im selben Mitbestimmungsrecht enthalten sein? § 87 Abs. 1 Nr. 6 BetrVG betrifft beispielsweise die »Einführung« von technischen Einrichtungen, aber auch ihre »Anwendung« einschließlich der Änderung. Warum sollen dies nicht zwei verschiedene »Angelegenheiten« sein? Dasselbe liegt bei Sozialeinrichtungen nahe: Ihre Form ist das eine, ihre Verwaltung das andere. Hier zu differenzieren, würde naheliegen;[4] in der neuesten Literatur wird das Problem aufgegriffen.[5] Dazu kommt das vom BAG entwickelte Verbot der Delegierung: Wenn man schon die Mitbestimmung des GBR auf den gesamten Gegenstand des Mitbestimmungsrechts ausdehnt, sollte dann nicht wenigstens die Möglichkeit bestehen, im Einvernehmen die untere Ebene über bestimmte Fragen entscheiden zu lassen? Wo bleibt hier die sonst so gerne gepriesene Flexibilität? Warum sollte man dort, wo es kein zwingendes Bedürfnis für Einheitlichkeit mehr gibt, nicht eine dezentrale Regelung zulassen?

Was tun, wenn sich nichts ändert?

Ob sich die Rechtsprechung eines Besseren besinnt, ist eine offene Frage. In der Regel ist hier eher Skepsis angebracht, da Richter nicht gerne zugeben, früher falschgelegen zu haben, und da – wichtiger – die getroffenen Entscheidungen Orientierung für den Bürger vermitteln wollen und dies nicht mehr funktionieren würde, wenn es allzu häufig »neue Erkenntnisse« gäbe. Deshalb muss man sich realistischerweise Gedanken machen, wie man sich am besten auf der Grundlage der bestehenden Rechtsprechung einrichtet.[6]

Hilfslösung 1: Die ausnahmsweise zulässige Delegierung

Das BAG hat einen kleinen Ausweg gelassen und eine Öffnungsklausel zugunsten einer freiwilligen Regelung auf örtlicher Ebene erwogen, die jedenfalls die Materien erfassen könne, die die Betriebsparteien auch dem Arbeitgeber zur Alleinentscheidung überlassen könnten.[7] In der Literatur ist dieser Vorschlag begrüßt worden.[8] Im Bereich der hier interessierenden Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG könnte diese Aussage Bedeutung gewinnen. Niemand hätte Bedenken dagegen, dass der Arbeitgeber darüber entscheidet, welche der auf Unternehmensebene durch den GBR gebilligten Funktionen im Betrieb A und welche im Betrieb B aktiviert werden. Unterstellt, eine Telefonanlage besitzt eine Weiterleitungsfunktion, die vom GBR auch akzeptiert wurde, weil die Erstellung eines »Arbeitsprofils« und überhaupt jede Verwendung zur Kontrolle von Verhalten und Leistung ausgeschlossen wurde. Im Betrieb A gibt es sehr viele Besprechungen, so dass der verbreitete Wunsch nach Erreichbarkeit besteht. Im Betrieb B bleiben die Beschäftigten typischerweise an ihrem Arbeitsplatz, so dass die Situation eine andere ist. Möglich wäre es daher, die Aktivierung der Funktion der gemeinsamen Entscheidung von Betriebsrat und Betriebsleitung zu überlassen.[9] Die Mitbestimmung des Einzelbetriebsrats würde allerdings bei einer definitiven Nicht-Einigung ihr Ende finden. Es wäre dann Sache des GBR, die Angelegenheit wieder an sich zu ziehen und von seinem Mitbestimmungsrecht Gebrauch zu machen.

Hilfslösung 2: Dezentralisierung des GBR

Gibt es für den GBR Möglichkeiten, sich vor Ort um die Bedürfnisse der Beschäftigten zu kümmern und sie in seine Entscheidungen einfließen zu lassen?

Zu denken ist an die Bildung von Ausschüssen, die auch dem GBR gestattet ist. Ihnen können allerdings Aufgaben zur selbstständigen Erledigung nur übertragen werden, wenn zugleich ein Gesamtbetriebsausschuss besteht. Auch dann ist freilich der Abschluss von (Gesamt-)Betriebsvereinbarungen ausgeschlossen.[10] Ausschüsse ermöglichen eine Spezialisierung, erweitern jedoch nicht die verfügbaren Ressourcen. Ob der GBR auch Betriebsratsmitglieder in einen Ausschuss berufen kann, die ihm nicht angehören, ist kaum erörtert. Ersichtlich ist nur eine Stimme, die dies bejaht, allerdings auf Fälle beschränkt, in denen der Ausschuss keine Befugnis zur selbstständigen Erledigung bestimmter Angelegenheiten hat.[11] Dies ist konsequent, da andernfalls das spezifische Stimmengewicht, das für Beschlüsse des GBR besteht, ausgehebelt werden könnte. Der GBR hat deshalb keine realistische Möglichkeit, örtliche Betriebsratsmitglieder oder gar einen dort bestehenden »IT-Ausschuss« zu seinem eigenen Organ zu machen – ganz abgesehen davon, dass der Vorwurf naheliegen könnte, damit würde die gesetzliche Arbeitsteilung zwischen Betriebsrat und GBR umgangen.

Nach § 80 Abs. 2 Satz 3 BetrVG kann der Betriebsrat vom Arbeitgeber verlangen, dass er ihm sachkundige Arbeitnehmer als Auskunftspersonen zur Verfügung stellt, soweit dies für die ordnungsgemäße Erfüllung seiner Aufgaben erforderlich ist. Zur Sachkunde gehört es auch, Informationen über den Einsatz technischer Systeme vermitteln zu können. Fraglich ist allein, ob auch der GBR Auskunftspersonen heranziehen kann. § 51 BetrVG verweist nicht direkt auf § 80 BetrVG, doch gelten nach seinem Abs. 5 die Rechte und Pflichten des Betriebsrats für den GBR entsprechend, soweit nichts Abweichendes bestimmt ist. Mit Recht hat daher das BAG dem GBR das Recht eingeräumt, entsprechend § 80 Abs. 3 BetrVG einen Sachverständigen heranzuziehen.[12] Dasselbe muss für innerbetriebliche Auskunftspersonen nach § 80 Abs. 2 Satz 3 BetrVG gelten.[13] Ihr spezifisches Wissen zu nutzen, kann die eher kostenträchtige Heranziehung von Sachverständigen sogar überflüssig machen.

Auskunftspersonen des GBR können auch Betriebsratsmitglieder aus Betrieben sein, wo Probleme des Technikeinsatzes bestehen. Daneben kann es einzelne Spezialisten geben, die mit Zustimmung des Betriebsrats Anlaufstelle für Wünsche und Beschwerden der Beschäftigten sind. Der Weg über § 80 Abs. 2 Satz 3 BetrVG erweitert die Ressourcen des GBR, ändert jedoch nichts daran, dass die Entscheidungszuständigkeit bei einem von den Betroffenen recht weit entfernten Gremium verbleibt. Soweit Harmonie herrscht, kann diese Tatsache völlig in den Hintergrund treten: Folgt der GBR praktisch immer den von »unten« kommenden Vorschlägen, kommt dies einer Mitbestimmung auf örtlicher Ebene sehr nahe. Sind die Verhältnisse andere, bleibt es bei vermeidbaren Konflikten.

Hilfslösung 3: Administrative Unterstützung für den GBR

Einen weiteren Ausweg zeigte das BAG im Fall eines großen Schichtbetriebs auf. Dem GBR war durch einen Einigungsstellenspruch die Zuständigkeit in Fragen der Schichtarbeit zugesprochen worden, wogegen er sich mit dem Argument wehrte, er sei gar nicht in der Lage, die ihm zugewiesenen Aufgaben zu erfüllen.[14] Das BAG meinte, die Einigungsstelle hätte in der Tat ein Verfahren vorsehen müssen, wie der Betriebsrat seinen Schutzauftrag erfüllen könne.[15] Die Überforderung der GBR-Mitglieder mache die Regelung jedoch nicht unwirksam: Nach § 40 Abs. 2 BetrVG habe der GBR gegen den Arbeitgeber einen Anspruch auf Überlassung von Büropersonal, »soweit dies zur Wahrnehmung seiner gesetzlichen Aufgaben erforderlich« sei. Das erfasse auch solche Hilfspersonen, die der (Gesamt-)Betriebsrat für die Vorbereitung und Abwicklung von Entscheidungen über die Wahrnehmung seiner Beteiligungsrechte benötige. Soweit sich die Mitbestimmung nicht auf eine einmalige Entscheidung, sondern auf einen Prozess bezieht, kann der Betriebsrat daher beispielsweise die Hilfe eines Informatikers in Anspruch nehmen.

Zeit für vernünftigen Pragmatismus

Alles Gesagte gilt entsprechend für das Verhältnis zwischen KBR auf der einen und GBR und Einzelbetriebsräten auf der anderen Seite. Dennoch bleibt die Frage: Wäre es nicht besser, wenn die Zuständigkeit von GBR/KBR von vornherein auf die Sachfragen beschränkt wäre, bei denen wirklich eine einheitliche Entscheidung erforderlich ist? Sollte man nicht wenigstens eine Delegierung zulassen? Vielleicht hat vernünftiger Pragmatismus ja doch eine Chance. ◁

Dr. Wolfgang Däubler,
Professor für Deutsches und Europäisches Arbeitsrecht, Bürgerliches Recht, Bremen.

3 BAG (Fn. 2).
4 Näher Däubler, DB 2017, 667, 668.
5 Wie hier DKKW-Trittin, 16. Aufl. 2018, § 50 Rn. 44; ablehnend GK-Kreutz/Franzen, BetrVG, 11. Aufl. 2018, § 50 Rn. 46.
6 Zum Folgenden s. auch Däubler, DB 2017, 667, 669, wo dieselben Probleme in Bezug auf Schichtarbeit erörtert werden.
7 BAG (Fn. 2): »Dabei konnte vorliegend dahinstehen, ob Gesamtbetriebsrat und Arbeitgeber befugt sind, eine mitbestimmte Angelegenheit zwar zu regeln, zugleich aber – zumindest in dem Umfang, in dem auch eine Übertragung der Entscheidung auf den Arbeitgeber zulässig wäre – im Wege einer Öffnungsklausel eine freiwillige Regelung durch Arbeitgeber und örtliche Betriebsräte zu ermöglichen.«
8 Kreutz/Franzen (Fn. 5), § 50 Rn. 46 a. E.
9 Das Beispiel lässt sich auf die Smartphone-Epoche übertragen: Im einen Betrieb muss man es immer dabei haben, im anderen nicht.
10 Dies folgt aus der Verweisung des § 51 Abs. 1 Satz 1 auf § 28 Abs. 1 Satz 3, der seinerseits auf § 27 Abs. 2 Satz 2 BetrVG verweist. Dort ist der Abschluss von Betriebsvereinbarungen ausdrücklich ausgenommen.
11 DKKW-Trittin, § 51 Rn. 38.
12 BAG, DB 2010, 43 Tz. 26.
13 Ebenso Fitting (Fn. 1), § 80 Rn. 81.
14 BAG, NZA 2012, 1237, 1238 links unten.
15 BAG, a.a.O. Tz 26.

Privacy Shield im Arbeitsverhältnis

DATENTRANSFER *Was können Betriebsräte tun, wenn die Übermittlung von Beschäftigtendaten in die USA gegen europäische Grundrechte verstößt? Die Regelungen des sogenannten Privacy Shield sollten Abhilfe schaffen, zeigen aber deutliche Defizite. Experten sprechen sich für eine arbeitsgerichtliche Überprüfung aus.*

VON **THILO WEICHERT**

DARUM GEHT ES

1. Transfers von Beschäftigtendaten aus Europa in die USA sind an der Tagesordnung.

2. »Privacy Shield« sollte dagegen Schutzmechanismen schaffen und enthält Spezialregelungen für Personaldaten.

3. Doch massive Datenschutzdefizite existieren weiterhin. Alternativen sind derzeit nicht in Sicht.

Transfers von Beschäftigtendaten aus Europa in die USA sind an der Tagesordnung, zumal viele hiesige Unternehmen US-Mütter oder Tochterunternehmen haben, oft eine zentralisierte oder arbeitsteilige Personaldatenverarbeitung erfolgt und US-Cloud-Dienste genutzt werden. Nachdem der Europäische Gerichtshof (EuGH) mit Urteil vom 6.10.2015 den Safe-Harbor-Rechtsrahmen zur Daten-Übermittlung in die USA aufhob,[1] beschloss die EU-Kommission am 12.7.2016 ein »EU-U.S.-Datenschutzschild« (künftig Privacy Shield).[2] Viele Juristen und Datenschützer sind überzeugt, dass auch dieser Beschluss zum Datentransfer in die USA gegen europäische Grundrechte verstößt. Für Beschäftigte, Betriebsräte und Arbeitgeber stellt sich so die Frage: »Was tun?«

Rechtliche Grundlagen

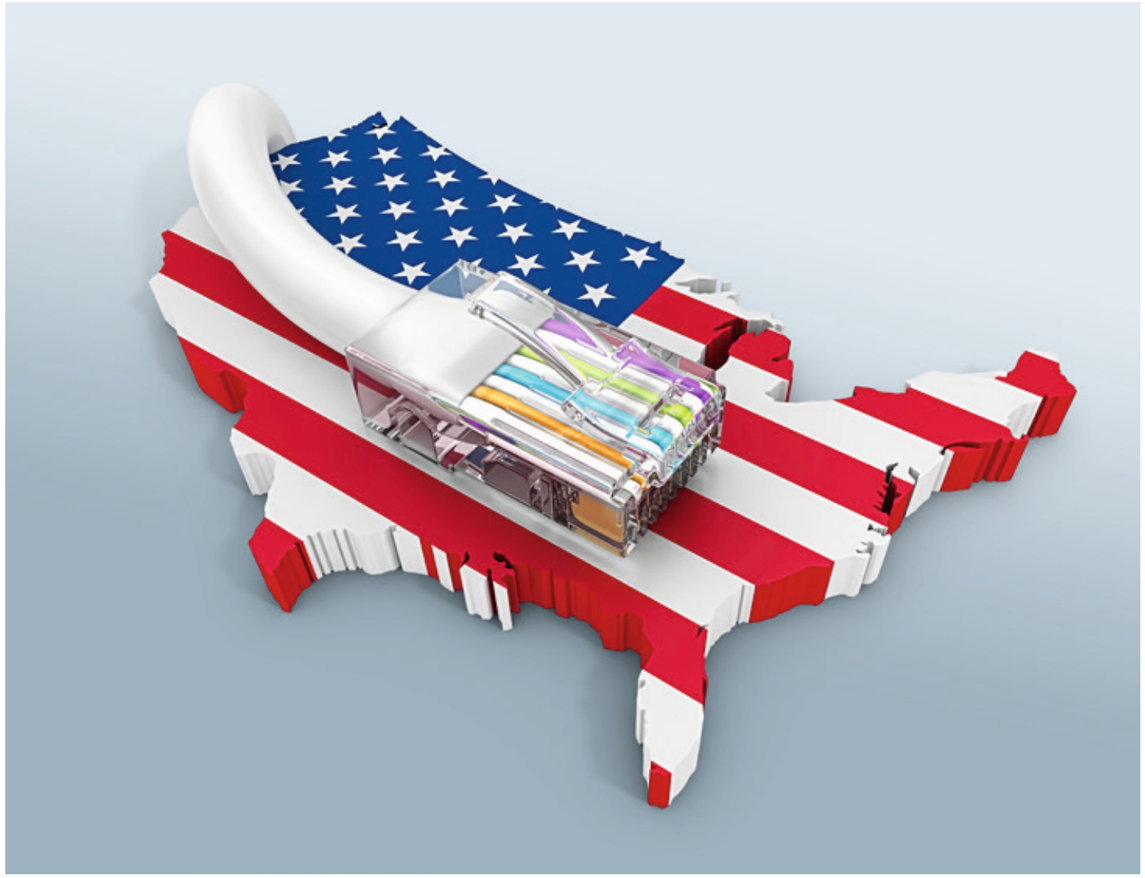
Auf europäischer Ebene gilt seit 2009 die Europäische Grundrechte-Charta (GRCh). Art. 7 GRCh schützt das Recht auf Vertraulichkeit der Kommunikation, Art. 8 GRCh garantiert den Menschen, dass ihre Daten nach Treu und Glauben für festgelegte Zwecke verarbeitet werden. Jede Person hat ein Recht auf Auskunft über ihre Daten. Die Einhaltung des Datenschutzes muss von einer unabhängigen Stelle überwacht werden. Art. 47 GRCh gibt eine Rechtsschutzgarantie. Dieser Schutz soll nicht nur innerhalb eines Staates oder innerhalb der Europäischen Union (EU) gelten, sondern auch bei grenzüberschreitenden Datenflüssen. Dieses Grundprinzip wurde 1995 von der Europäischen Datenschutzrichtlinie (EG-DSRl) dadurch normiert, dass die Übermittlung in Drittstaaten nur erlaubt wurde, wenn »dieses Drittland ein angemessenes Schutzniveau gewährleistet«, was die EU-Kommission feststellen kann (Art. 25 EG-DSRl). Einen solchen Beschluss fällte die EU-Kommission am 26.7.2000 in Bezug auf die USA, wenn sich das jeweilige US-Unternehmen im Rahmen des dort festgehaltenen Safe-Harbor-Regelwerks zur Beachtung bestimmter Datenschutzgrundsätze selbst verpflichtet.[3] Eine solche Selbstverpflichtung hatten 2015 ca. 4.400 US-Unternehmen abgegeben, darunter auch sämtliche großen IT-Unternehmen in den USA (Google, Facebook, Microsoft, Amazon, Salesforce). Eine derartige Selbstzertifizierung erfolgte auch von vielen US-Mutterunternehmen mit Töchtern in der EU in Bezug auf die Verarbeitung von Beschäftigtendaten. Dank Safe Harbor war so der Datentransfer von der EU in die USA aus Datenschutzgründen faktisch nicht beschränkt.

Mit Urteil vom 6.10.2015 stellte der EuGH fest, dass der Safe-Harbor-Rechtsrahmen gegen Art. 7, 8 und 47 GRCh verstößt und deshalb die Safe-Harbor-Entscheidung der EU-Kommission aufgehoben wird.[4]

Diese Rechtsprechung des EuGH fand Eingang in die kurz danach erfolgte Beschlussfassung zur Europäischen Datenschutz-Grundverordnung (DSGVO),[5] die am 25.5.2016 in Kraft trat und vom 25.5.2018 an die bisherige EG-DSRl ablöst. Gemäß Art. 44 DSGVO darf bei einer Übermittlung ins Drittland das durch die DSGVO »gewährleistete Schutzniveau für natürliche Personen nicht untergraben« werden. Art. 45 DSGVO sieht vor, dass die Kommission dies für ein Drittland, beispielsweise die USA, feststellen kann, wobei nach Abs. 2 hierfür folgende Kriterien zu berücksichtigen sind: Rechtsstaatlichkeit, Achtung der Menschenrechte und Grundfreiheiten, auch in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit sowie die wirksame Funktionsweise unabhängiger Aufsichtsbehörden. Als weitere Rechtfertigung für Datentransfers ins Drittausland werden die ebenso von der Kommission zu beschließenden Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c DSGVO) sowie von Aufsichtsbehörden zu genehmigende »verbindliche interne Datenschutzvorschriften« (Binding Corporate Rules, Art. 47 DSGVO) anerkannt.

Privacy Shield

Es ist schon lange klar, dass in den USA generell kein den europäischen Standards entsprechendes Datenschutzniveau besteht,[6] weshalb auch der EuGH den Safe-Harbor-Beschluss der EU-Kommission aufhob. Bei dem Privacy Shield handelt es sich nicht um ein internationales Abkommen,[7] sondern um einen von der EU-Kommission vorgenommenen einseitigen Rechtsakt, der auf Selbstverpflichtungen basiert, sich an die darin formulierten Regeln zu halten und der für politische Amtsträger der US-Administration sowie für sich selbst zertifizierende Daten verarbeitende Stellen gilt.



Nach dem Privacy Shield dürfen Daten aus Beschäftigungsverhältnissen nur an selbstzertifizierte US-Unternehmen übermittelt werden, die mit dem Arbeitergeber ökonomisch verbunden oder als Dienstleister tätig sind.

1 EuGH 6.10.2015 – C-362/14, NJW 2015, 3151 = JZ 2016, 360.
2 Durchführungsbeschluss (EU) 2016/1250 der EU-Kommission v. 12.7.2016 gemäß der Richtlinie 95/46/EG über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes, ABl. EU v. 1.8.2016, L 207.
3 Entscheidung 2000/520/EG, ABl. EG v. 25.8.2000, L 215/7.
4 EuGH (Fn. 1).
5 Verordnung (EU) 2016/679 v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 v. 4.5.2016, 1 ff.
6 Weichert, RDV 2012, 113; Däubler, Gläserne Belegschaften? 7. Aufl. 2017, Rn. 504; Schantz in Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 767.
7 Von Lewinski in Auernhammer, DSGVO/BDSG, 5. Aufl. 2017, Art. 96 DSGVO Rn. 7.

Diese Stellen werden vom US-Handelsministerium in einer Datenschutzschild-Liste eingetragen.[8] Grundlage des insgesamt 111 Seiten umfassenden Privacy-Shield-Beschlusses mit 155 Erwägungsgründen ist – wie bei Safe Harbor – ein Grundsatztext mit Anhängen und Briefen von US-Amtsträgern. Dieser Rechtsrahmen ist unklar strukturiert und formuliert, in mancher Hinsicht widersprüchlich und selbst für Spezialjuristen nur sehr schwer zu erfassen. Wie bei Safe Harbor verpflichten sich US-Unternehmen in einer Selbstzertifizierung, dass ihre »Datenschutzbestimmungen den Grundsätzen des Datenschutzschildes entsprechen«. Materiell-rechtlich bleibt das Privacy Shield hinter den europäischen Standards zurück: Wie bei Safe Harbor gibt es keine festen Normen, sondern Grundsätze: 1. Informationspflicht, 2. Wahlmöglichkeit, 3. Verantwortlichkeit bei der Weitergabe, 4. Sicherheit, 5. Datenintegrität und Zweckbindung, 6. Auskunftsrecht, 7. Rechtsschutz, Durchsetzung und Haftung. Für die Durchsetzung sind Rechtsbehelfe für die Betroffenen vorgesehen, die weder transparent noch praktikabel sind. Es ist daher klar: Das Privacy Shield genügt den Angemessenheitsanforderungen des europäischen Datenschutzrechts nicht.[9]

Spezialregelung für Personaldaten

Die Regeln zum Transfer von Beschäftigtendaten, vom Privacy Shield »Personaldaten« genannt, scheinen auf den ersten Blick stringenter und konkreter.[10] Danach dürfen Daten aus Beschäftigungsverhältnissen nur an selbstzertifizierte »Organisationen« (US-Unternehmen) übermittelt werden, die mit dem Arbeitgeber ökonomisch verbunden oder als Dienstleister tätig sind. Unter den Zusatzgrundsätzen ist unter 6 lit. c die Selbstzertifizierung geregelt, wonach US-Unternehmen einer gesetzlichen Aufsichtsbehörde erlauben müssen, »Beschwerden gegen die Organisation aufgrund der Verarbeitung von Personaldaten entgegenzunehmen« und mit dieser »Datenschutzbehörde in der EU zusammenzuarbeiten und den Empfehlungen dieser Behörden nachzukommen«. Sie müssen zudem dem US-Handelsministerium ihre »Datenschutzbestimmungen für Personaldaten« übermitteln sowie angeben, wo »diese von den betroffenen Mitarbeitern eingesehen werden können«.[11] »Die Rechtsvorschriften des EU-Mitgliedsstaats, aus dem sie stammen, sollen vor der Übermittlung anwendbar (9.a.i.). Dann heißt es weiter: »Sämtliche nach diesen Rechtsvorschriften geltenden Bedingungen und Beschränkungen der Übermittlung müssen beachtet werden.« Dieser etwas unklar formulierte Halbsatz soll offenbar auch für den Importeur gelten, der damit die vom nationalen Arbeits- und Datenschutzrecht vorgegebenen Verarbeitungsbedingungen beachten muss.

Die Zweckbindung der Daten soll aufgehoben werden können, wenn den Grundsätzen der Informationspflicht und Wahlmöglichkeit entsprochen wurde (9.b.i.). Damit wird beispielsweise die Datenauswertung durch eine US-Konzernmutter erlaubt, wenn der Beschäftigte dem nicht, nach entsprechender Information, widersprochen hat. Nur bei der Weiterverarbeitung von sensitiven Daten, zum Beispiel über die Gesundheit, wird die Zweckänderung darauf beschränkt, dass der Betroffene »die ausdrückliche Zustimmung« (Opt-in) erteilt hat. Auch hinsichtlich sensitiver Daten ist kein »Opt-in« nötig, wenn dies »zur Erfüllung der arbeitsrechtlichen Pflichten der Organisation notwendig ist« (Grundsätze III.1.a.). Unter Grundsätze III. 9.b.i. Satz 4 heißt es dann: »Macht ein Beschäftigter von seinem Recht Gebrauch, die Erlaubnis zu versagen, darf das keine Minderung seiner Berufschancen und keine Sanktionen gegen ihn zur Folge haben.«

EU-Mitgliedstaaten sollen die Regelungsbefugnis haben, dass »die Nutzung der Daten für andere Zwecke … ausgeschlossen werden kann; solche Bedingungen müssen eingehalten werden« (9.b.ii.). Wenn das politisch gewollt wäre, könnte der deutsche Gesetzgeber also ein Weiterverarbeitungsverbot vorsehen. Weiter heißt es, dass »den individuellen Datenschutzbedürfnissen des Arbeitnehmers angemessen Rechnung zu tragen« sei, was beispielsweise durch Zugriffsbeschränkungen oder eine Pseudonymisierung bzgl. seiner Daten umgesetzt werden könnte (9.b.iii.). Einschränkungen bzgl. der Betroffenenrechte bestehen anlässlich von Beförderungen, Ernennungen und ähnlichen Personalentscheidungen (9.b.iv.). Dem Auskunftsrecht kann direkt durch die US-Organisation oder unter Einbeziehung des EU-Arbeitgebers entsprochen werden (9.c.).

Gemäß den Regeln zur Rechtsdurchsetzung (9.d.) bleibt der EU-Arbeitgeber als Exporteur nach einer Übermittlung an das US-Unternehmen rechtlich verantwortlich. Ein Betroffener kann sich daher an den Datenschutzbeauftragten des Arbeitgebers wenden und im Beschwerdefall an die für diesen zuständige Aufsichtsbehörde, selbst wenn die Entscheidung über die Weiterverarbeitung durch die US-Organisation getroffen wurde. Zitat Privacy Shield (9.d.i. Satz 4): »So lässt sich am ehesten klären, wie die einander überschneidenden Bestimmungen des Arbeitsrechts, der Tarifverträge und des Datenschutzrechts miteinander in Einklang zu bringen sind.« Das US-Unternehmen hat also »gegebenenfalls bei Untersuchungen der in der EU jeweils zuständigen Behörden mitzuwirken und deren Empfehlungen zu befolgen« (9.d.ii.).[12]

»Materiell-rechtlich bleibt das Privacy Shield hinter den europäischen Standards zurück.«

THILO WEICHERT

All dies wird dann aber wieder von Erwägungsgrund 40 des EU-Kommissions-Beschlusses relativiert, wo von »unabhängiger alternativer Streitbeilegung oder im Privatsektor entwickelten Datenschutzprogramme, welche die Datenschutzgrundsätze inkorporieren«, die Rede ist.[13] Worauf sich diese Passage bezieht, ist unklar.

Eine Sonderregelung hat das Privacy Shield im Hinblick auf Beschäftigtendaten bei »operativen Erfordernissen« wie dem Buchen von Flügen, Hotelzimmern oder beim Abschluss von Versicherungen, doch müssen auch hier die Grundsätze der Informationspflicht und der Wahlmöglichkeit eingehalten werden.[14]

Behördenzugriffe

Ebenso wie bei sonstigen Datentransfers in die USA im nicht-öffentlichen Bereich bestehen bei Beschäftigtendaten große Datenschutzdefizite, wenn diese für behördliche Zwecke angefordert und verwendet werden.[15] Insofern gilt das allgemeine Regelwerk des Privacy Shield. Der Zugriff von Geheimdiensten ist de facto unbegrenzt und weitgehend unkontrolliert.[16]

Der Nutzung von bei US-Unternehmen beschafften Beschäftigtendaten wird kein verfassungsrechtliches und kein hinreichendes gesetzliches Korrektiv entgegengesetzt.[17] Die Dokumente zum Privacy Shield behandeln ausführlich die Presidential Policy Directive (PPD) 28, die aber keine verbindlichen Vorgaben zur Beachtung des Verhältnismäßigkeitsgrundsatzes vorsieht und keine grenzenlosen Massendatensammlungen verhindert.[18] Anders als im europäischen Recht, das jede Form der Datenverarbeitung einschließlich der Erhebung und Nutzung unter Gesetzesvorbehalt stellt, konzentrieren sich die US-Regelungen auf die Speicherung und die Weitergabe. Keiner der vielen erwähnten Rechtsbehelfe gewährleistet effektiven Rechtsschutz vor einem unabhängigen Gericht in einem öffentlichen Verfahren,[19] wie es nicht nur in Art. 6 Abs. 1, Art. 8 EMRK, sondern selbst in den Art. 14 Abs. 1, Art. 17 des Internationalen Paktes über bürgerliche und politische Rechte von 1966 zur Pflicht gemacht wird. Daran änderte auch der Judicial Redress Act nichts, der zudem weiterhin Ausländer gegenüber US-Bürgern hinsichtlich des Rechtsschutzes diskriminiert.[20] Erst recht wird bei der geheimdienstlichen Verarbeitung jedes rechtsstaatliche Maß an Bestimmtheit, Transparenz und individuelle Abwehrmöglichkeit unterschritten.[21] Die zugesicherte Unabhängigkeit einer Ombudsperson ist rechtlich in keiner Weise abgesichert.[22] Im Safe-Harbor-Urteil hat der EuGH darauf hingewiesen, dass es gerade der unkontrollierte und übermäßige Behördenzugriff auf personenbezogene Daten ohne Rechtsschutzmöglichkeiten ist, der den Wesensgehalt der Grundrechte der Betroffenen verletzt. Es ist daher absehbar, dass auch der EU-Kommissions-Beschluss zum Privacy Shield vom EuGH aufgehoben werden wird.

Alternativen

Genügt das Privacy Shield nicht den Angemessenheitsanforderungen des europäischen Rechts, stellt sich die Frage, welche Alternativen hierzu bestehen. Zumeist keine Alternative ist die Einwilligung des Beschäftigten (Art. 49 Abs. 1 lit. a DSGVO), da es regelmäßig an der nötigen Freiwilligkeit und Widerrufbarkeit fehlen dürfte (§ 26 Abs. 2 BDSG 2018). Auch auf

8 EU-Kommissions-Beschluss (Fn. 2), ErwGr 14, 32, L207/3, 7; Weichert, ZD 2016, 211; diese Liste ist zu finden unter https://www.privacyshield.gov/list.
9 Börding, CR 2016, 440; Weichert, ZD 2016, 217; Prantl, DuD 2016, 351; Däubler (Fn. 7), Rn. 504d; Grau/Granetzny, NZA 2016, 405; Schreiber/Krohm, ZD 2016, 255; Schantz in Schantz/Wolff (Fn. 7), Rn. 770; kritisch auch Ritzmann/Hänig, K&R Beilage 1 zu Heft 9/2016, 43.
10 EU-Kommissions-Beschluss (Fn. 2) Anhang II Zusatzgrundsätze III.9. »Personaldaten«, L 207/59 f.
11 EU-Kommissions-Beschluss (Fn. 2) Anhang II Zusatzgrundsätze III 6, L207/55.
12 Weichert, ZD 2016, 210.
13 EU-Kommissions-Beschluss (Fn. 2), ErwGr 40, L 207/8, 9.
14 EU-Kommissions-Beschluss (Fn. 2) Anhang II Zusatzgrundsätze III.9. e., L 207/60.
15 Schantz in Schantz/Wolff (Fn. 7), Rn. 770.
16 Weichert, ZD 2016, 216.
17 Börding, CR 2016, 434, 437.
18 Weichert, ZD 2016, 212.
19 Ausführlich dazu Weichert in ZD 2016, 213 f., 216 f.
20 Börding, CR 2016, 435 f.
21 Börding, CR 2016, 437 f.
22 Börding, CR 2016, 439; vgl. Weichert, ZD 2016, 213, 216.

den Art. 49 Abs. 1 lit. c DSGVO, der auf die Erfüllung eines Vertrags abstellt, kann nur in Ausnahmefällen zurückgegriffen werden, z. B. weil die Verarbeitung zumeist auch in Europa stattfinden kann.[23]

Wie schon bisher die EG-DSRl erlaubt die DSGVO in Art. 46 Abs. 2 lit. c Standardvertragsklauseln und in Art. 47 verbindliche interne Datenschutzvorschriften (Binding Corporate Rules – BCRs).[24] Problematisch bleibt aber, dass darin bisher zumeist die im Urteil des EuGH formulierten Vorgaben nicht berücksichtigt sind. Das Problem des behördlichen Datenzugriffs auf Unternehmensdaten wird regelmäßig nicht adressiert. Gemäß den geltenden Standardvertragsklauseln muss der Datenimporteur erklären, dass er seines Wissens nach keinen Gesetzen unterliegt, die ihm die Verfolgung der vom Exporteur auferlegten vertraglichen Pflichten unmöglich machen.[25] Solche Gesetze gibt es aber in den USA. Die bisherigen Kommissionsgenehmigungen von Standardverträgen werden daher mittelfristig vom EuGH aufgehoben werden. Als Alternative hat das Netzwerk Datenschutzexpertise schon kurz nach dem EuGH-Urteil zu Safe Harbor einen Vorschlag für einen zwischen EU-Unternehmen und US-Unternehmen abzuschließenden Export-Import-Vertrag erarbeitet und veröffentlicht.[26] Hierbei handelt es sich um eine Weiterentwicklung der von der Kommission genehmigten Standardvertragsklauseln unter Berücksichtigung des Safe-Harbor-Urteils des EuGH.

Dessen Grundansatz liegt darin, dass die Verantwortlichkeit des Datenexporteurs nach dem Export bestehen bleibt und der Importeur sich diesem gegenüber zur Einhaltung des europäischen Datenschutzrechts verpflichtet und ihm gegenüber informationspflichtig ist. Der Importeur wird vertraglich u. a. zur Beachtung der Zweckbindung und der Verhältnismäßigkeit und zur Realisierung der Betroffenenrechte verpflichtet. Diese Verträge haben drittschützende Wirkung. Betroffene können also ihre Rechte gegenüber dem Exporteur geltend machen und über diesen eine unabhängige Datenschutzkontrolle bei der für diesen zuständigen Datenschutzaufsichtsbehörde initiieren sowie ihm gegenüber in Europa Rechtsschutz erhalten. Der relevante Unterschied zum Privacy Shield besteht darin, dass für den Fall des Verstoßes gegen Vertragspflichten wirksame Sanktionen vorgesehen sind. Nach Art. 6 des Export-Import-Vertrags werden vertragliche Haftungs- und Schadensersatzansprüche bei Verletzungen des Datenschutzes statuiert. Vorgesehen sind weiterhin die Aussetzung des weiteren Datenexports sowie bei einer Prognose weiterer wesentlicher Vertragsverstöße die vollständige Einstellung des weiteren Datenexportes.

Durch diese Regelungen werden auch nach europäischem Recht nicht-konforme Datenbeschaffungen von US-Behörden erfasst sowie Informationsverweigerungen des Importeurs, die mit US-Recht (sog. gag-orders, behördliches Redeverbot) begründet werden. Zwar lassen sich damit die Folgen unzulässiger Datenverarbeitungen nicht vollständig beseitigen, dies wird aber auch nicht von der DSGVO gemäß den Art. 44 ff. gefordert.

Das Datenschutzniveau in den USA entspricht nicht den europäischen Standards.

23 Dazu Grau/Granetzny, NZA 2016, 409; Arbeitspapier der Art.-29-Arbeitgruppe (WP) 114 v. 25.11.2005, S. 13; offener Nolan, NZA 2016, 45.
24 Däubler (Fn. 7), Rn. 507g ff.
25 Grau/Granetzny, NZA 2016, 408.
26 Weichert/Schuler, Export-Import-Standardvertrag, http://www.netzwerk-datenschutzexpertise.de/sites/default/files/entwurf_2016_01_exportimportvertrag_08.pdf; diess. Ein »Export-Import-Standardvertrag« für Drittlands-Datentransfer, DuD 2016, 386.

»Es ist an der Zeit, auch arbeitsgerichtlich überprüfen zu lassen, inwieweit das Privacy Shield den europäischen rechtlichen Vorgaben zur Verarbeitung von Beschäftigtendaten entspricht.«

THILO WEICHERT

Die Regelungen des Export-Import-Vertragsmusters lassen sich generell für Datenexporte in die USA nutzen. Sie können zur Grundlage für Binding Corporate Rules gemäß Art. 47 DSGVO verwendet werden (Art. 46 Abs. 2 lit. b DSGVO), für Verhaltensregeln nach Art. 40 DSGVO (Art. 46 Abs. 2 lit. e DSGVO) sowie für Zertifizierungen nach Art. 42 Abs. 2, mit denen geeignete Garantien für Drittlandsdatentransfers geboten werden (Art. 46 Abs. 2 lit. f DSGVO). In jedem Fall kann sich an dem Muster ein individueller Vertrag zwischen Exporteur und Importeur orientieren, der von der zuständigen Aufsichtsbehörde gem. Art. 46 Abs. 3 DSGVO zu genehmigen ist.[27] Ein Export-Import-Vertrag kann auch zur Grundlage für Kollektivvereinbarungen nach Art. 88 Abs. 1 DSGVO, also beispielsweise für eine Betriebsvereinbarung, genommen werden. Arbeitgeber sind gem. § 87 Abs. 1 Nr. 6 BetrVG zur Mitbestimmung verpflichtet, wenn ein IT-Verfahren geeignet ist, »das Verhalten oder die Leistung der Arbeitnehmer zu überwachen«.[28] Diese Voraussetzungen sind bei Datenübermittlungen ins Drittausland gegeben.

Betriebsräte und Beschäftigte, die die Rechtmäßigkeit der Verarbeitung der Beschäftigtendaten in den USA kontrollieren wollen, sollten zunächst die herangezogene Rechtsgrundlage erkunden. Wird hierfür das Privacy Shield angegeben, sollte anhand der Liste des Department of Commerce (DOC) geprüft werden, ob die Selbstzertifizierung noch valide ist.[29] Für die Verarbeitung von Beschäftigtendaten ist eine spezielle Selbstzertifizierung nötig, die mit HR (Human Resources) gekennzeichnet ist. Dann sollten die Datenschutzbestimmungen eingesehen werden; der Zugang hierzu muss gemäß Zusatzgrundsatz 6. Selbstzertifizierung (lit. c letzter Satz) allgemein eröffnet werden; die dazu nötigen Kontaktdaten finden sich auf der vom US-Handelsministerium geführten Privacy-Shield-Liste. Wird eine Anfrage oder Beschwerde innerhalb von 45 Tagen nicht beantwortet, sollte man sich an die für den Arbeitgeber zuständige Datenschutzbehörde wenden.

Arbeitsgerichtliche Überprüfung wichtig

Es ist wohl an der Zeit, auch arbeitsgerichtlich überprüfen zu lassen, inwieweit das Privacy Shield den europäischen rechtlichen Vorgaben zur Verarbeitung von Beschäftigtendaten entspricht. Bei der Internationalisierung solcher Anwendungen nehmen US-Unternehmen Spitzenpositionen ein. Der rechtlich inakzeptable niedrige Standard von Privacy Shield droht Vorbild für andere Drittländer zu werden. Das sollte nicht ohne Widerspruch hingenommen werden. ◁

Dr. Thilo Weichert, Netzwerk Datenschutzexpertise, Datenschutzbeauftragter des Landes Schleswig-Holstein (2004 – 2015).

27 Zur Niederlassungsproblematik bei Art. 46 Abs. 3 Däubler (Fn. 7), Rn. 507a.
28 Däubler (Fn. 7), Rn. 710 ff.
29 Im Netz abzurufen unter https://www.privacyshield.gov/list.

MEHR WISSEN

Eine ausführliche Darstellung des Privacy Shields aus Beschäftigtensicht, der Kritik hieran und der Alternativen sind zu finden unter **www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2017_privacyshield_personaldaten_fin.pdf**

Aktuelle BAG-Rechtsprechung

RECHTSPRECHUNG *Immer häufiger befasst sich das BAG mit dem Beschäftigtendatenschutz und dem Recht auf informationelle Selbstbestimmung. Die meisten Entscheidungen stärken dieses Recht, aber es gibt Fälle, bei denen gesetzliche Vorgaben wenig beachtet werden.*

VON **STEFAN BRINK**

DARUM GEHT ES

1. Bei Risiken und Gefahren sozialer Medien hat der Betriebsrat ein Wörtchen mitzureden.

2. Mit personenbezogenen Daten aus illegaler Spähsoftware lässt sich kein Kündigungsgrund beweisen.

3. Die Rechtsprechung zum BEM ist teilweise wechselhaft und sorgt somit für Diskussionen in der Praxis.

Schlagworte wie Arbeitswelt 4.0 und Big Data lassen erahnen, dass es das klassische Arbeitsverhältnis fast nicht mehr gibt. Das führt auch beim Bundesarbeitsgericht (BAG) zur Änderung seiner Rechtsprechungsthemen. Facebook, Google+ und Twitter werden längst nicht mehr nur von Privaten genutzt. Die Vorteile globaler Vernetzung, permanenter Erreichbarkeit und Präsenz möchten sich die meisten Unternehmen nicht entgehen lassen. Eine seriöse Facebook-Seite pflegt bestehende Geschäftskontakte und ermöglicht das Knüpfen neuer; das kann zur Gewinnsteigerung des Unternehmens beitragen.

Soziale Medien und die Arbeitswelt

Trotz dieser Vorteile dürfen Arbeitgeber die Risiken und mögliche Gefahren sozialer Medien nicht aus den Augen verlieren. Hierzu stellte das BAG kürzlich fest, dass der Betriebsrat zum Glück auch ein Wörtchen mitzureden hat (sog. Facebook-Beschluss):[1]

Die Konzernmutter eines lokalen Blutspendedienstes betrieb eine Facebook-Seite, bei der die Aktivitäten aller angehörigen Unternehmen dargestellt wurden. Ein Facebook-Nutzer konnte über die Funktion »Besucher-Beiträge« einen Post zu einer seiner Meinung nach nicht ordnungsgemäßen Behandlung durch einen Mitarbeiter hinterlassen. Der Beitrag war für alle Besucher der Facebook-Seite sichtbar. Der Konzernbetriebsrat berief sich insoweit auf sein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG und forderte den Arbeitgeber auf, die Facebook-Seite abzuschalten oder zumindest die Funktion »Besucher-Beiträge« zu deaktivieren. Das BAG entschied, dass die Bereitstellung der Funktion »Besucher-Beiträge« der Mitbestimmung des Betriebsrats unterliege. Eine vom Arbeitgeber betriebene Facebook-Seite, die es den Nutzern von Facebook ermöglicht, über die Funktion »Besucher-Beiträge« Postings zum Verhalten und zur Leistung von Arbeitnehmern einzustellen, sei eine technische Einrichtung, die zur Überwachung der Arbeitnehmer nach § 87 Abs. 1 Nr. 6 BetrVG bestimmt sei.[2]

Die Aussage des BAG muss für alle Fälle, bei denen Dritte sich auf Plattformen sozialer Medien gegenüber einer breiten Öffentlichkeit zum Verhalten oder zur Leistung einzelner Beschäftigter äußern können, Gültigkeit haben. Soziale Medien weisen im Unterschied zu herkömmlichen Kommunikationswegen eine besondere Qualität auf, sie machen Vorgänge weltweit zugänglich und sind häufig wertender Natur. Mit seiner Entscheidung geht das BAG einen Schritt in die richtige Richtung in Sachen Beschäftigtendatenschutz. Es bleibt nur zu hoffen, dass Betriebsräte solchen Maßnahmen nicht ohne Weiteres zustimmen.

Spähsoftware und Videoüberwachung: Beweisverwertungsverbot?

Im Beschäftigtendatenschutz wurde ein weiterer Meilenstein gelegt. Das BAG entschied: Mit personenbezogenen Daten aus illegaler Spähsoftware lässt sich kein Kündigungsgrund beweisen.[3] Eine Arbeitgeberin beschloss, das gesamte Surfverhalten ihrer Beschäftigten vollständig zu überwachen und informierte die Mitarbeiter entsprechend. Auf dem Dienst-PC des Klägers wurde deswegen ein Tool (sog. Keylogger) installiert, das sämtliche Tastatureingaben protokollierte und regelmäßig Bildschirmfotos (Screenshots) fertigte. Nach Auswertung der mithilfe des Keyloggers erstellten Dateien konnte dem Kläger nachgewiesen werden, den Dienst-PC zur Erledigung privater Angelegenheiten genutzt zu haben, weswegen er fristlos gekündigt wurde.

Der Arbeitnehmer hielt die Kündigung für rechtswidrig und das BAG gab ihm Recht. Nach Auffassung der Erfurter Richter ist der Einsatz eines Keyloggers rechtswidrig, wenn kein auf den Arbeitnehmer bezogener, durch konkrete Tatsachen begründeter Verdacht einer Straftat oder einer anderen schwerwiegenden Pflichtverletzung besteht.

Das BAG geht zu Recht von einem Beweisverwertungsverbot für die durch den Keylogger gewonnenen Erkenntnisse über die Privattätigkeit des Klägers aus, denn die Arbeitgeberin hat das Recht auf informationelle Selbstbestimmung des Arbeitnehmers in erheblicher Weise verletzt. Die Bedingung der Datenerhebung nach § 32 Abs. 1 Satz 2 Bundesdatenschutzgesetz (BDSG a.F.), nämlich ein zu dokumentierender, auf tatsächlichen Anhaltspunkten beruhender Verdacht einer im Beschäftigungsverhältnis begangenen Straftat durch einen Beschäftigten, lag offensichtlich nicht vor. Die von der Arbeitgeberin »ins Blaue hinein« veranlasste Maßnahme war daher rechtswidrig und durfte deswegen auch nicht gerichtlich verwertet werden.

Auch wenn es im Arbeitsrecht an Vorschriften zur prozessualen Verwertbarkeit rechtswidrig erlangter Beweise mangelt, ist die Erhebung von Beweismitteln, deren Erlangung gegen das BDSG verstoßen, ein wichtiges Indiz dafür, dass die Verwertung des Beweismittels durch das Gericht ein nicht zu rechtfertigender Eingriff in das Grundrecht auf informationelle Selbstbestimmung sein kann. Bei der Annahme von Beweisverwertungsverboten bleibt zu hoffen, dass das BAG auch in Zukunft an seiner Linie festhält – hier gibt es nämlich durchaus eine positive Entwicklung zu verzeichnen. In einer früheren Entscheidung hatte das BAG das Vorliegen eines Beweisverwertungsverbots noch verneint und sich dazu über die Grenzen des § 32 Abs. 1 Satz 2 BDSG hinweggesetzt.[4]

Das Bundesarbeitsgericht mit Sitz in Erfurt.

Eine Arbeitgeberin, die Inventurverluste feststellte, die nur von der eigenen Belegschaft stammen konnten, installierte eine verdeckte Videokamera. Der gegen zwei bestimmte Mitarbeiterinnen gerichtete Verdacht eines Diebstahls wurde durch die Videoaufzeichnung bestätigt und brachte einen sogenannten Zufallsfund zutage: Die Videosequenz zeigte, wie die Klägerin einen regulären Kassiervorgang manipulierte und der Kasse Geld entnahm. Folge war die fristlose Kündigung des Arbeitsverhältnisses.

Die Kündigungsschutzklage der Klägerin hatte damals vor dem BAG keinen Erfolg. Laut BAG durften die Vorinstanzen Zeugen zum Inhalt der (inzwischen gelöschten) Videosequenz vernehmen und das Beweisergebnis verwerten. Da gegen zwei konkrete Mitarbeiterinnen der Verdacht einer Straftat bestand, sei die Videoaufzeichnung ihnen gegenüber nach § 32 Abs. 1 Satz 2 BDSG zulässig. Die Maßnahme sei im Verhältnis zu den von der Videoaufzeichnung betroffenen weiteren Arbeitnehmern – hier der Klägerin – auch nach § 6b Abs. 1 Nr. 3 BDSG zulässig gewesen. Die weitere Verarbeitung und Nutzung der Videoaufzeichnung an sich sei dann wiederum für die Beendigung des Beschäftigungsverhältnisses mit der Klägerin erforderlich und somit nach § 32 Abs. 1 Satz 1 BDSG zulässig. Dabei beging das BAG jedoch einen entscheidenden Fehler, indem es die gesetzlichen Vorgaben aus § 32 Abs. 1 BDSG außer Acht ließ. Die Ansicht, dass eine verdeckte Videoüberwachung zur Aufdeckung von Straftaten von Beschäftigten nicht nur dann erfolgen darf, wenn sichergestellt sei, dass von ihr ausschließlich Arbeitnehmer betroffen sind, gegen die ein dokumentierter Verdacht einer während des Be-

1 BAG 13.12.2016 – 1 ABR 7/15.

2 1 ABR 7/15 Rn. 36.

3 BAG 27.7.2017 – 2 AZR 684/16.

4 BAG 22. 9. 2016 – 2 AZR 848/15.

MEHR WISSEN

Mehr zum Beschäftigtendatenschutz erfahren Sie im Ratgeber des LfDI Baden-Württemberg zum Beschäftigtendatenschutz

schäftigungsverhältnisses begangenen Straftat besteht, widerspricht dem eindeutigen Wortlaut von § 32 Abs. 1 Satz 2 BDSG: »eines« Beschäftigten, »der« Betroffene. Sieht das BAG das anders, hätte es die Entscheidung dem Bundesverfassungsgericht vorlegen müssen.[5]

Das Gericht hätte klären müssen, ob der Zufallsfund zulasten der Klägerin überhaupt entstanden wäre, wenn die Videoüberwachung zielgerichtet und verhältnismäßig auf die des Diebstahls verdächtigten Mitarbeiterinnen ausgerichtet worden wäre. Wäre das BAG von einer unzulässigen Datenerhebung ausgegangen, hätte es angesichts seiner jüngsten Entscheidung zur unzulässigen Erhebung personenbezogener Daten[6] mithilfe illegaler Spähsoftware ein Beweisverwertungsverbot annehmen müssen. Man sieht: Auch Bundesgerichte können dazulernen!

Datenerhebungsverweigerer gekündigt

Mit einer weiteren Entscheidung stellt das BAG die Interessen eines Nahverkehrsunternehmens leider zu Unrecht über die des Arbeitnehmers.[7]

Ein Busunternehmen setzte ein System ein, mit dessen Hilfe »Fahrereignisse« elektronisch ausgewertet werden können. Die abgeschlossene Betriebsvereinbarung sah die verpflichtende Teilnahme an dieser Maßnahme vor. Fährt ein Busfahrer zu hochtourig, überschreitet Leerlaufzeiten, bremst zu scharf oder fährt zu schnell, weist ihn eine Warnleuchte des Systems darauf hin. Alle Daten hierzu werden aufgezeichnet und gespeichert. Die Arbeitnehmer konnten zwischen einer personalisierten und bei »guter Führung« prämienbewährten und einer »anonymisierten« Variante wählen. Der Kläger weigerte sich am System teilzunehmen, wofür er nach Ausspruch dreier Abmahnungen die fristlose Kündigung kassierte.

Das BAG bestätigte die Kündigung. Unabhängig von der Wirksamkeit der Betriebsvereinbarung sei das System nach § 32 Abs. 1 Satz 1 BDSG zulässig. Nach Auffassung des Gerichts handle es sich bei den erhobenen und verarbeiteten Daten zwar um personenbezogene Daten, weil die Anonymisierung ohne besonderen Aufwand aufgehoben werden könne, die Datenerhebung und Verarbeitung seien jedoch für die Durchführung des Arbeitsverhältnisses erforderlich. Dies trifft jedoch nicht zu, da der Zweck des Systems, die Busfahrer zu einer vorausschauenden und sparsamen Fahrweise anzuhalten, auch durch gleich geeignete mildere Mittel hätte erreicht werden können. Schulungen oder begleitete Kontrollfahrten wären zur Zweckerreichung ausreichend gewesen.

Im Übrigen ist es eine gruselige Vorstellung, dass Gerichte es für denkbar halten, der Arbeitgeber könnte mal eben »Modernisierungsverweigerer« aussortieren – eine wirklich problematische Entscheidung des BAG!

Der Irrweg des Betrieblichen Eingliederungsmanagements

Die Rechtsprechung zum Betrieblichen Eingliederungsmanagement (BEM) ist leider teilweise wechselhaft und sorgt somit für Diskussionen in der Praxis. 2012 entschied das BAG noch, dass es erforderlich sei, dem Betriebsrat eine Namensliste aller Arbeitnehmer zu überlassen, denen ein BEM anzubieten ist.[8] Mit einer anonymisierten Unterrichtung ließen sich die aus § 84 Abs. 2 Satz 1 SGB IX (jetzt: § 167 Abs. 2 Satz 1 SGB IX) ergebenden Pflichten des Arbeitgebers nicht überwachen. Auf die Einwilligung des Betroffenen komme es nicht an.

Mit seiner neusten Entscheidung zur Mitbestimmung des Betriebsrats in Fragen des BEM hat das BAG von seiner früheren Rechtsprechung Abstand genommen und die Rechte des Betriebsrats geschmälert.[9] Das BAG legt dem Wortlaut des § 84 Abs. 2 Satz 1 SGB IX: »[…] klärt der Arbeitgeber mit der zuständigen Interessenvertretung […]« ein anderes Verständnis als in dem zuvor genannten Beschluss aus dem Jahr 2012 zugrunde. Nun hält es die Hinzuziehung des Betriebsrats nur mit dem Einverständnis des Arbeitnehmers für zulässig.[10] Dem ist zuzustimmen: Das Recht auf informationelle Selbstbestimmung der Betroffenen steht nur diesen selbst zu und wird durch den Betriebsrat zwar unterstützt, aber nicht stellvertretend wahrgenommen.

Insgesamt also Licht und Schatten bei der Rechtsprechung des BAG zum Beschäftigtendatenschutz – aber die Richtung stimmt. Die Datenschutzbehörden werden die Entwicklung weiter beobachten und stehen jedermann/-frau mit Rat und Tat zur Seite! ◁

Dr. Stefan Brink,
Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg.

5 Art. 100 Abs. 1 GG.
6 Vgl. BAG 27.7.2017 – 2 AZR 684/16.
7 BAG 17.11.2016 – 2 AZR 730/15.
8 BAG 7.2.2012 – 1 ABR 46/10.
9 BAG 22.3.2016 – 1 ABR 14/14.
10 BAG 22.3.2016 – 1 ABR 14/14, Rn. 11.

Rechte der Personalräte und DSGVO

DIENSTVEREINBARUNGEN *Die DSGVO und das BDSG 2018 sind nicht nur formal neue Regeln, die Personalräte beachten müssen. Sie beinhalten auch eine Vielzahl inhaltlich neuer Vorgaben. Diese führen in den bestehenden Dienstvereinbarungen zum Datenschutz oder im IT-Bereich zu einem erheblichen Anpassungsbedarf.*

VON **ACHIM THANNHEISER**

DARUM GEHT ES

1. DSGVO und BDSG 2018 haben erhebliche Auswirkungen auf Dienstvereinbarungen und Rahmen-IT-Dienstvereinbarungen.

2. Datenschutzmanagement und Datenschutz-Folgenabschätzung sind bisher nicht bekannte Verfahren, die eingeführt werden müssen.

3. Die Rechte der Beschäftigten sind erheblich ausgeweitet worden und müssen in den Dienstvereinbarungen abgebildet werden.

Die Neuregelungen im europäischen Datenschutzrecht greifen ab Mai 2018 und es stellt sich die Frage, was dies für Personalratsarbeit praktisch bedeutet.[1] Die Datenschutz-Grundverordnung der Europäischen Union (DSGVO) wurde im April 2016 beschlossen und gilt direkt. Sie ist komplex aufgebaut und enthält 99 Artikel und 173 Erwägungsgründe (Auslegungshilfen). Auch das Bundesdatenschutzgesetz vom 30.6.2017 (BDSG neu) wurde überarbeitet und tritt zum 25.5.2018 in Kraft. Der Beschäftigtendatenschutz in Art. 88 DSGVO regelt keine Details, sondern bestimmt, dass die Mitgliedstaaten durch Rechtsvorschriften (BDSG Bund und die Länder DSG) oder durch Kollektivvereinbarungen (also Dienstvereinbarungen) spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten bei der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorsehen können. In § 26 BDSG 2018 wurde dies realisiert. Danach ist die Verarbeitung personenbezogener Daten nur zulässig, wenn sie

- für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist oder
- wegen gesetzlicher Pflichten oder
- auf Basis tarifvertraglicher Regelungen oder
- aus Dienstvereinbarungen folgt oder
- zur Aufdeckung von Straftaten, nach Abwägung schutzwürdiger Interessen der Beschäftigten gegenüber Art und Ausmaß des Anlasses erforderlich ist

BDSG 2018 – Beschäftigte

Der Begriff der Beschäftigten wurde in § 26 Abs. 8 BDSG 2018 erweitert. Dies sind nun:

- Arbeitnehmerinnen und Arbeitnehmer
- Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher
- zu ihrer Berufsbildung Beschäftigte
- Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitanden)
- in anerkannten Werkstätten für behinderte Menschen Beschäftigte
- Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstegesetz oder dem Bundesfreiwilligendienstgesetz leisten
- Personen, die wegen ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten
- Beamtinnen und Beamte
- Richterinnen und Richter
- Soldatinnen und Soldaten
- Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis
- sowie Personen, deren Beschäftigungsverhältnis beendet ist

Dienstvereinbarungen

Dienstvereinbarungen sind weiterhin als Rechtsgrundlage für die Verarbeitung perso-

1 Dieser Beitrag basiert auf dem Vortrag im Rahmen der dtb-Tagung »Arbeit 4.0: Neue Regeln braucht das Land«.

nenbezogener Daten geeignet. Die Frage der Durchsetzbarkeit ist abhängig von den Mitbestimmungsrechten im Bund und in den Ländern. Diese Beteiligungsrechte sind sehr unterschiedlich ausgestaltet.[2]

Prüfpunkte für Dienstvereinbarungen

Die Dienstvereinbarungen zum Schutz personenbezogener Daten müssen den nachfolgenden Kriterien entsprechen:

▸ Transparenzgebot
Die Beschäftigten müssen klar erkennen und nachvollziehen können, ob, von wem und zu welchem Zweck ihre personenbezogenen Daten erhoben werden.

▸ Erforderlichkeit
Die Verarbeitung von Beschäftigtendaten muss für Zwecke der Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses nötig sein. Die Vereinbarung muss leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst sein.

▸ Verhältnismäßigkeitsgrundsatz
Die Verarbeitung ist erforderlich, wenn sie für Zwecke des Beschäftigungsverhältnisses geeignet ist, das mildeste aller dem Arbeitgeber zur Verfügung stehenden gleich effektiven Mittel ist und schutzwürdige Interessen des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegen.

▸ Betroffenenrechte
Betroffenenrechte, die den Beschäftigten zukommen, dürfen durch die Betriebs-/Dienstvereinbarung nicht begrenzt werden. Ein »Mehr« an Datenschutz ist zulässig, ein Absenken des Niveaus nicht.

Rahmen-IT-Dienstvereinbarung neu formulieren

Die oft bestehenden Rahmen-IT-Dienstvereinbarungen sind zu überarbeiten. Folgende Inhalte sind beispielweise neu zu formulieren:

▸ Gegenstand
Für die Beschäftigten sollte erkennbar sein, dass gerade durch diese Dienstvereinbarung der Umgang mit personenbezogenen Daten gestattet wird.

▸ Geltungsbereich
Der Beschäftigtenbegriff wurde erweitert:
- Azubi
- Trainee
- Leih-Arbeitnehmer
- Zeit-Arbeitnehmer
- Berater, wenn arbeitnehmerähnlich beschäftigt
- ausgeschiedene Beschäftigte

▸ Datenverarbeitung durch Dritte
Es ist sicherzustellen, dass diese Dritten durch Unterzeichnung einer Verpflichtungserklärung für Externe vor Erteilung der Zugriffsberechtigung an die Inhalte dieser Rahmen-IT-Dienstvereinbarung gebunden werden. Dazu hat eine Sicherung der Auskunftsrechte für Personalrat und für Beschäftigte zu erfolgen.

▸ Zugangsbeschränkungen
Zu klären sind: Wer hat zu welchen personenbezogenen Daten Zugang?

Wer kann sich Zugang »verschaffen« (beispielsweise Admin)? Dies gilt übrigens auch im Personalratsbüro!

▸ Straftaten
Die Verarbeitung personenbezogener Daten für Zwecke der Aufdeckung von Straftaten im Beschäftigungsverhältnis ist zulässig. Allerdings erst nach Abwägung der schutzwürdigen Interessen der Beschäftigten in Bezug auf Art und Ausmaß der Straftat.

▸ Rechte der Beschäftigten
Ziel ist die Wahrung des Transparenzgebots und Einhaltung der Informationspflichten des Arbeitgebers:
- Auskunftsrecht (Art. 15 DSGVO)
- Recht zur Datenberichtigung (Art. 16 DSGVO)
- Recht auf Löschung personenbezogener Daten (Art. 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
- Widerspruchsrecht (Art. 21 DSGVO)
- Recht auf »Vergessenwerden« (Art. 17 DSGVO)

▸ Informationspflicht
Die Dienststelle hat in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu informieren über die gespeicherten Daten, die Kontaktdaten der verantwortlichen Stelle und des Datenschutzbeauftragten, die Zwecke der Datenverarbeitung, die Empfänger der Daten, ggf. über die Übermittlung ins Ausland und die Speicherdauer; sie hat auf die Betroffenenrechte hinzuweisen und über Widerrufsrechte der Betroffenen aufzuklären.

▸ Rechte ehemaliger Beschäftigter
Ausgeschiedenen Beschäftigten steht der Anspruch auf Löschung zu, denn nach dem Ausscheiden der/des Beschäftigten hat sich der Zweck für die Erhebung erledigt.

▸ Datenschutzbeauftragte
Eine Aufgabenabgrenzung zum Personalrat wäre sinnvoll. Dazu sollte die Beschreibung der Zusammenarbeit bei der Datenschutz-Folgenabschätzung erfolgen. Schließlich sollten die Berichte der Datenschutzbeauftragten auch zum Personalrat gelangen.

▸ Personalrat
Die Sicherung des Informationsrechts ist zu beschreiben, ebenso der Informationsumfang (vollständig als Kontroll- und Informationsrecht zur Ausübung der Mitbestimmung, § 26 Abs. 1 Satz 1 BDSG 2018), ein Zugangsrecht zu IT-Bereichen, ein Einsichtsrecht in Dokumentationen, Server, Datenbanken und das Datenschutzmanagement der Dienststelle; und schließlich auch die Beteiligung oder Information bei Datenschutz-Folgenabschätzungen.

▸ Datenschutzmanagement
Dieses stellt sicher, dass personenbezogene Daten und vor allem »besondere Kategorien personenbezogener Daten« besonders zu schützen sind und der Zugang zu beschränken ist (Art. 9 DSGVO). Besondere Kategorien personenbezogener Daten beziehen sich auf
- rassische und ethnische Herkunft
- politische Meinung
- religiöse oder weltanschauliche Überzeugung
- Gewerkschaftszugehörigkeit
- genetische und biometrische Daten
- gesundheitliche Daten oder
- Daten zum Sexualleben oder der sexuellen Orientierung

»Dienstvereinbarungen sind weiterhin als Rechtsgrundlage für die Verarbeitung personenbezogener Daten geeignet.«

ACHIM THANNHEISER

Rahmen-IT-Dienstvereinbarungen sollten jetzt überarbeitet werden.

2 Siehe dazu Thannheiser, Möglichkeiten des Personalrats, Der Personalrat 4/2018, S. 8 ff.

Bei der Verletzung des Schutzes personenbezogener Daten sieht die DSGVO Geldbußen bis zu 20 Millionen Euro vor.

Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung wurde zwingend eingeführt (Art. 35 DSGVO, § 67 BDSG 2018). Sie ist durchzuführen bei Verwendung neuer Technologien oder bei Gefahren für die Grundrechte der Beschäftigten wegen der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung. Beispiele dazu:

1. Profiling- oder Scoringverfahren,
2. systematische Überwachung (z. B. Video),
3. biometrische Verfahren oder
4. systematische technisch basierte Bewertung persönlicher Aspekte von Personen.

Unzulässige Pauschalverweise

Eine häufig verwendete, aber ab Mai 2018 unzulässige Klausel zur Verarbeitung/Auswertung ist folgende: »Mit Ausnahme von Rechtsgrundlagen bzw. gesetzlichen Vorschriften durch die eingeführten beziehungsweise einzuführenden EDV-Systeme erfolgt keine individuelle personenbezogene Leistungs- oder Verhaltenskontrolle.« Darin liegt insbesondere ein Verstoß gegen das Transparenzverbot. Zu klären ist, welche Kontrollen erfolgen konkret, wann, wo, in welchem Umfang. Welche Rechtsgrundlagen oder gesetzlichen Vorschriften sind gemeint?

Zusammenarbeit mit Datenschutzbeauftragten

Der Verantwortliche (die Dienststelle) hat mit dem Datenschutzbeauftragten des Bundes (der Länder) zusammenzuarbeiten (§ 68 BDSG 2018), und zwar beispielsweise bei der Datenschutz-Folgenabschätzung. Ebenso ist eine Zusammenarbeit hinsichtlich der Meldepflichten sinnvoll. Im Falle einer Verletzung des Schutzes personenbezogener Daten hat der Verantwortliche (Dienststelle) unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde zu melden. Dies gilt dann nicht, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Vertretung betroffener Personen

Schließlich ist eine Zusammenarbeit auch für die Vertretung von betroffenen Personen sinnvoll. Künftig sind nicht nur der Personalrat, der Datenschutzbeauftragte der Dienststelle oder der Datenschutzbeauftragte des Landes oder des Bundes klagebefugt, sondern auch

- gemeinnützige Einrichtungen,
- Organisationen oder
- Vereinigungen, beispielsweise Verbraucherverbände.

Diese bündeln Beschwerden gegen einen Arbeitgeber, können Klageverfahren gegen Arbeitgeber führen und die Betroffenen vertreten. In der DSGVO sind Geldbußen bis zu 20 Millionen Euro vorgesehen.

Rechte der Beschäftigten erheblich ausgeweitet

Die DSGVO und das BDSG 2018 sind nicht nur formal neue Regeln, sie beinhalten auch inhaltlich neue Regeln, die in den bestehenden Dienstvereinbarungen und Rahmen-IT-Dienstvereinbarungen? zum Datenschutz oder IT-Bereich zu einem erheblichen Anpassungsbedarf führen. Datenschutzmanagement und Datenschutz-Folgenabschätzung sind bisher nicht bekannte Verfahren, die eingeführt werden müssen. Die Rechte der Beschäftigten sind erheblich ausgeweitet worden und müssen in den Dienstvereinbarungen abgebildet werden. ◁

Achim Thannheiser, Rechtsanwalt und Betriebswirt bei Rechtsanwälte Thannheiser und Koll., Hannover.
www.thannheiser.de

Datenschutz im Betriebsratsbüro

RECHTE UND PFLICHTEN *Betriebsräte haben im Rahmen des Mitbestimmungsverfahrens Zugriff auf eine Vielzahl von Unterlagen mit oft besonders sensiblen persönlichen Informationen über Beschäftigte. Daher ist die zeitnahe Umsetzung der neuen Datenschutzregelungen bei der Gremienarbeit und im Betriebsratsbüro besonders wichtig.*

VON **HAJO KÖPPEN**

Betriebsräte müssen sich in zweifacher Hinsicht um den Datenschutz kümmern. Zunächst haben sie, gemeinsam mit dem Arbeitgeber, nach § 75 Abs. 2 BetrVG »die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern« und nach § 80 Abs. 1 Nr. 1 BetrVG darüber zu »wachen, dass die zugunsten der Arbeitnehmer geltenden Gesetze, Verordnungen, Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen durchgeführt werden«. Dazu hat das Bundesarbeitsgericht bereits 1987 entschieden, dass das Bundesdatenschutzgesetz (BDSG) ein zugunsten der Arbeitnehmer geltendes Gesetz im Sinne von § 80 Abs. 1 Nr. 1 BetrVG ist.[1] Das gilt auch für die Europäische Datenschutz-Grundverordnung (DSGVO)[2] und das neue Bundesdatenschutzgesetz (BDSG 2018) vom 30.6.2017.[3] Neben der Erfüllung dieses Auftrags unterliegen Betriebsräte der Verpflichtung, für die datenschutzkonforme Verarbeitung von Beschäftigtendaten in ihrem Tätigkeits- und Verantwortungsbereich zu sorgen.

Zweckbindungsgrundsatz gilt auch für den Betriebsrat

Das gelingt nicht immer, wie Beispiele aus den Tätigkeitsberichten[4] der Aufsichtsbehörden für den Datenschutz zeigen. Etwa wenn ein Betriebsratsmitglied Beschäftigtendaten zweckentfremdet.[5] In seiner Funktion hatte ein Betriebsratsmitglied zulässigerweise Zugriff auf die Gehaltsdaten von Beschäftigten, um im Rahmen von Mitbestimmungsverfahren bei Eingruppierungen oder Gewährung sonstiger Gehaltsbestandteile Stellung nehmen zu können. Zu diesem Zweck durfte der Betriebsrat die Beschäftigtendaten nutzen. Bei der Datenschutzbehörde wurde angefragt, ob es datenschutzrechtlich zu beanstanden sei, wenn ein Betriebsrat, der zugleich Mitglied einer DGB-Einzelgewerkschaft ist, die Gehaltsdaten der Mitarbeiter, die ebenfalls Mitglied in der betreffenden Gewerkschaft sind, zur Überprüfung verwendet, ob diese ihren satzungsmäßigen Gewerkschaftsbeitrag zahlen. Da die Rechtslage eindeutig ist, fiel die Stellungnahme der Datenschutzbehörde entsprechend knapp aus: »Nutzt der Betriebsrat diese Gehaltsdaten zur Überprüfung, ob ein bestimmter Mitarbeiter seinen Gewerkschaftsbeitrag entrichtet hat, ist dies nicht mehr von dem gerechtfertigten Zweck umfasst und damit datenschutzrechtlich unzulässig.«

AUS DEM GESETZ

Artikel 5 Abs. 1 lit. b DSGVO
Personenbezogene Daten müssen (...)
für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (...) (»Zweckbindung«).

DARUM GEHT ES

1. Betriebsräte haben nicht nur den Arbeitgeber bei der Einhaltung der Persönlichkeits- und Datenschutzrechte von Beschäftigten zu überwachen.

2. Gleichzeitig müssen sie auch die datenschutzkonforme Verarbeitung von Beschäftigtendaten in ihrem Tätigkeits- und Verantwortungsbereich sorgfältig beachten.

3. Wichtig sind daher klare Regelungen für den Umgang mit Beschäftigtendaten und die notwendigen Kontrollen.

1 Zum BDSG alte Fassung (a.F.) BAG 17.3.1987 – 1 ABR 59/85, AiB 1987, 287.
2 Abgedruckt im Amtsblatt der Europäischen Union vom 4.5.2016, L 119, Seite 1 ff., abrufbar unter http://eur-lex.europa.eu.
3 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – EU-DSAnpUG) vom 30.6.2017, BGBl I 2017, S. 2097 ff.
4 Alle seit 1971 erschienen Tätigkeitsberichte sind abrufbar über www.zaftda.de.
5 6. Tätigkeitsbericht des Bayerischen Landesamtes für Datenschutzaufsicht (2013/14), Seite 110.

Datenleck bei Betriebsratswahl

Über ein Datenschutzleck bei einem Betriebsrat berichtete der Thüringer Landesbeauftragte für Datenschutz und Informationsfreiheit in seinem Bericht für die Jahre 2014/2015.[6] »Der Betriebsrat hat die Wahlakten mindestens bis zur Beendigung seiner Amtszeit aufzubewahren.« So lautet § 19 der Wahlordnung zum BetrVG. Während der Aufbewahrungszeit ist sicherzustellen, dass die Unterlagen gegen unbefugte Kenntnisnahme geschützt sind. In einem Eigenbetrieb eines Thüringer Landkreises wurde diese einfache Regel aber nicht eingehalten.

Nach einer Betriebsratswahl wurden die Wahlakten im Auftrag des Wahlvorstands unter Verschluss genommen und versiegelt und unter Versicherung, dass von den Unterlagen keine Kopien existieren, dem neuen Betriebsrat ausgehändigt. Dann wurde die Betriebsratswahl angefochten. Bei der Verhandlung vor dem Arbeitsgericht legte der neue Betriebsratsvorsitzende die versiegelten Wahlunterlagen dem Gericht vor, um dann festzustellen, dass das Gericht und alle Arbeitgebervertreter bereits im Besitz von Kopien eben dieser Unterlagen waren. Nachdem der Betriebsrat Strafantrag wegen der Veröffentlichung vertraulicher Unterlagen gestellt hatte, wandte er sich auch an den Landesdatenschutzbeauftragten. Der gab folgende Stellungnahme ab: »Wahlunterlagen enthalten personenbezogene Daten und dienen dazu, den Nachweis der ordnungsgemäßen Durchführung zu erbringen. Zum Zweck der Wahlanfechtung kann Einblick genommen werden.

Auch Unterstützungsunterschriften können zum Zweck der Einschätzung der Wirksamkeit überprüft werden, selbst wenn der Wahlvorstand ursprünglich irrtümlich gegenüber den unterzeichneten Unterstützern die Versicherung abgegeben hatte, dass die Unternehmensleitung davon nichts erfahre. (…) Unterlagen mit personenbezogenen Daten sind gegen unbefugte Kenntnis zu schützen. Die besten technischen und organisatorischen Maßnahmen gehen ins Leere, wenn eine befugte Person die Unterlagen bewusst pflichtwidrig anderen Personen zugänglich macht. Das unbefugte Zugänglichmachen kann als Straftat oder Ordnungswidrigkeit geahndet werden.«

Betriebsräte sollten sich jetzt zu den neuen Datenschutzregeln auch bei der Umsetzung im Betriebsratsbüro schulen lassen.

6 11. Tätigkeitsbericht, Thüringer Landesbeauftragte für Datenschutz und Informationsfreiheit (2014/15), Seite 172.

Einigungsstelle missachtet Persönlichkeitsrechte von Beschäftigten

Dass auch Einigungstellen nicht vor Verstößen gegen den Beschäftigtendatenschutz gefeit sind, zeigt ein Beschluss des Bundesarbeitsgerichts[7] (BAG) aus dem letzten Jahr. Die Einigungsstelle beschloss in einer Gesamtbetriebsvereinbarung die Durchführung einer »Belastungsstatistik« für die Außenstellen-Sachbearbeiter eines Versicherungsunternehmens, wonach durch technische Überwachungseinrichtungen neben der Anzahl der bearbeiteten Fälle und den Rückständen die einzelnen Arbeitsschritte im Detail aufgezeichnet, gespeichert und analysiert und bei Abweichungen dem Gruppenleiter angezeigt werden sollten. Für das BAG stellt eine solche Regelung, die »durch eine technische Überwachungseinrichtung i. S. d. § 87 Abs. 1 Nr. 6 BetrVG dauerhaft die Erfassung, Speicherung und Auswertung einzelner Arbeitsschritte und damit des wesentlichen Arbeitsverhaltens der Arbeitnehmer anhand quantitativer Kriterien während ihrer gesamten Arbeitszeit vorsieht«, einen schwerwiegenden Eingriff in das Persönlichkeitsrecht der Beschäftigten dar. Ein solcher Eingriff ist, so das BAG, nicht durch überwiegend schutzwürdige Belange des Arbeitgebers gedeckt.

Datenschutz-Verantwortung von Betriebsräten

Die aufgeführten Fälle zeigen, dass Betriebsräte nicht nur den Arbeitgeber bei der Einhaltung der Persönlichkeits- und Datenschutzrechte von Beschäftigten überwachen sollten, sondern auch grundsätzlich für die datenschutzkonforme Verarbeitung von Beschäftigtendaten in ihrem Tätigkeits- und Verantwortungsbereich Sorge tragen müssen.

Neben den Regelungen des Betriebsverfassungsgesetzes mit Erlaubnistatbeständen für die Weitergabe von Beschäftigtendaten durch den Arbeitgeber an den Betriebsrat zur Wahrnehmung von Informations-, Beteiligungs- und Mitbestimmungsrechten (etwa § 80 Abs. 2 Satz 2 BetrVG – Unterrichtungspflicht durch den Arbeitgeber und § 99 Abs. 1 BetrVG – Mitbestimmung bei personellen Einzelmaßnahmen) sind seit dem 25.5.2018 bei der Gremienarbeit auch die Vorgaben der DSGVO und des BDSG 2018 einzuhalten. Da die DSGVO sogenannte Öffnungsklauseln enthält (etwa in Art. 88 (Datenverarbeitung im Beschäftigungskontext)), war die Schaffung eines neuen BDSG zur Schließung der »Lücken« in der DSGVO erforderlich. Mit dem § 26 BDSG 2018 hat der Gesetzgeber die datenschutzrechtliche Grundlage für die »Datenverarbeitung für Zwecke des Beschäftigtenverhältnisses« geschlossen. Beide Normtexte, DSGVO und BDSG 2018, sind daher stets zusammen zu lesen.

Die Datenschutzgrundsätze

Wenn auch viel von einem »neuen« Datenschutzrecht die Rede ist, finden sich in der DSGVO neben einer Reihe von wirklich neuen rechtlichen Vorgaben eine Vielzahl aus dem »alten« Datenschutzrecht bekannte Begriffe und Grundsätze wieder. So gilt auch nach dem »neuen« Datenschutzrecht der Grundsatz des sogenannten Verbots mit Erlaubnisvorbehalt. Demnach ist die Verarbeitung personenbezogener Daten[8] nur zulässig, wenn eine Einwilligung der betroffenen Person vorliegt oder eine Rechtsvorschrift dies erlaubt. § 26 Abs. 2 BDSG 2018, der die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses regelt, ermöglicht ausdrücklich auch die Verarbeitung von Beschäftigtendaten auf der Grundlage einer Einwilligung des Arbeitnehmers, was bisher umstritten war. Allerdings ist die Verarbeitung von Beschäftigtendaten auf Grundlage einer Einwilligung durch Arbeitnehmer eine höchst labile Basis, da eine Einwilligung nach Art. 7 Abs. 3 DSGVO (Bedingungen der Einwilligung) jederzeit widerrufen werden kann. Daher wird eine Einwilligung durch den Arbeitnehmer für den Arbeitgeber regelmäßig nur dann Sinn machen, wenn der Arbeitnehmer dadurch einen »rechtlichen oder wirtschaftlichen Vorteil« erlangt. Etwa, wenn der Arbeitgeber Arbeitnehmern die Kita- oder Kindergartenkosten erstattet oder Gewerkschaftsbeiträge übernimmt. In diesen und vergleichbaren Fällen muss der Arbeitnehmer dem Arbeitgeber mehr persönliche Daten mitteilen, als es für Zwecke der »Durchführung des Beschäftigungsverhältnisses« erforderlich ist.

Wenn auch große Teile des § 26 BDSG 2018 wort- und inhaltsgleich mit dem § 32 BDSG a.F. sind, hat der Gesetzgeber jetzt im § 26 Abs. 1 Satz 1 BDSG 2018 ausdrücklich festgehalten, dass personenbezogene Daten von Beschäftigten für Zwecke des Beschäfti-

7 BAG 25.4.2017 – 1 ABR 46/15, AuR 2017, 465.

8 Definition siehe Art. 4 Nr. 1 DSGVO.

gungsverhältnisses verarbeitet werden dürfen, wenn dies »zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist«. Damit ist § 26 Abs. 1 BDSG 2018 als datenschutzrechtliche Grundlage für die Verarbeitung von Beschäftigtendaten durch Betriebsräte anzusehen,[9] wobei die einschlägigen Vorschriften des Mitbestimmungsrechts bestimmen, welche Beschäftigtendaten dem Betriebsrat zur Verfügung zu stellen sind.[10] Als Ermächtigung für die Weitergabe von Beschäftigtendaten durch den Arbeitgeber an den Betriebsrat ist § 80 Abs. 2 Satz 2 BetrVG i.V.m § 26 Abs. 1 BDSG 2018 anzusehen, der dem Betriebsrat das Recht auf Einsicht in Bruttolohn- und Gehaltslisten einräumt. Auch die Vorschrift des § 99 Abs. 1 BetrVG, wonach der Arbeitgeber dem Betriebsrat vor jeder Einstellung die erforderlichen Bewerbungsunterlagen vorzulegen hat, ist als Erlaubnistatbestand für die Weitergabe von Beschäftigtendaten anzusehen. Insgesamt enthält das BetrVG wenige Festlegungen und Aussagen zum Umgang mit Beschäftigtendaten durch den Betriebsrat. Soweit das BetrVG keine datenschutzrechtlichen Vorgaben macht, kommen Regelungen des BDSG 2018 und der DSGVO zum Zuge.

AUS DEM GESETZ

§ 26 Abs. 2 BDSG 2018
Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären.

Was der Betriebsrat beachten muss

Neben dem Verbot mit Erlaubnisvorbehalt und dem Grundsatz der Zweckbindung gilt auch weiterhin der bisher anzuwendende datenschutzrechtliche Grundsatz der Erforderlichkeit, in Art. 5 Abs. 1 lit. c DSGVO als Grundsatz der »Datenminimierung« bezeichnet. Danach müssen personenbezogene Daten »dem Zweck angemessen und erheblich und auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein«. Zusätzlich dürfen nach Art. 5 Abs. 1 lit. e DSGVO personenbezogene Daten nach der sogenannten Speicherbegrenzung ausschließlich »in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist«. Nach Art. 17 Abs. 1 lit. a DSGVO sind personenbezogene Daten unverzüglich zu löschen, wenn sie für die Zwecke, für die sie verarbeitet werden, nicht mehr notwendig sind.

Aus dem Grundsatz der Erforderlichkeit ergibt sich, dass Arbeitgeber und Betriebsrat die Frage klären müssen, welche Beschäftigtendaten im Rahmen von Mitbestimmungsverfahren durch den Arbeitgeber an den Betriebsrat weitergegeben werden dürfen. So hat das Bundesverwaltungsgericht zum Beispiel entschieden, dass ein Personalrat nicht verlangen kann, »dass ihm die in der elektronischen Arbeitszeiterfassung gespeicherten Daten unter Namensnennung der Beschäftigten zur Verfügung gestellt werden«, da er seine Überwachungsaufgabe bereits effektiv wahrnehmen kann, wenn er zunächst nur die anonymisierten Arbeitszeitlisten erhält.[11] Auf der anderen Seite haben Gerichte aber auch entschieden, dass Unterlagen, die ein Personalrat zur Wahrnehmung seiner Beteiligungsrechte immer wieder benötigt, in Kopie auf Dauer überlassen werden können.[12] So ist durch arbeitsgerichtliche Rechtsprechung beispielsweise entschieden, dass ein Arbeitgeber auch ohne Zustimmung der Betroffenen verpflichtet ist, dem Betriebsrat die Arbeitnehmer namentlich zu benennen, die innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig waren.[13]

9 Vgl. Eder, CuA 4/2018, 9.
10 Vgl. Maschmann in Kühling/Buchner, § 26 BDSG Rn. 53.
11 BVerwG 19.3.2014 – 6 P 1.13; PersR 1/2015, 48; kritisch dazu Däubler, PersR 1/2015, 26.
12 BVerwG 4.9.1990 – 6 P 28/87.
13 BAG 7.2.2012 – 1 ABR 46/10.

Der Bayerische Landesdatenschutzbeauftragte weist am Beispiel eines Personalrats darauf hin, dass dieser aufgrund der Beschwerde eines Beschäftigten erhaltene persönliche Informationen nur soweit und so lange aufbewahren darf (etwa in einem gesonderten Ordner) wie es für die Behandlung der Beschwerde durch den Personalrat unbedingt erforderlich ist.[14] Ferner wird ausgeführt: »In diesem Zusammenhang ist allerdings zu beachten, dass mit Ablauf der Amtszeit des Personalrats die rechtliche Existenz und die Befugnisse des Personalrats enden. Spätestens zu diesem Zeitpunkt sind daher die im Rahmen der Behandlung der Beschäftigtenbeschwerde durch den Personalrat angefallenen personenbezogenen Daten zu löschen.« Längere Fristen für die Aufbewahrung von Betriebsratsunterlagen bestehen für Sitzungsniederschriften nach § 34 BetrVG. Die Dauer der Aufbewahrung der Niederschriften ist im BetrVG zwar nicht geregelt, aus ihrem Zweck als Beweis- und Informationsmittel sollten sie aber mindestens für die Dauer der Amtszeit des Betriebsrats aufbewahrt werden. Soweit sie zum Nachweis fortwirkender Beschlüsse des Betriebsrats erforderlich sind, können Niederschriften auch länger aufbewahrt werden. Sitzungsniederschriften dürfen so lange aufbewahrt werden, wie ihr Inhalt von rechtlicher Bedeutung ist.[15]

Daten aufbewahren oder schreddern?

Soweit ein Betriebsrat zulässigerweise Beschäftigtendaten in Ausübung seiner Mitbestimmungsrechte verwendet, muss er eindeutig festlegen (etwa in einer internen Geschäftsordnung zum Datenschutz) wie durch technische und organisatorische Maßnahmen sichergestellt wird, dass Beschäftigtendaten nur so lange in seinem Verantwortungsbereich verbleiben, wie es für die Mitbestimmungszwecke unbedingt erforderlich ist. So sind nach Abschluss eines Mitbestimmungsverfahrens durch entsprechende Beschlüsse die dem Betriebsrat in diesem Zusammenhang zur Verfügung gestellten personenbezogenen Beschäftigtendaten zu löschen oder die überlassenen Unterlagen dem Arbeitgeber zurückzugeben. Eine nicht für einen konkreten Anlass erforderliche, ständige Aufbewahrung von Unterlagen und dauernde Speicherung geschützter Beschäftigtendaten über den Abschluss von Beteiligungsverfahren hinaus sind unzulässig und daher rechtswidrig. Bei der Vernichtung von Papierunterlagen, die für die Aufgabenerfüllung nicht mehr erforderlich sind, sollte das Betriebsratsbüro mit einem Aktenvernichter ausgestattet sein, der mindestens die Sicherheitsstufe 4 der DIN 66399[16] erfüllt.

Ohne konkreten Anlass dürfen Beschäftigtendaten auch im Betriebsratsbüro nicht ständig aufbewahrt werden.

14 26. Tätigkeitsbericht des LfD Bayern, S. 236.
15 BAG 30.9.2014 – 1 ABR 32/13.
16 Siehe dazu Flyer der TH Mittelhessen unter: www.thm.de/datenschutz/veroeffentlichungen/flyer-datenschutz-tipps.html.

Datensicherheit und Datenschutzschulung

Eine gesetzeskonforme Verwendung von Arbeitnehmerdaten durch den Betriebsrat erfordert auch die Einhaltung der mit Art. 32 DSGVO (Sicherheit der Verarbeitung) geforderten technischen und organisatorischen Maßnahmen (TOM), um ein angemessenes Schutzniveau für die verarbeiteten Beschäftigtendaten zu realisieren. Als Maßnahmen werden »Pseudonymisierung« und »Verschlüsselung« sowie die Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Daten genannt. Betriebsräte haben für ihren Verantwortungsbereich technisch-organisatorische Maßnahmen[17] gegen den Missbrauch von Daten eigenständig und nach pflichtgemäßem Ermessen umzusetzen.[18] Sie haben sich daher eigenverantwortlich mit der IT-Struktur des Betriebsrats, den Zugriffsberechtigungen, einer eventuell erforderlichen Datenverschlüsslung und mit Backup-Verfahren zu befassen.[19] Auch um die Datenschutzunterrichtung und -schulung der Betriebsratsmitglieder muss sich der Betriebsrat kümmern.

Wer den Datenschutz beim Betriebsrat kontrolliert

Hinsichtlich der Datenverarbeitung von Beschäftigtendaten im Betrieb darf und muss der Betriebsrat den Arbeitgeber kontrollieren. Aber wer überwacht, ob der Betriebsrat datenschutzkonform mit den ihm auf der Grundlage des BetrVG anvertrauten Beschäftigtendaten umgeht? Der Arbeitgeber darf es nicht, und der betriebliche Datenschutzbeauftragte auch nicht. Schon 1997 hatten sich die BAG-Richter dagegen ausgesprochen, dass der Betriebsrat der Kontrolle des betrieblichen Datenschutzbeauftragten unterliegt.[20] Für das BAG ist ein Kontrollrecht des betrieblichen Datenschutzbeauftragten mit der vom BetrVG vorgeschriebenen Unabhängigkeit des Betriebsrats vom Arbeitgeber nicht vereinbar. Dem BDSG a.F. ist – nach Auffassung der Richter – ein so massiver und wertungswidersprüchlicher Eingriff in ein Strukturprinzip des BetrVG nicht zu entnehmen. Das BAG begründet das damit, dass der betriebliche Datenschutzbeauftragte vom Arbeitgeber ohne die Mitbestimmung des Betriebsrats bestellt wird. Somit könne der Betriebsrat nicht mit dafür sorgen, dass ein Beauftragter bestellt wird, der auch das Vertrauen des Betriebsrats genießt. Nach der Konzeption des BDSG a.F.,[21] so das Gericht, ist der betriebliche Datenschutzbeauftragte »ein Instrument der Selbstkontrolle des Unternehmens« und somit als eine Art Gewährsmann des Arbeitgebers anzusehen, auch wenn er bei der Ausübung seiner gesetzlichen Pflichten von Weisungen des Arbeitgebers frei ist.

Lediglich die Aufsichtsbehörden für den Datenschutz, also die Landesdatenschutzbeauftragten,[22] sind befugt, die Beschäftigtendatenverarbeitung im Betriebsratsgremium zu kontrollieren. Daneben bleibt nur die Selbstkontrolle des Betriebsrats in Sachen Datenschutz. Daher sollten Betriebsräte ein Mitglied des Gremiums zum/r »Sonderbeauftragten« für den Beschäftigtendatenschutz benennen, das sich um alle Datenschutzaufgaben und -fragen bei der Betriebsratsarbeit kümmert und in dieser Funktion auch als Ansprechpartner für die Aufsichtsbehörde, den Arbeitgeber und für die Beschäftigten bei Datenschutzanfragen fungieren kann.[23] Allerdings ist auch nicht ausgeschlossen, durch externe Sachverständige die Datenschutzkonformität der Betriebsratsarbeit überprüfen zu lassen.

Klare Regelungen in Geschäftsordnung festhalten

Betriebsräte erlangen im Rahmen von Mitbestimmungsverfahren eine Vielzahl von Unterlagen mit zum Teil besonders sensiblen persönlichen Informationen über Beschäftigte. Dazu gehören etwa Bewerbungsunterlagen und Kündigungsvorlagen, Lohn- und Gehaltslisten, Bewertungs- und Auswahllisten beispielsweise zur Sozialauswahl sowie Daten aus Wiedereingliederungsmaßnahmen.

Betriebsräte sollten sich daher spätestens jetzt um die Umsetzung der neuen Datenschutzregelungen bei der Gremienarbeit und im Betriebsratsbüro kümmern. Klare Regelungen für den Umgang mit Beschäftigtendaten können zum Beispiel in einer BR-Geschäftsordnung festgeschrieben werden, deren Einhaltung durch eine/n »Sonderbeauftragte/n für den Datenschutz« aus dem Kreis der Betriebsratsmitglieder kontrolliert wird. ◁

Hajo Köppen, Rechtsanwalt, Gießen. Dozent für Datenschutzrecht an der TH Mittelhessen.
www.zaftda.de

17 Die Datenschutzkonferenz (DSK) hat in das Papier »Hinweise zum Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO« einen Maßnahmenkatalog aufgenommen. Abrufbar über https://www.datenschutz.bremen.de/sixcms/detail.php?gsid=bremen236.c.14925.de.
18 Vgl. BAG 12.8.2009 – 7 ABR 15/08, NZA 2009, 1218.
19 Vgl. Kiesche/Wilke, CuA 11/2012, 18 ff.
20 BAG 11.11.1997 – 1 ABR 21/97, DuD 1998, 227.
21 Die Entscheidung bezieht sich auf das bis zum 25.5.2018 geltende BDSG. Die einschlägigen Vorschriften der DSGVO und des neuen BDSG führen aber zu keinem anderen Ergebnis.
22 Mit Ausnahme in Bayern, dort ist das Bayerische Landesamt für Datenschutzaufsicht für den nichtöffentlichen Bereich zuständig.
23 Siehe dazu Kiesche/Wilke, CuA 11/2012, 18 ff.

Big Data und Profiling

PERSONALINFORMATIONSSYSTEME *SuccessFactors®, Workday® & Co. unterstützen mit ihren Funktionen genau die Bereiche des Personalmanagements, in denen viele Mitbestimmungsrechte von Betriebs- und Personalräten bestehen. Wie können betriebliche Interessenvertretungen solche Systeme datenschutzkonform regeln?*

VON **MATTIAS RUCHHÖFT**

Moderne Personalinformationssysteme aus der Cloud wie beispielsweise SAP SuccessFactors® oder Workday® sollen alle Funktionen des Personalmanagements verknüpfen und viele Standardarbeiten möglichst automatisieren. Zusätzlich sollen diese Systeme den Einsatz der Mitarbeiter und Mitarbeiterinnen effizienter machen. Dazu werden Module für die Bewerberauswahl, die Beurteilung und den Vergleich der Beschäftigten angeboten, um Potenziale in der eigenen Belegschaft zu entdecken und diese zu entwickeln. Doch wie datenschutzkonform sind solche Module und Funktionen?

Dieser Artikel führt ein in Funktionen der Beurteilung von Beschäftigten in einem Personalinformationssystem und gibt Hinweise auf Herausforderungen im Datenschutz nach der EU-Datenschutz-Grundervordnung (DSGVO) und dem Bundesdatenschutzgesetz neue Fassung (BDSG 2018). Zudem sollen Möglichkeiten für Betriebs- und Personalräte zur Regelung von SuccessFactors®, Workday® & Co. aufgezeigt werden.

Personalinformationssysteme

Es gibt schon seit Längerem viele Personalverwaltungssysteme, die Funktionen zur Beurteilung von Beschäftigten anbieten und das Mitarbeitergespräch abbilden können. Prominentestes Beispiel für solch ein System ist SAP Human Capital Management (HCM). Relativ neu in Deutschland ist der Einsatz von integrierten Personalinformationssystemen, die in den USA entwickelt wurden und auf Cloud-Servern zur Miete angeboten werden. Bekannteste Vertreter solcher Systeme sind Workday® und SuccessFactors®. Der Unterschied zu den klassischen Personalsystemen ist der Ansatz, dass die Beurteilung der Beschäftigten, das Finden von Potenzialträgern und die Förderung von Talenten im Mittelpunkt stehen. Die folgende Werbebotschaft eines Anbieters verdeutlicht diesen Ansatz:

»*Verschaffen Sie sich einen Überblick über Ihre Talentsituation, richten Sie Talente an Unternehmensziele aus und entwickeln Sie die Führungskräfte von morgen. Mit der HR-Talentmanagementsoftware von ABC* (Name vom Verfasser entfernt) *können Sie sinnvoll in Ihre Mitarbeiter und deren Zukunft investieren, sodass Sie bestens auf die Zukunft vorbereitet sind.*«

Um dieses Versprechen umzusetzen, müssen die Funktionen in einem Personalinformationssystem ineinandergreifen und viele personenbezogene Daten der Beschäftigten sammeln und zur Verfügung stellen. Dies gilt insbesondere für deren Zielvorgaben und Leistungsmessung. Die Ausrichtung der »Talente« an Unternehmensziele soll durch einheitliche Zielbibliotheken und Kompetenzmodelle umgesetzt werden.

Abbildung 1 auf Seite 42 verdeutlicht, wie Funktionen der Mitarbeiterbeurteilung miteinander vernetzt sind.

DARUM GEHT ES

1. Personalinformationssysteme greifen auf eine Vielzahl von personenbezogenen Daten der Beschäftigten zu.

2. Zur datenschutzkonformen Regelung dieser Systeme eignen sich Dienst- und Betriebsvereinbarungen.

3. Die zentrale Frage vor der Regelung für Betriebs- und Personalräte ist: »Was wollen wir und was nicht?«

Die Mitarbeiterziele sollen möglichst weltweit harmonisiert werden, um eine Datenbasis für den Vergleich der Leistung einzelner Personen zu haben. Um von der Zielvereinbarung und der Leistungsbeurteilung hin zu einer Talentsuche zu kommen, wird zudem eine Potenzialaussage im System hinterlegt. Diese Aussage über den Beschäftigten treffen die zuständigen Führungskräfte häufig in Verbindung mit der Personalabteilung. Zusätzlich können Kompetenzsysteme zu Stellen und Personen hinterlegt werden.

Verknüpft sind die Zielvereinbarung und die Leistungsbeurteilung mit dem Modul Lernen, da hier die Maßnahmen der Personalentwicklung verwaltet werden. Trainings, E-Learning und andere Angebote können im System direkt einem Mitarbeiter oder einer Mitarbeiterin zugeordnet werden.

Die vernetzte Leistungsbeurteilung und der Vergleich der Beschäftigten setzen eine umfangreiche Datenbasis und Möglichkeiten zu einer umfangreichen Analyse voraus. Personalinformationssysteme liefern eine umfangreiche Datenanalysebibliothek direkt mit. Von vordefinierten grafischen Datenanzeigen bis hin zu freien Abfragen sogenannter Querys finden sich viele Werkzeuge für die Analyse der Daten. Für noch umfangreichere Auswertungen werden zusätzliche Module zur »Workforce Analytics« (zu Deutsch: Belegschaftsanalyse) angeboten. Die Analyse dieser vielen Daten (Big Data) ist das eine, eine automatisierte Vorhersage, um Entscheidungen zu treffen, das andere. Damit Personalinformationssysteme wie Workday® oder SuccessFactors® Vorschläge für Stellenbesetzungen machen können, benötigen sie die Anforderungen der Stelle sowie die Leistungsdaten, berufliche Erfahrungen und Kompetenzen der Person, die die Stelle besetzen soll. Aus einem Abgleich zwischen Stellenanforderung und den Eigenschaften der Beschäftigten oder Bewerber ergeben sich dann die Vorschläge aus dem System.

Im Talentmanagement kann so eine automatisierte Nachfolgeplanung für die Stellen erfolgen, die als Schlüsselpositionen im System hinterlegt sind. Wenn intern keine Nachfolger gefunden werden können, können über das Bewerbermanagement die Auswahlprozesse gestartet werden. Auch hier bieten sich Automatisierungspotenziale für die Sichtung vieler Bewerbungen an. Hierbei können Schlüsselwörter und Voraussetzungen mit den Unterlagen des einzelnen Bewerbers verglichen werden.

ABBILDUNG 1

Beurteilungsfunktionen der Cloud-Personalinformationssysteme

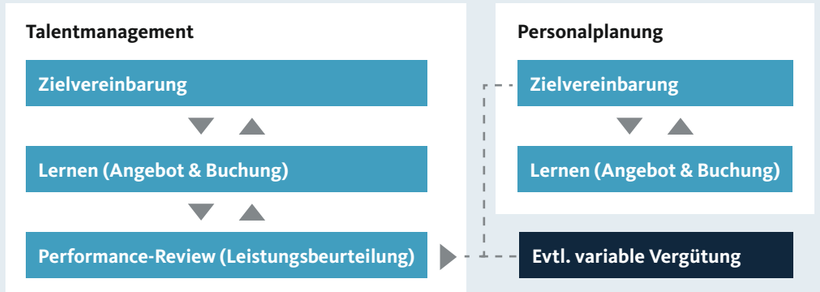


Abbildung : Beurteilungsfunktionen in Personalinformationssystemen (z. B. Workday®, SuccessFactors®) – eigene Darstellung in Anlehnung an Robert-Christian Ziebell et. al. (2016): HR-Cloud-Transformation – Vorgehen und Erfolgsfaktoren, Wiesbaden

Personalinformationssysteme und die DSGVO

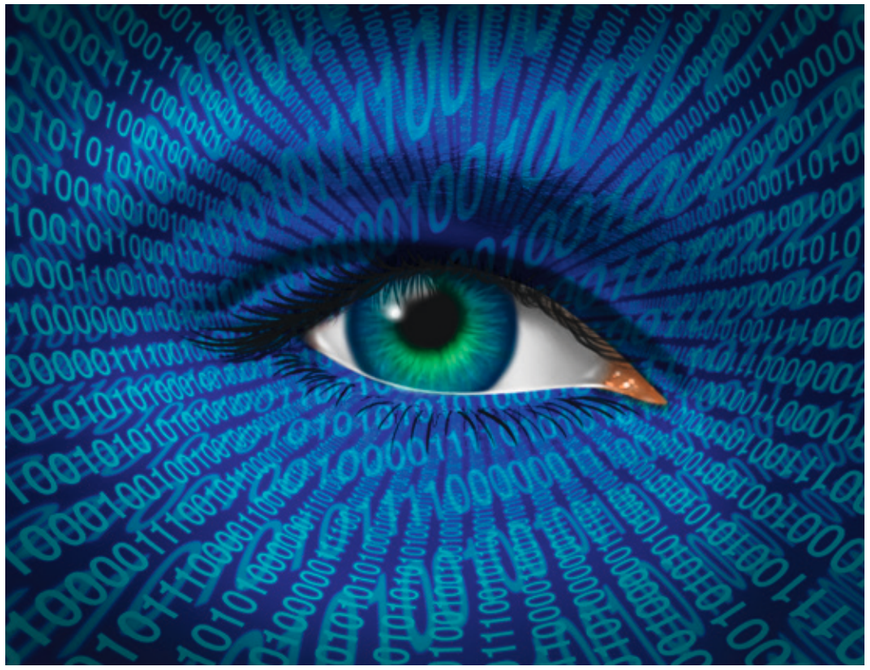
Die Vernetzung vieler Daten der Beschäftigten greift tief in die Persönlichkeitsrechte von Beschäftigten ein, um diese umfangreich zu beurteilen und zu vergleichen. Die Absicherung dieses Grundrechts über Datenschutzgesetze beißt sich kulturell mit der Entwicklung der momentan prominentesten Personalinformationssysteme SuccessFactors® und Workday® in den USA. Am 25.5.2018 traten die EU-Datenschutz-Grundverordnung und das Bundesdatenschutzgesetz in neuer Fassung in Kraft. Hier soll aufgezeigt werden, wie die neuen Datenschutzgesetze beim Einsatz von Personalinformationssystemen umgesetzt werden können. Der Autor konzentriert sich dabei auf die größten Herausforderungen im Sinne des Datenschutzes.

Für Hersteller von IT-Systemen besteht die Herausforderung darin, den »Datenschutz in die Werkseinstellungen« (privacy by design) einzubauen, wie es Art. 25 DSGVO vorschreibt. Diese Regelungen wurden angestrebt, weil sich die Nutzer oder Verbraucher in der Regel nicht darum kümmern, entsprechende Einstellungen für ihren eigenen Datenschutz vorzunehmen. Die Verantwortung liegt dabei bei den Verantwortlichen (Unternehmen) oder Herstellern.

In Erwägungsgrund 78 der DSGVO werden einige Maßnahmen aufgeführt, die Hersteller oder Verantwortliche in ihre Systeme einbauen sollten. Dazu gehört die Minimierung der Verarbeitung personenbezogener Daten, das heißt, nur so viele zu verarbeiten, wie es der jeweilige Verarbeitungszweck gestattet. Gerade Personalinformationssysteme verarbeiten viele personenbezogene Daten der Beschäftigten. Um hier den Überblick zu behalten, sollte eine entsprechende Transparenz herrschen, um die Verarbeitung dieser Daten zu überwachen. Die Daten sollten nach den jeweiligen Verarbeitungszwecken schnell pseudonymisiert oder für die Zugriffe gesperrt werden, die für den Verwendungszweck nicht mehr zuständig sind

In internationalen Unternehmensverbünden oder Konzernen wird die Datensammelei aus anderen Ländern wie beispielsweise den

AiB extra August|2018 Big Data und Profiling MATTIAS RUCHHÖFT



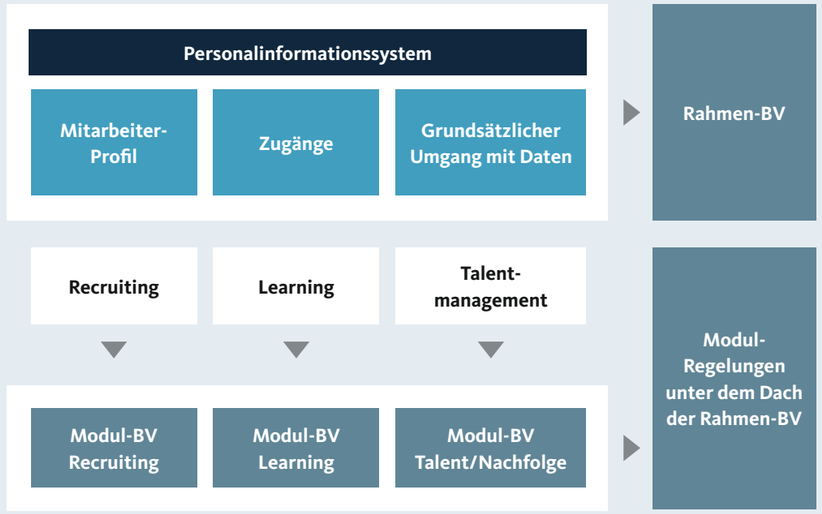
Zur Stärkung der Persönlichkeitsrechte bei der Datenverarbeitung wurde das Recht auf Vergessenwerden des Einzelnen geschaffen.

»Die Vernetzung vieler Daten der Beschäftigten greift tief in die Persönlichkeitsrechte von Beschäftigten ein.«

MATTIAS RUCHHÖFT

ABBILDUNG 2

Struktur einer Betriebsvereinbarung (BV)



Quelle: Struktur Betriebsvereinbarung PIS

USA vorgenommen, die nicht über ein so ausgedehntes Datenschutzverständnis verfügen. Hier bestehen häufig Verständnisschwierigkeiten, weshalb viele Funktionen datenschutzrechtlich bedenklich sind. Hier bietet sich der erhöhte Bußgeldrahmen zur Durchsetzung des europäischen Datenschutzes als starkes Argument an.

Zur Stärkung der Persönlichkeitsrechte bei der Datenverarbeitung wurde mit Art. 17 DSGVO das Recht auf Vergessenwerden des Einzelnen geschaffen. Das ist im Personalmanagement, wo viele personenbezogene Daten der Beschäftigten gesammelt und gespeichert werden, eine Herausforderung. In Verbindung mit Art. 25 DSGVO stellte SuccessFactors® als Beispiel in den letzten beiden Quartals-Releases (jeweils umfangreiches Paket mit Neuerungen) einige neue Funktionen für die Identifikation und Löschung personenbezogener Daten zur Verfügung. Insbesondere die Funktion für das Data Retention Time Management (DRTM) (zu Deutsch: »Datenverweildauer-Management«) soll Verantwortlichen dabei helfen, die Umsetzung der Löschverpflichtungen zu automatisieren. Dazu können Löschregeln erstellt werden, die abhängig von Datentypen, wie Länderzugehörigkeit oder der Information, ob ein Nutzer aktiv oder inaktiv ist, die Verweildauer personenbezogener Daten definieren.

Rein automatische Einzelentscheidungen zu Beschäftigten, wie oben beschrieben (Einstellung oder andere Prozesse), sind nach Art. 22 DSGVO untersagt oder nur in ganz begrenztem Umfang möglich. Viele Personaler in Deutschland stehen nach den Erfahrungen des Autors einer kompletten Automatisierung der Beurteilung und Auswahl von Bewerbern und

GUT ZU WISSEN 1

Dennoch bleibt die Aufgabe für Unternehmen und Behörden, die Prozesse zur Verarbeitung personenbezogener Daten neu zu bewerten, transparent zu gestalten und organisatorisch zu verankern, um den Anforderungen des Datenschutzes zu genügen. Hierzu gehören auch Qualifizierungen für Kolleginnen und Kollegen des Personalmanagements oder für Führungskräfte, wie sie zukünftig mit personenbezogenen Daten der Beschäftigten umzugehen haben.

Beschäftigten sowieso kritisch gegenüber. Die Dienste von amerikanischen Cloud-Anbietern stehen ungeachtet der Integration neuer Funktionen zur Umsetzung von Datenschutzanforderungen unter dem Diktat des US Cloud Act und müssen hinsichtlich der Konformität zur DSGVO neu bewertet werden (siehe Infokasten »Gut zu Wissen 2«).

Was können Betriebs- und Personalräte tun?

Personalinformationssysteme unterstützen mit ihren Funktionen genau die Bereiche des Personalmanagements, in denen viele Mitbestimmungsrechte von Betriebs- und Personalräten bestehen. Das fängt bei der Aufstellung von Auswahlrichtlinien an und hört bei personellen Einzelmaßnahmen wie Einstellungen und Versetzungen auf. Somit ist die Einführung eines integrierten, vernetzten Personalinformationssystems wie SuccessFactors® oder Workday® neben der Betrachtung des technischen Systems nach § 87 Abs. 1 Nr. 6 BetrVG (Schutz vor Leistungs- und Verhaltenskontrolle) für die Arbeitnehmervertretung und die Arbeitgeberseite eine »Operation am offenen Herzen der Mitbestimmung«.

Daher sollten sich Betriebs- und Personalräte unter anderem zunächst fragen, was sie als Gremium wollen. Wie soll das Mitarbeitergespräch durchgeführt werden? Wie kommen Ziele für die Beschäftigten in das System? Welche Kriterien für die Definition von Potenzialen und Talenten wollen wir für unsere Kollegen? Welche Personalentwicklungsmaßnahmen sollen angeboten werden? Um die Vorstellungen der Arbeitnehmervertretung umsetzen zu können, bietet sich die Mitbestimmung bei technischen Systemen an. Zudem besteht mit der Umsetzung der DSGVO die Möglichkeit, in Art. 88 DSGVO eine kollektivrechtliche Vereinbarung (Dienst- oder Betriebsvereinbarung) als Erlaubnistatbestand für die Verarbeitung von personenbezogenen Daten der Beschäftigten zu nutzen. Damit haben Betriebs- und Personalräte einen Hebel, ihre Vorstellungen durchzusetzen.

Da Personalinformationssysteme in der Regel aus vielen Modulen bestehen, die die Beurteilungs- und Qualifizierungsfunktionen von denen der Stammdatenverwaltung für Abrechnung oder Personalmanagement trennen, sollte eine Regelung des Gesamtsystems als Rahmenbetriebsvereinbarung über den Regelungen einzelner Module (beispielsweise zum Talentmanagement) stehen. Darunter können dann Vereinbarungen abgeschlossen werden, die sowohl die technischen Einstellungen als auch die personalwirtschaftlichen Fachprozesse wie die Beurteilung umfassen können.

Arbeitnehmervertretungen haben also viele Ansätze und Möglichkeiten, Personalinformationssysteme im Sinne ihrer Kolleginnen und Kollegen mitzubestimmen und damit auch zu gestalten. Das fängt aber immer mit der Frage an: »Was wollen wir und was nicht?« ◁

GUT ZU WISSEN 2

Seit dem 23.3.2018 ist der Cloud Act in den USA in Kraft. Dadurch dürfen US-Behörden Zugriff auch auf personenbezogene Daten von US-Unternehmen erhalten, die nicht in den USA gespeichert werden. Und dies gilt ungeachtet dessen, ob es internationale Rechtshilfeabkommen gibt oder nicht. Rechtliche Mittel gegen dieses Vorgehen nach dem Cloud Act haben US-fremde Personen kaum. Einige US-Anbieter haben bereits angekündigt, sich dagegen zu wehren. Wie aussichtsreich dies ist, bleibt abzuwarten.
Unabhängig von diesen Überlegungen ist fraglich, ob die direkte Datenübermittlung eines Unternehmens an eine US-Behörde nach der DSGVO überhaupt zulässig ist. In Art. 48 DSGVO ist diese Übermittlung nur zulässig, wenn eine in Kraft befindliche internationale Übereinkunft besteht. Danach sind auch im Hinblick auf die angedrohten Bußgelder nach Art. 83 DSGVO die Bedingungen US-amerikanischer Cloud-Anbieter zu prüfen. Ein Ausweg könnte ein Datentreuhänder sein, der in der Cloud für das Verwalten der Daten des jeweiligen Kunden zuständig ist und nicht in den USA sitzt. Ein solches Modell bietet Microsoft® mit dem deutschen Office 365 an, in dem die Telekom der Datentreuhänder ist.
Auf die Unternehmen, die US-amerikanische Cloud-Modelle nutzen, kommen einige Herausforderungen zu.

Mattias Ruchhöft,
Technologieberater und
Fachautor beim Bund-Verlag.
www.dtb-kassel.de

Betriebsvereinbarung und die DSGVO

BETRIEBSVEREINBARUNGEN *Verstoßen Betriebsvereinbarungen gegen den neuen Datenschutz, sind sie ganz oder teilweise unanwendbar. Den Unternehmen können hierdurch hohe Bußgelder drohen. Warum neue Betriebsvereinbarungen ausgehandelt und bestehende Betriebsvereinbarungen angepasst werden sollten.*

VON **EBERHARD KIESCHE, MATTHIAS WILKE** UND **THOMAS BERGER**

DARUM GEHT ES

1. Auch nach dem neuen Datenschutzrecht können Betriebsvereinbarungen für die Verarbeitung von Beschäftigtendaten geschlossen werden.

2. Betriebsvereinbarungen müssen der Datenschutz-Grundverordnung und dem neuen Bundesdatenschutzgesetz entsprechen.

3. Betriebsvereinbarungen oder Tarifverträge sind entscheidend für die Schaffung spezifischer und konkretisierender Regelungen des Beschäftigtendatenschutzes im Konzern, Unternehmen und im Betrieb.

Seit dem 25.5.2018 gibt es ein neues Datenschutzrecht: Die Datenschutz-Grundverordnung (DSGVO) und das Bundesdatenschutzgesetz (BDSG 2018). Für Arbeitgeber und Betriebsräte stellt sich die dringende Frage, ob sie bestehende Betriebsvereinbarungen als zulässige Rechtsgrundlage für die Personaldatenverarbeitung anpassen müssen und wie zukünftige Betriebsvereinbarungen aussehen müssen, damit sie der DSGVO genügen.[1] Regelungsgegenstände in Betriebsvereinbarungen können alle betrieblichen Prozesse sein, in denen Daten verarbeitet werden. Dies sind etwa Videoüberwachung, Nutzung von Telefon, E-Mail und Internet, Datenübermittlungen im Konzern, die elektronische Personalakte, Einführung und Nutzung von Smartphones und Compliance/Interne Ermittlungen.

Betriebsvereinbarungen können den Datenschutz spezifischer regeln

Die DSGVO wirkt in allen EU-Staaten wie ein Gesetz. Die in ihr enthaltenen Rechte, auf die sich grundsätzlich auch Beschäftigte berufen können, sind teilweise sehr allgemein formuliert. Deshalb ermöglicht die DSGVO in Art. 88 Abs. 1, dass der Beschäftigtendatenschutz künftig auch durch Kollektivvereinbarungen – also Tarifverträge und Betriebsvereinbarungen – ausgestaltet werden kann. Die Schaffung solcher bereichsspezifischer Regelungen, die passgenau auf die Datenverarbeitungen im Betrieb, Unternehmen und Konzern zugeschnitten sind und den Beschäftigtendatenschutz konkretisieren, sind auf dieser Grundlage möglich, sinnvoll und erforderlich.

Neue Anforderungen der DSGVO

Allerdings enthält die DSGVO neue Anforderungen, die an bisher abgeschlossene Kollektivvereinbarungen noch nicht gestellt wurden. Alle Tarifverträge und Betriebsvereinbarungen, die Datenverarbeitungen im Unternehmen legitimieren, müssen daher überprüft und gegebenenfalls angepasst werden. Verstoßen sie mit ihren Regelungen gegen die DSGVO oder erfüllen sie neu gestellte Anforderungen nicht, kann das dazu führen, dass die Betriebsvereinbarungen insgesamt unanwendbar werden, weil der verbleibende Teil ohne die unwirksamen Bestimmungen keine sinnvolle und in sich geschlossene Regelung enthält.[2] Ein Beispiel hierfür sind Vereinbarungen zur Einführung und Anwendung einer Software im Rahmen eines Hinweisgebersystems/Compliancesystems. Ohne Regelungen, die eine Datenschutz-Folgenabschätzung im Zusammenhang mit der Einführung regeln, ist die Betriebsvereinbarung lückenhaft und nicht anwendbar.

Normen im BDSG setzen DSGVO

Der Bundestag hat die aus Art. 88 Abs. 1 DSGVO eröffnete Möglichkeit mit § 26 Abs. 4 BDSG 2018 umgesetzt. Betriebsvereinbarungen mit dem sachlichen Gegenstand Datenverarbeitung und Datenschutz sind daher zulässig. Der Bundesgesetzgeber hat mit Ausnahme der sonstigen Regelungen des § 26 BDSG 2018 von seiner nach Art. 88 Abs. 1 DSGVO bestehenden Möglichkeit, spezifischere, also konkretere Regelungen für das Beschäftigungsverhältnis zu erlassen, selbst keinen Gebrauch gemacht. Er überlässt die Normierung konkreter bereichsspezifischer, also betrieblicher oder unternehmensbezogener, Regelungen des Beschäftigtendatenschutzes den Tarif- und den Betriebsparteien.

Notwendigkeit, unternehmensspezifische Regelungen zu schaffen

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit unterstreicht diesen Punkt in ihrem Jahresbericht 2017 Datenschutz und Informationsfreiheit wie folgt:[3]

»Durch spezifischere Rechtsvorschriften oder Kollektivvereinbarungen kann der Schutz der Rechte und Freiheiten bei der Verarbeitung personenbezogener Beschäftigtendaten besser gewährleistet werden.«[4]

Mögliche Inhalte von Betriebsvereinbarungen

Art. 88 Abs. 1 DSGVO sollte von jedem Betriebsrat gelesen werden. Er ermöglicht ganz allgemein die Schaffung »spezifischerer Vorschriften« zur Gewährleistung des Schutzes der Rechte und Freiheiten von Beschäftigten im Hinblick auf die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext. Diese Ermächtigungsnorm ist sehr weitgehend. Sie erlaubt die Regelung konkretisierender persönlichkeitsschützender Ansprüche für Beschäftigte in Kollektivvereinbarungen und Regelungen, die das gesamte betriebliche Geschehen umfassen, soweit es mit Datenverarbeitungen organisiert wird. Gegenstand dieser Regelungen können somit Datenverarbeitungen sein, die sich auf Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags oder der Beendigung des Beschäftigungsverhältnisses beziehen, des Weiteren auf die Erfüllung von in Gesetzen, Tarifverträgen und Betriebsvereinbarungen festgelegten Pflichten. Ferner können auch Regelungen des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden Bezugspunkt sein. Schließlich werden Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen genannt. Da es sich insoweit nur um eine beispielhafte Aufzählung handelt, ist der Anwendungsbereich für Betriebsvereinbarungen sehr weit, erfasst natürlich auch Gegenstände des § 87 Abs. 1 Nr. 6 BetrVG, ist hierauf aber nicht begrenzt. Anwendungsbereich sind letztlich die gesamte Datenverarbeitung und der gesamte Datenschutz im Beschäftigungskontext.

Betriebsräte können datenschutzrechtliche Betriebsvereinbarungen durchsetzen

Die Grundlage, eine Betriebsvereinbarung zum Datenschutz gegebenenfalls auch gegen den Willen des Arbeitgebers durchzusetzen, kann in der zwingenden Mitbestimmung zu technischen Einrichtungen gemäß § 87 Abs. 1 Nr. 6 BetrVG oder zu Datenschutzverhaltensregeln nach § 87 Abs. 1 Nr. 1 BetrVG sowie zu Personalauswahl- und Beurteilungsgrundsätzen nach §§ 94 und 95 BetrVG liegen. Da die Datenverarbeitung durch technische Einrichtungen im Sinne von § 87 Abs. 1 Nr. 6 BetrVG der Regelfall ist, haben Betriebsräte, die einen wirksamen Beschäftigtendatenschutz durchsetzen wollen, sehr weitgehende Mitbestimmungsrechte. Initiativrechte sind nach neuerer Rechtsprechung auch bei § 87 Abs. 1 Nr. 6 BetrVG möglich.[5]

Rahmenbetriebsvereinbarungen

Betriebsräte schließen zudem oft eine Rahmenbetriebsvereinbarung über Informationstechnik und Datenschutz ab. Sinn dieser Rahmenbetriebsvereinbarung ist die Regelung allgemeiner Transparenz-, Schutz-, Kontroll- und Einsichtsnormen des Betriebsrats und der Beschäftigten, soweit diese für alle oder jedenfalls eine Vielzahl von technischen Einrichtungen gleich geregelt werden können. Oft enthalten Rahmenbetriebsvereinbarungen mitbestimmungspflichtige und mitbestimmungsfreie Regelungen. Soweit die Regelungen mitbestimmungsrechtlich nicht erzwungen werden können, kann § 88 BetrVG als Rechts-

1 Der Beitrag ist eine überarbeitete Version von »Betriebsvereinbarungen jetzt updaten«, AiB 3/2018, 15.

2 BAG 9.7.2013 – 1 ABR 19/12.

3 www.datenschutz-berlin.de.

4 Unter 8.1 des Jahresberichts 2017 des Beauftragten für Datenschutz und Informationsfreiheit Berlin.

5 LAG Berlin-Brandenburg 22.1.2015 – 10 TaBV 1812/14, 1 – 10 TaBV 2124/14.

CHECKLISTE

Eckpunkte einer Verfahrensvereinbarung zur Umsetzung der Datenschutz-Grundverordnung in Betrieb/Unternehmen/Konzern

Erstellung eines »Maßnahmeplans DSGVO« und Beteiligung des Betriebsrats
(1) Der Arbeitgeber wird einen Maßnahmeplan »DSGVO« für das Unternehmen und jeden Betrieb feststellen und sodann in eigener Verantwortung umsetzen.
(2) Der Arbeitgeber hat den Betriebsrat bei der Entwicklung des Maßnahmeplans zu beteiligen. Auf Verlangen ist der Betriebsrat auch an der Feststellung und der Umsetzung zu beteiligen.
(3) Die Beteiligung nach Abs. 2 besteht in der rechtzeitigen und umfassenden mündlichen und schriftlichen Unterrichtung, Anhörung und Konsultation. Auf Verlangen des Betriebsrats ist über die Gegenstände der Datenverarbeitung, einschließlich etwaiger Teilschritte, Prozesse oder nachfolgender Bausteine, eine Betriebsvereinbarung zu schließen.
(4) Der Betriebsrat kann einen technischen und einen juristischen Berater hinzuziehen, wenn und soweit er das für Aufgaben aus den § 2 – § 4 erforderlich hält. Der Arbeitgeber stellt hierfür einen Kostenrahmen von x zur Verfügung. Nach Ausschöpfung des Kostenrahmens kann der Betriebsrat eine Erweiterung des Kostenrahmens beantragen.

Der Maßnahmeplan enthält folgende Bausteine:

1. Informationen von Geschäftsleitung und Betriebsrat an die Belegschaft
2. Schaffung einer »Projektgruppe DSGVO«, die paritätisch aus jeweils zwei Vertretern der Geschäftsführung und des Betriebsrats besetzt ist und die den betrieblichen Datenschutzbeauftragten hinzuzieht
3. Bestandsaufnahme durch die Projektgruppe
4. Feststellung des Handlungsbedarfs durch die Projektgruppe
   a) Festlegung einer Aufbauorganisation des Datenschutzes im Unternehmen und in den Betrieben, einschließlich von Datenschutzbeauftragten und konkreter Regelung der Zusammenarbeit zwischen den Datenschutzbeauftragten und dem Betriebsrat
   b) Festlegung einer Ablauforganisation, einschließlich der Anpassungen der Prozesse zur Gewährleistung des Datenschutzes, insbesondere Implementierung von Löschkonzepten, Zugriffsberechtigungskonzepten, elektronischen Zugriffsrechten der Beschäftigten und jederzeitiger unbeschränkter Leserechte des Betriebsrats zur Kontrolle der Einhaltung der Gesetze und der Betriebsvereinbarung
   c) Feststellung und Festlegung der Zwecke von Datenverarbeitungen und der jeweiligen Rechtsgrundlagen der Datenverarbeitungen
   d) Schaffung bereichsspezifischer Regelungen durch Gesamt- und/oder Betriebsvereinbarungen im Unternehmen und/oder Betrieb
   e) Konkretisierung der Datenschutzrechte der Beschäftigten
   f) Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung
   g) Umsetzung des Datenschutzes durch die Vereinbarung von Verhaltensregeln, mit denen die Vorgaben der DSGVO präzisiert werden
   h) Überprüfung und Anpassung der bestehenden Verträge im Hinblick auf alle Dienstleistungsbeziehungen
   i) Umsetzung der Dokumentationspflichten
   j) Prüfung des Erfordernisses einer Datenschutz-Folgenabschätzung (DSFA)
   k) Organisation und Konkretisierung von Meldepflichten
   l) Überprüfung der Datensicherheit
   m) Prüfung der Notwendigkeit der Zertifizierung
   n) Konzept zur Nachweisbarkeit der Einhaltung der Anforderungen aus DSGVO und BDSG 2018
   o) Festlegung von Reaktionsmechanismen auf Datenpannen
   p) Aufbau der Dokumentation
   q) Erstellung eines Verfahrensverzeichnisses

grundlage herangezogen werden. Der Abschluss von Rahmenbetriebsvereinbarungen ist auch deshalb angeraten, weil Betriebsräte sich in der Praxis oft überfordert fühlen, zu jeder einzelnen technischen Einrichtung, zu jeder Software und zu jedem Softwareupdate eine gesonderte Betriebsvereinbarung abzuschließen.

Kein Verzicht auf Mitbestimmung

Der Abschluss von Rahmenbetriebsvereinbarungen darf jedoch keinen Verzicht auf Mitbestimmungsrechte zu einzelnen technischen Einrichtungen beinhalten. Die Rahmenbetriebsvereinbarung kann Aufbau- und Ablauforganisation, Zuständigkeiten und Prozesse zur Vereinfachung regeln, ohne dem Betriebsrat die Möglichkeit zu nehmen, zu einem bestimmten technischen System verlangen zu können, eine gesonderte Betriebsvereinbarung abzuschließen. Die Rahmenbetriebsvereinbarung sollte systemübergreifend nach der DSGVO etablierte Betroffenenrechte, insbesondere nach den Art. 12 ff. DSGVO, konkretisieren und technische und organisatorische Umsetzungsmaßnahmen der aus der Verordnung folgenden Arbeitgeberpflichten regeln. Vor allem können sie Einsichts- und Kontrollrechte des Betriebsrats spezifizieren.

Rahmenbetriebsvereinbarungen als Risiko

Betriebsräte sollten aber stark darauf achten, dass sie nicht einfach eine vom Arbeitgeber vorgelegte Rahmenbetriebsvereinbarung unterschreiben, die keine konkreten Datenschutzregelungen enthält. Solche Rahmenbetriebsvereinbarungen sollen Betriebsräte dazu verleiten, sich mit allen bestehenden und künftigen technischen Einrichtungen einverstanden zu erklären. Sie sollen verhindern, dass überhaupt allgemeine und spezifische Einführungs- und Anwendungsbedingungen für Hard- und Software geregelt werden. Sie beinhalten oft nur eine Wiederholung oder Verweise auf ohnehin bestehende gesetzliche Rechte. Sie wirken zudem oft als (unzulässiger) pauschaler Verzicht auf die Ausübung der Mitbestimmung durch pauschale Zustimmung zur Einführung unbekannter Hard- oder Software. Solche Rahmenvereinbarungen bewirken selbst einen Zustand von Intransparenz, der gegen Grundsätze der DSGVO verstößt. Sie sind wegen der Anforderungen aus Art. 88 Abs. 1 und 2 DSGVO datenschutzrechtlich unanwendbar. Die Betriebsvereinbarungen müssen nämlich spezifisch, also konkret sein, und es müssen besondere Maßnahmen geregelt werden.

Defizite bei Umsetzung der DSGVO

In den meisten von uns durchgeführten Beratungen fordern die Betriebsräte ihre Arbeitgeber zur Beachtung der DSGVO und zur Umsetzung und Schaffung konkreter Regelungen des Beschäftigtendatenschutzes im Unternehmen auf. Die Arbeitgeber, die für die Umsetzung der DSGVO und ihrer Verpflichtungen verantwortlich sind, bleiben im Beschäftigungskontext (noch) zu passiv. Diese Beobachtung wird durch die Einschätzung der Datenschutzkonferenz – DSK – gestützt. Im Kurzpapier 8 der DSK heißt es: »Viele Unternehmen sind aber noch nicht auf die DSGVO und deren Auswirkungen auf die Unternehmensprozesse vorbereitet.«[6]

Viele Arbeitgeber meiden das Thema DSGVO auch im Beschäftigungskontext. Eine Überarbeitung und Anpassung von Betriebsvereinbarungen haben die wenigsten Arbeitgeber im Blick. Teilweise versuchen Arbeitgeber, von ihren eigenen Unzulänglichkeiten zum Thema DSGVO abzulenken, was mitunter sogar dazu führt, dass den Betriebsräten Protokollnotizen zur Unterschrift vorgelegt werden, in denen sie sich zur Verschwiegenheit hinsichtlich bekanntgewordener Defizite im Unternehmen verpflichten sollen. Es gibt aber auch vorbildliche Unternehmen, die gut beraten ihrer Initiativlast nachkommen, um Compliancerisiken zu minimieren.

Art. 88 Abs. 2 DSGVO ist in Betriebsvereinbarung und Sprüchen zu beachten

Betriebsvereinbarungen dürfen nicht gegen höheres Recht verstoßen. Betriebs- und Personalräte sowie Einigungsstellen sind somit Adressaten der Vorschrift. Sie können und müssen damit zunächst dem Maßstab von Art. 88 Abs. 2 DSGVO genügen. Betriebsvereinbarungen oder diese ersetzende Sprüche der Einigungsstelle müssen daher geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen. Sie müssen insbeson-

6 Kurzpapiere der Datenschutzkonferenz (DSK) abrufbar unter: https.//www.bfdi.bund.de.

AiB extra August|2018 Betriebsvereinbarung und die DSGVO KIESCHE, WILKE, BERGER

KURZ UND KNAPP

Zehn gute Gründe, Betriebsvereinbarungen oder Tarifverträge zum Datenschutz abzuschließen

1. Sicherstellen, dass die Rechtslage nach Inkrafttreten der DSGVO im Unternehmen umgesetzt wird Das Inkrafttreten der DSGVO und des BDSG 2018 am 25.5.2018 ist vor allem eine große Chance für Betriebsräte, Datenschutz und Datensicherheit im Betrieb und Unternehmen zu thematisieren sowie die Beschäftigten über die Wichtigkeit des Themas und ihre Rechte aufzuklären. Rechte werden nicht schon dann Realität, wenn sie vom Gesetzgeber erlassen worden sind. Sie müssen auch im Unternehmen durchgesetzt, ihre Einhaltung muss kontrolliert werden. Die Initiative und Aktivität von Betriebsräten sind daher sinnvoll, oft sogar notwendig, damit die Gesetzeslage im Unternehmen angewendet wird.

2. Nicht dem Arbeitgeber das Feld überlassen Wird der Betriebsrat nicht aktiv, besteht das Risiko, dass der Arbeitgeber ohne Abschluss von Betriebsvereinbarungen die Rechtslage im Unternehmensinteresse interpretiert und anwendet. In vielen, aber bei Weitem noch nicht allen Unternehmen bereitet die Arbeitgeberseite seit Monaten intensiv die veränderte Rechtslage nach dem 25.5.2018 vor. Betriebsräte sollten sich in diesen Prozess einbringen und so verhindern, dass der Arbeitgeber einseitig an Unternehmensinteressen orientiert das Thema besetzt. Dazu ist es für die Beschäftigten in jeder Hinsicht zu wichtig. Viele Unternehmen werden selbst die Notwendigkeit von Betriebsvereinbarungen als Rechtsgrundlage für Datenverarbeitungen erkennen und solche anstreben. Betriebsräte haben auch hinsichtlich von Rechtsfragen, die durch Spruch der Einigungsstelle nicht erzwingbar sind, eine starke Verhandlungsposition. Hintergrund ist, dass die wohl überwiegende Meinung in der Rechtsliteratur davon ausgeht, das Datenschutzniveau der DSGVO dürfe nicht unterschritten werden.

3. DSGVO will Tarifverträge und Betriebsvereinbarungen zum Umgang mit Beschäftigtendaten Die DSGVO sieht in der Betriebsvereinbarung und in Tarifverträgen ausdrücklich eine wichtige Rechtsgrundlage für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext. Nach Art. 88 Abs. 1 DSGVO können »Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext (insbesondere …) vorsehen«.
Nach Erwägungsgrund 155 zur DSGVO können »in Kollektivvereinbarungen (einschließlich ›Betriebsvereinbarungen‹) (…) spezifische Vorschriften für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorgesehen werden, und zwar insbesondere Vorschriften über die Bedingungen, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen, über die Verarbeitung dieser Daten für Zwecke

- der Einstellung,
- der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten des Managements,
- der Planung und der Organisation der Arbeit,
- der Gleichheit und Diversität am Arbeitsplatz,
- der Gesundheit und Sicherheit am Arbeitsplatz sowie
- für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und
- für Zwecke der Beendigung des Beschäftigungsverhältnisses.

4. Schaffung von angemessenen Maßnahmen zur Wahrung der Grundrechte Neue Betriebsvereinbarungen/Tarifverträge geben die Gelegenheit, besondere Maßnahmen zur Wahrung der (Grund-)Rechte der Arbeitnehmer zu schaffen. Art. 88 Abs. 2 DSGVO enthält inhaltliche Vorgaben für alle Betriebsvereinbarungen, die künftig zwingend und konkret zu regeln sind. Die Betriebsvereinbarungen müssen »angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz« umfassen.

5. Haftungsrisiko als Hebel für gute Betriebsvereinbarungen nutzen Betriebsräte sollten die enormen Haftungs- und Bußgeldrisiken der Unternehmen und der persönlichen Haftung von Geschäftsführern und Vorständen nutzen, um ein hohes Datenschutzniveau zugunsten der Beschäftigten zu etablieren. Viele Unternehmen werden bereits aus Eigeninteresse den Abschluss von Rahmenbetriebsvereinbarungen anstreben. Dies gilt jedenfalls für die Unternehmen, die ihrerseits seriös und im Hinblick auf Compliancerisiken vorausschauend beraten werden.

6. Haftung vorbeugen – Geld lieber in Gehälter und gute Arbeitsbedingungen stecken Eine Haftung des Unternehmens ist auch für die Beschäftigten von Nachteil. Sie setzt voraus, dass es zu Rechtsverletzungen in der Regel zulasten der Beschäftigten gekommen ist. Bußgelder fließen aus dem Unternehmen ab und können so weder zur Verbesserung von Entgelt noch sonstiger Arbeitsbedingungen eingesetzt werden. Reputationsschäden des Unternehmens bringen oft auch Arbeitsplätze in Gefahr.

7. Achtung: (Alte) Betriebsvereinbarungen, die der DSGVO nicht entsprechen, sind unanwendbar Soweit bisherige Betriebsvereinbarungen zum Datenschutz oder zu technischen Einrichtungen gemäß § 87 Abs. 1 Nr. 6 BetrVG die Anforderungen der DSGVO nicht erfüllen, sind sie in der Regel unanwendbar. Im Hinblick auf die europäische Neuordnung des Datenschutzes sollten Betriebsräte unbedingt (neue) Betriebsvereinbarungen unter Beachtung der strengen Vorgaben der DSGVO abschließen. Bestehende Betriebsvereinbarungen lassen sich gegebenenfalls nachbessern. Empfehlenswert ist der Abschluss einer Rahmenbetriebsvereinbarung, die die Umsetzung der DSGVO für das Unternehmen und den Betrieb konkretisiert.

8. Hinzuziehung von Sachverständigen ist anzuraten Angesichts bestehender Rechtsunsicherheiten, der Bedeutung des neuen Datenschutzrechts für die Beschäftigten sowie der rechtlichen und tatsächlichen Komplexität der DSGVO ist die Hinzuziehung von Sachverständigen durch den Betriebsrat nach § 80 Abs. 3 BetrVG grundsätzlich anzuraten. Dies ermöglicht eine professionelle Beratung des Betriebsrats und Verhandlungen auf Augenhöhe mit der Geschäftsführung oder dem Vorstand. So lässt sich auch der Gefahr begegnen, dass Betriebsvereinbarungen das Datenschutzniveau der DSGVO unterschreiten.

9. Betriebsrat hat eigenen Durchführungsanspruch Eine Betriebsvereinbarung schafft die konkreten Voraussetzungen, damit die Beschäftigten die weitgehenden Rechte, die ihnen die DSGVO einräumt, auch geltend machen können. Der Betriebsrat ist nicht nur auf die Kontrolle der Einhaltung der DSGVO beschränkt. Vielmehr hat er einen selbstständigen Durchführungsanspruch – unabhängig von den betroffenen Beschäftigten. Er kann auch seine eigenen Rechte auf Unterrichtung in der Betriebsvereinbarung absichern. So kann er wirksam der Gefahr begegnen, dass die Rechte der Beschäftigten zwar auf dem Papier stehen, aber kein Mitarbeiter sich traut, sie geltend zu machen.

10. Wer nicht regelt, wird geregelt! Das Selbstbestimmungsrecht über die eigenen Daten, grundrechtlich geschützt als Recht auf informationelle Selbstbestimmung, ist bei Arbeit 4.0 noch stärker gefährdet und verletzlicher als je zuvor. Das Selbstbestimmungsrecht ist eine Herausforderung, die Beschäftigte nur mit ihren Betriebsräten in den Griff kriegen können. Betriebsräte sollten deshalb Betriebsvereinbarungen zum Datenschutz 4.0 offensiv anstreben. Wer nicht regelt, wird geregelt!

dere die Transparenz der Verarbeitung und der Übermittlung der Beschäftigtendaten im Unternehmen oder innerhalb von Unternehmensgruppen sicherstellen. Diese besonderen Maßnahmen sind in Betriebsvereinbarungen festzulegen. Hierzu gehören insbesondere technisch-organisatorische Maßnahmen des Datenschutzes, Regelungen zur Erhöhung und Sicherstellung der Transparenz der Datenverarbeitung, die Wahl des mildesten Mittels bei der Datenverarbeitung, insbesondere auch Pseudonymisierung, die Festlegung von Sachvortrags- und Beweisverwertungsverboten.

Datenschutzrechtliche Betriebsvereinbarungen müssen DSGVO entsprechen

Die Betriebsvereinbarungen müssen auch im Übrigen den Vorgaben der DSGVO genügen. Art. 5 DSGVO regelt die Grundsätze des Datenschutzes. Der Verantwortliche, hier der Arbeitgeber, muss die Umsetzung von Art. 5 DSGVO nachweisen. Die Rechenschaftspflicht hat Folgen für die Betriebsvereinbarungen.

Betriebsräte sollten Rahmenbetriebsvereinbarungen nur dann abschließen, wenn sie die Wirkung von diesen Vereinbarungen auf die Rechte aus dem neuen Datenschutz überblicken!

Bisherige Betriebsvereinbarungen erfüllen oft nicht die Mindestanforderungen

Bestehende Betriebsvereinbarungen zur Regelung von Informationstechnik und Datenschutz erfüllen diese Vorgaben oft nicht oder

nicht ausreichend. Die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO vor Einführung einer geplanten Datenverarbeitung ist ein neues Instrument im Datenschutzrecht. Sie soll erforderliche Schutzmaßnahmen zugunsten der Beschäftigten identifizieren und umsetzen. Bei jeder Datenschutz-Folgenabschätzung sind das Risiko für die Rechte und die Interessen von natürlichen Personen und erforderliche Schutzmaßnahmen zu bewerten. Es geht um die Würde des Menschen und um das Grundrecht auf den Schutz personenbezogener Daten. Im besonders sensiblen Bereich der Verarbeitung von Beschäftigtendaten sollte ihre Durchführung Standard sein.

Auch reine IT-Betriebsvereinbarungen neu verhandeln?

IT-Betriebsvereinbarungen, die in der betrieblichen Praxis den Einsatz von betrieblichen Informationssystemen wie beispielsweise Kundenbindungssysteme, Krankenhausinformationssysteme, Firewalls oder ERP-Systeme (Enterprise Resource Planning bezeichnet eine Softwarelösung zur Ressourcenplanung eines Unternehmens) regeln und nicht ausdrücklich als Rechtsgrundlage der Verarbeitung von Beschäftigtendaten dienen, haben ebenfalls stets einen Bezug zum Beschäftigtendatenschutz. Insofern sind auch sie dem neuen Datenschutzrecht anzupassen. Die Frage, ob alle Betriebsvereinbarungen mit Datenschutzrelevanz zu ändern sind, kann letztlich nur der Europäische Gerichtshof (EuGH) entscheiden. Jedenfalls dürfen sie nicht gegen die DSGVO verstoßen. Schon aufgrund der Bußgeldandrohungen in der DSGVO ist zu empfehlen, dass Arbeitgeber und Betriebsräte bestehende Betriebsvereinbarungen mit Datenschutzrelevanz auf Kompatibilität mit der DSGVO überprüfen und überarbeiten sollten. Zeigt sich Anpassungsbedarf, sind sie entsprechend zu verändern. Falls die Vorgaben aus Art. 88 Abs. 2 DSGVO in den IT-Betriebsvereinbarungen nicht umgesetzt sind, können diese Vorgaben gegebenenfalls in einer flankierenden Rahmenbetriebsvereinbarung umgesetzt werden.

§ 26 BDSG 2018 in Kraft getreten

Der ebenfalls am 25.5.2018 in Kraft getretene § 26 BDSG 2018 ist eine Grundnorm des Beschäftigungsdatenschutzes.[7] § 26 Abs. 4 BDSG 2018 sieht Kollektivvereinbarungen als Grundlage für die Verarbeitung von Beschäftigtendaten vor, allerdings nur, soweit Art. 88 Abs. 2 DSGVO beachtet wird. § 26 BDSG 2018 ersetzt § 32 BDSG a.F., ist aber deutlich erweitert. Nach § 26 Abs. 1, 2 und 3 BDSG 2018 ist Datenverarbeitung, soweit erforderlich, zulässig

- für die Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses,
- für Rechte und Pflichten der Interessenvertretung,
- zwecks Aufklärung eines konkreten Straftatverdachts im Rahmen der Verhältnismäßigkeit,
- für besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) zur Ausübung oder zur Erfüllung rechtlicher Pflichten und bei Vorliegen einer Einwilligung nach § 26 Abs. 2 BDSG 2018.

Datenschutz gilt auch für Beschäftigtendaten außerhalb von Dateisystemen

Alles im Unternehmen, was mit Beschäftigtendaten zu tun hat, unterfällt § 26 Abs. 7 BDSG 2018. Danach sind die datenschutzrechtlichen Vorschriften im Beschäftigungskontext auch anzuwenden, wenn Beschäftigtendaten verarbeitet werden, die nicht in einem Dateisystem gespeichert werden sollen. Auch nach Art. 4 DSGVO ist jeder auch ohne Hilfe automatisierter Verfahren ausgeführte Vorgang vom Begriff der Datenverarbeitung erfasst. Deshalb fallen auch Anhörungen und Befragungen von Beschäftigten im Rahmen von Ermittlungsmaßnahmen von unternehmensinternen Ermittlungen, Fragebogenaktionen, Spindkontrollen oder Personalakten oder sogar jede beschäftigtenbezogene Notiz in den Anwendungsbereich.

Orientierung an der bisherigen Rechtsprechung von EuGH und BAG

Die bisherige Rechtsprechung des EuGH und des EGMR dürfte bereits deshalb Orientierungsmaßstab bleiben, weil die Europäische Richtlinie zum Datenschutz durch die DSGVO zwar abgelöst wurde, aber Bezugspunkt dieser bleibt. Auch die bisherigen Entscheidungen des Bundesarbeitsgerichts (BAG) mit ihren Vorgaben für Betriebsvereinbarungen bleiben ein Maßstab. In den Entscheidungen zu Torkontrollen[8] und zur Elektronischen Signaturkarte[9] werden grundlegende Anforderungen an Betriebs-/Dienstvereinbarungen zu Kontrollmaßnahmen formuliert. Sehen Betriebsvereinbarungen Kontrollen vor, muss zum Beispiel der Grundsatz der Verhältnismäßigkeit gewahrt werden. Dieser verlangt eine Regelung, die geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen ist, um den erstrebten Zweck zu erreichen. Den Betriebsparteien dürfen zur Zielerreichung keine anderen, gleich wirksamen und das Persönlichkeitsrecht der Arbeitnehmer weniger einschränkende Mittel zur Verfügung stehen.

BAG macht datenschutzrechtliche Vorgaben für die inhaltliche Gestaltung

Kollektivvereinbarungen müssen nach dem BAG dem Bestimmtheits- und Transparenzgebot sowie dem nationalen Recht genügen. Die Grundsätze des Datenschutzrechts für die Verarbeitung von Beschäftigtendaten im Betrieb müssen betrieblich genau beschrieben werden. Betriebsvereinbarungen mit Bezug zur DSGVO und zum BDSG 2018 sollten in klarer, präziser und verständlicher Sprache insbesondere folgende elf Punkte enthalten:

1. Einordnung der Betriebsvereinbarung als datenschutzrechtliche Erlaubnisregelung oder Verweis auf andere Erlaubnistatbestände nach Art. 6 Abs. 1 DSGVO und § 26 Abs. 1, 2 BDSG 2018
2. Transparente, umfassende und präzise Festlegung maßgeblicher Verarbeitungszwecke
3. Datenschutzgrundsätze erläutern (Art. 5 Abs. 1 DSGVO), etwa Rechtmäßigkeitsprinzip
4. Konkrete Regelungen zur Absicherung von Einwilligungen (§ 26 Abs. 2 BDSG 2018) im Beschäftigungskontext
5. Prozesse für die Ausübung von Betroffenenrechten nach DSGVO und § 32 – 35 BDSG 2018
6. Vorgaben zur Verhältnismäßigkeit von Kontrollmaßnahmen und Datenverarbeitung von Beschäftigtendaten
7. Technisch-organisatorische Maßnahmen zur Datensicherheit (Art. 32 DSGVO und § 22 Abs. 2 BDSG 2018)

7 Datenschutz-Anpassungs- und Umsetzungsgesetz EU-DSAnpUG-EU vom 27.4.2017.

8 BAG 9.7.2013 – 1 ABR 2/13 (A).

9 BAG 25.9.2013 – 10 AZR 270/12.

8. konkrete Vorgaben zur Dokumentationspflicht, Datenschutz-Folgenabschätzung, Datenminimierung, Speicherbegrenzung, Datenrichtigkeit und Berichtigung von Personaldaten
9. Schutzmaßnahmen zur Gewährleistung der Grundrechte der Beschäftigten bei Datenübermittlung im Konzern, Datenübermittlungen in Drittstaaten und bei Überwachungssystemen am Arbeitsplatz
10. Regelung der Auftragsdatenverarbeitung gemäß Art. 28 DSGVO.
11. Zugriffs- und Kontrollrechte für Interessenvertretungen.

Betriebsvereinbarungen dürfen geltendes Datenschutzniveau nicht absenken

Auch bei der bisherigen Rechtslage war umstritten, ob Betriebsvereinbarungen inhaltlich hinter dem Mindeststandard des BDSG a.F. zurückbleiben dürfen. Das BAG hatte dies mit dem Hinweis auf § 4 Abs. 1 BDSG a.F. bejaht.[10] Mit der DSGVO sollte diese Diskussion hinfällig geworden sein. Die Ermächtigungsgrundlage für den Abschluss von Betriebsvereinbarungen ist nunmehr allein Art. 88 Abs. 1 DSGVO, der durch § 26 Abs. 4 BDSG zwar aufgegriffen, aber nicht modifiziert wird. Art. 88 DSGVO erlaubt nur spezifischere Regelungen, nicht aber Regelungen, die das allgemeine Datenschutzniveau der DSGVO unterschreiten. Diese Sichtweise wird auch von den Aufsichtsbehörden geteilt. Im Gegenteil: Gerade Art. 88 Abs. 2 DSGVO stellt den darüber hinausgehenden Grundsatz auf, dass bei Abschluss von spezifischeren Regelungen nach Abs. 1 besondere und geeignete Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person getroffen werden müssen. Somit ist gerade auch ein höherer Standard durch Konkretisierung und Spezifizierung nicht ausgeschlossen, sondern gefordert. Eine Absenkung des Schutzniveaus lässt sich aus der Regelung nicht herleiten.

Grundrechtlicher und europarechtlicher Standard

Durch § 75 Abs. 2 BetrVG und Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz (GG) verpflichten sich die Betriebsparteien, die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Das Schutzniveau der Charta der Grundrechte der Europäischen Union (GRCh), der Menschenrechtskonvention, der DSGVO und des BDSG 2018 darf durch Kollektivvereinbarungen nicht unterschritten werden. Allerdings können die Betriebsparteien höhere Standards zum Schutz der Grundrechte der Beschäftigten aufgrund von Art. 88 Abs. 1, 2 DSGVO vereinbaren.

Bestehende Betriebsvereinbarungen mit Datenschutzrelevanz anpassen

Es ist unbestritten, dass Betriebsvereinbarungen als zulässige Kollektivvereinbarungen nach Art. 88 DSGVO mit dem neuen Datenschutz konform – also compliant – sein müssen. Compliance beschreibt die Gesamtheit der Maßnahmen eines Unternehmens zur Vermeidung von Gesetzesübertretungen und Regelverstößen, hier bezogen auf die DSGVO und das BDSG 2018. Das gilt seit dem 25.5.2018 sowohl für neue als auch für bestehende Betriebsvereinbarungen. Bestehende datenschutzrechtliche Betriebsvereinbarungen müssen mit ihren Begriffen, Verweisen und den inhaltlichen Bestimmungen der DSGVO und dem BDSG 2018 entsprechen. Sie müssen die DSGVO spezifizieren und konkretisieren. Ansonsten werden sie unanwendbar und verlieren ihre Geltung als datenlegitimierende Rechtsvorschrift nach Art. 88 Abs. 1 DSGVO. Es gibt in der DSGVO oder in § 26 BDSG 2018 keine Ausnahmeregelung für »Altfälle« der Betriebsvereinbarungen. Die Übergangsfrist von zwei Jahren wurde als ausreichend angesehen, um eine Anpassung an die DSGVO vorzunehmen.

Mit dem Arbeitgeber verhandeln

Daher ist geraten, jetzt Betriebsvereinbarungen zu überprüfen, die die Verarbeitung von Beschäftigtendaten rechtfertigen oder sich teilweise auf Datenschutzregelungen der DSGVO und auf Beschäftigtendaten beziehen. Dieses Kompatibilitätsscreening kann gemeinsam mit der Personalabteilung angegangen und nach Aufwand und Relevanz gewichtet werden. In den Fokus rücken dabei alle Betriebsvereinbarungen, die die Verarbeitung von Leistungs- und Verhaltensdaten regeln und für die entsprechende Schutzmaßnahmen nach Art. 88 Abs. 2 DSGVO dringend einzubauen sind.

10 BAG 27.5.1986 – 1 ABR 48/84.

Ebenso sind Rahmenbetriebsvereinbarungen zum IT-Einsatz bezüglich wichtiger Anpassungen an die DSGVO zu überprüfen. Und schließlich sind auch Betriebsvereinbarungen mit sonstigen Regelungsgegenständen zu überprüfen, sofern sie auch personenbezogene Datenverarbeitung voraussetzen oder regeln.

Initiative ergreifen und gemeinsamen Prozess vorschlagen

Sollten Betriebsräte bislang nicht in den Prozess der Anpassung des Unternehmens in das Zeitalter der DSGVO eingebunden worden sein, sollten sie die Initiative ergreifen. Als ersten Schritt sollten sie ihren Geschäftsführungen vorschlagen, gemeinsam einen Prozess zu definieren und zu vereinbaren, die (noch) nötigen Schritte zu gehen. Falls Arbeitgeber dann behaupten, sie hätten schon alles gemacht, kann man eine entsprechende Unterrichtung nach § 80 Abs. 2 BetrVG einfordern, die das anhand von Unterlagen belegt. Diese Nachweise sind nach der DSGVO zu erbringen.

Verfahrensvereinbarung mit Orientierung an den Empfehlungen der DSK

Der gemeinsame Prozess sollte sich an den Empfehlungen der Datenschutzkonferenz – DSK –, also den Publikationen der deutschen Aufsichtsbehörden orientieren. Hierzu könnte der Betriebsrat dem Arbeitgeber vorschlagen, eine entsprechende Verfahrensvereinbarung zur Umstellung auf die DSGVO und das BDSG 2018 abzuschließen, in der man den Anpassungsprozess verbindlich vereinbart. Eine solche freiwillige Verfahrensvereinbarung kann gegen den Willen der Betriebsparteien nicht erzwungen werden. Indessen sind Unternehmen gut beraten, den Weg gemeinsam mit ihren Betriebsräten zu gehen, und zwar gerade dann, wenn sie im Verzug sein sollten.

Inhalt der Verfahrensvereinbarung

Die Verfahrensvereinbarung kann notwendige betriebliche Umsetzungsschritte beschreiben und präzisieren, um die Überarbeitung der bestehenden Betriebsvereinbarungen einvernehmlich zu ermöglichen. Dies bietet die Chance, dass der Betriebsrat darauf einwirken kann, dass die Vorgaben der DSGVO eingehalten und auf das Unternehmen und den Betrieb bezogen spezifiziert werden. Ein Abschluss einer solchen Verfahrensvereinbarung kann auch Zeitabläufe und Schulungen für Betriebsräte zur DSGVO und der neuen Rechtslage sowie die Heranziehung von Sachverständigen/Beratern für den Betriebsrat konkret und verbindlich regeln.

Anpassung an die DSGVO

Bestehende Einzelbetriebsvereinbarungen an die DSGVO anzupassen und neue Vereinbarungen datenschutzkonform zu gestalten, ist eine komplexe Aufgabe und nicht zu unterschätzen. Faire Verfahrensvereinbarungen schaffen die Voraussetzung, dass die Betriebsräte bei der erstmaligen und laufenden Anpassung beteiligt werden. Dies ist im Interesse der Beschäftigten und der Unternehmen. Die Umstellung auf das neue Datenschutzrecht ist eine Chance auch für Beschäftigte, den Datenschutz zu verbessern. Art. 88 DSGVO und § 26 BDSG 2018 eröffnen hierfür genügend betriebliche Handlungs- und Ermessensspielräume. Die Chance sollte aber mit Sorgfalt und Ernsthaftigkeit wahrgenommen werden. Neue Handlungs- und Gestaltungsmöglichkeiten, die das neue Datenschutzrecht beinhaltet, sollten nicht durch vorschnelle Vereinbarungen von den Betriebsräten verschenkt werden. Betriebsräte sollten gelassen abwägen, was gut für die Rechte der Beschäftigten ist. Daher die wichtigste Empfehlung: Rahmenvereinbarungen nur dann abschließen, wenn Betriebsräte die Wirkung von diesen Vereinbarungen auf die Rechte aus dem neuen Datenschutz überblicken und sicher sind, dass sich der Datenschutz für die Beschäftigten verbessert und nicht verschlechtert. ◁

Dr. Eberhard Kiesche,
Arbeitnehmerorientierte Beratung (AoB), Bremen.
eberhard.kiesche@t-online.de

Matthias Wilke,
Datenschutz- und Technologieberatung (dtb), Kassel.
info@dtb-kassel.de

Thomas Berger, Fachanwalt für Arbeitsrecht, Berger Groß Höhmann & Partner Rechtsanwälte.
berger@bghp.de, www.bghp.de

Schutz besonders sensibler Daten

GESUNDHEITSDATEN *Die DSGVO überantwortet den Schutz besonders sensibler Daten im Arbeitsverhältnis weitestgehend dem nationalen Gesetzgeber. Die Umsetzung des Regelungsauftrags schafft indes keine Rechtssicherheit, vielmehr wirft sie eine Reihe neuer Fragen auf.*

VON **BENEDIKT BUCHNER** UND **TIM SPERLICH**

DARUM GEHT ES

1. DSGVO und BDSG 2018 bilden künftig den gemeinsamen Rechtsrahmen für die Verarbeitung besonders schutzwürdiger Beschäftigtendaten.

2. Die Einwilligung ist und bleibt eine zentrale Legitimationsgrundlage für die Verarbeitung von Gesundheitsdaten.

3. Die datenschutzrechtliche Maxime einer freiwilligen Einwilligung ist mit der arbeitsvertraglichen Realität oftmals nur schwer vereinbar.

Die Frage, ob das Datenschutzrecht abstrakt nach mehr und weniger schutzbedürftigen Daten differenzieren soll, ist immer wieder kontrovers diskutiert worden. Das Bundesverfassungsgericht hat bereits in seinem Volkszählungsurteil betont, dass je nach Kontext der Datenverarbeitung auch ein für sich gesehen »belangloses« Datum einen neuen Stellenwert bekommen kann und es unter den Bedingungen der automatischen Datenverarbeitung keine belanglosen Daten mehr gibt. Gute Gründe sprechen daher dafür, die Schutzwürdigkeit personenbezogener Daten gerade nicht abstrakt, sondern stattdessen stets nur in Bezug auf den jeweiligen Verwendungszweck zu beurteilen. Dessen ungeachtet ist jedoch auch die europäische Datenschutz-Grundverordnung (DSGVO), wie schon die Vorgänger-Richtlinie, von der Idee geprägt, dass es bestimmte Kategorien personenbezogener Daten gibt, die »besonders sensibel« sind und die deshalb auch einen »besonderen Schutz [verdienen]« (Erwägungsgrund (ErwGr) 51 der DSGVO). Diese Differenzierung nach mehr oder weniger schutzwürdigen Daten gilt auch für den Beschäftigtendatenschutz. Welche Vorgaben hier künftig unter DSGVO und BDSG 2018 für die Verarbeitung besonderer Kategorien personenbezogener Daten gelten werden, soll im Folgenden überblicksartig dargestellt werden.

Daten über den Gesundheitszustand eines Menschen sind besonders sensible Daten.

DSGVO und BDSG 2018: Alles neu im Datenschutzrecht?

Seit dem 25.5.2018 gilt für den Schutz personenbezogener Daten die DSGVO, ergänzt um ein neues BDSG und eine Vielzahl von bereichsspezifischen Datenschutzvorschriften. Immer wieder ist in diesem Zusammenhang vom »Beginn einer neuen Zeitrechnung« zu lesen, die den Datenschutz künftig prägen soll. In mancherlei Hinsicht trifft dies sicherlich zu, insbesondere was die Durchsetzungskraft des neuen Datenschutzrechts angeht. Verwiesen sei hier nur auf die Bußgeldnorm des Art. 83 DSGVO, die künftig Geldbußen in Millionen- und – je nach Unternehmensgröße – sogar in Milliardenhöhe ermöglichen wird. Was hingegen die materiell-rechtlichen Neuerungen beim Beschäftigtendatenschutz angeht, sind die Neuerungen, die mit DSGVO und BDSG 2018 einhergehen, eher überschaubar – egal, ob es um die Verarbeitung normaler oder besonders sensibler Beschäftigtendaten geht. Auch beim Beschäftigtendatenschutz präsentiert sich die DSGVO als »atypisches Hybrid«[1] aus Verordnung und Richtlinie, das mittels zahlreicher Öffnungsklauseln den Mitgliedstaaten die Befugnis einräumt, im nationalen Recht weitere Regelungen zum Datenschutz zu treffen. Konkret für den Beschäftigtendatenschutz räumt die Öffnungsklausel des Art. 88 DSGVO den Mitgliedstaaten die Befugnis ein, »spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext« zu normieren. Und auch die Regulierung der Verarbeitung besonderer Kategorien personenbezogener Daten (wie etwa Gesundheitsdaten) hat die DSGVO in weitem Umfang dem nationalen Gesetzgeber überantwortet. Art. 9 Abs. 2 DSGVO, dessen Regelungsgegenstand die Zulässigkeit einer Verarbeitung von besonders schutzwürdigen Daten ist, sieht für viele und ganz zentrale Bereiche der Datenverarbeitung (insbesondere für den Arbeits-, Sozial- und Gesundheitsbereich) vor, dass insoweit in den mitgliedstaatlichen Rechtsordnungen konkretisierende Regelungen getroffen werden (s. Art. 9 Abs. 2 lit. b, g, h, i, j DSGVO).

Bei einem Blick auf die Regelungen des BDSG 2018 kann man sich des Eindrucks nicht erwehren, dass der deutsche Gesetzgeber mit dem durch die DSGVO eröffneten Regelungsspielraum nicht sonderlich viel anzufangen wusste. Von der Öffnungsklausel des Art. 88 DSGVO zum Beschäftigtendatenschutz hat der Bundesgesetzgeber dergestalt Gebrauch gemacht, dass die bisherige Regelung des § 32 BDSG a.F. zum Beschäftigtendatenschutz weitestgehend inhaltsgleich in die neue Regelung des § 26 BDSG 2018 überführt wurde. Und auch die neuen BDSG-Regelungen zur Verarbeitung besonderer Kategorien personenbezogener Daten muten nicht sonderlich innovativ an. An sich liegt den in Art. 9 Abs. 2 DSGVO normierten Öffnungsklauseln die Idee zugrunde, dass in der DSGVO der grundsätzliche datenschutzrechtliche Regelungsrahmen gezogen wird und darauf aufbauend dann im nationalen Recht die Regelungen weiter konkretisiert werden. Demgegenüber beschränkt sich jedoch der deutsche Gesetzgeber im neuen BDSG weitestgehend darauf, in § 22 Abs. 1 und § 26 Abs. 3 BDSG 2018 für den Arbeitsbereich die sehr allgemeinen Vorgaben des Art. 9 Abs. 2 DSGVO zu übernehmen.

Die Hoffnung, dass der Gesetzgeber hierzulande die DSGVO zum Anlass nimmt, das bisherige »Regelungswirrwarr«[2] beim Schutz besonders sensibler Daten aufzulösen und in einen konsistenteren und transparenteren Regelungsrahmen zu überführen, hat sich somit bislang nicht erfüllt. Im Gegenteil: Es steht zu befürchten, dass unter der DSGVO die Rechtsanwendung künftig nochmals komplizierter wird, da mit der DSGVO noch eine weitere Regelungsebene hinzutritt und in vielerlei Hinsicht ungeklärt ist, wie das Zusammenspiel zwischen DSGVO und nationalem Recht zukünftig aussehen wird.

Der Regelungsrahmen für die Verarbeitung besonders sensibler Daten

Art. 9 DSGVO, § 26 (insbes. Abs. 3) und § 22 BDSG 2018 regeln künftig den Beschäftigtendatenschutz im Fall der Verarbeitung besonderer Kategorien personenbezogener Daten. Ausgangspunkt ist Art. 9 DSGVO als zentrale Norm der DSGVO für die Verarbeitung sensitiver Daten. Art. 9 Abs. 1 DSGVO normiert ein grundsätzliches Verbot der Verarbeitung sensitiver Daten, wiederholt dem Grunde nach also lediglich das auch ansonsten im Datenschutzrecht geltende Verbotsprinzip (mit Erlaubnisvorbehalt). Der normative Aussagegehalt von Art. 9 Abs. 1 DSGVO beschränkt sich damit im Ergebnis auf eine Aufzählung der verschiedenen »Kategorien« besonders schutzwürdiger Daten.[3] Dazu gehören dann auch – ebenso wie schon unter der Richtlinie – die Gesundheitsdaten, definiert in Art. 4 Nr. 15 DSGVO als personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Auch Schwangerschaft und die Anerkennung als Schwerbehinderter sind solche Gesundheitsdaten im Sinne von Art. 4 Nr. 15 DSGVO.[4]

Art. 9 Abs. 2 DSGVO normiert dann eine Vielzahl von Ausnahmen vom Verbot der Verarbeitung sensitiver Daten, überantwortet allerdings die nähere Ausgestaltung der Anforderungen an eine zulässige Datenverarbeitung für den Bereich des Arbeitnehmerdatenschutzes weitestgehend dem nationalen Gesetzge-

1 Kühling/Martini, EuZW 2016, 448 (449).

2 Weichert, DuD 2017, 538 (542).
3 Schulz in Gola, DSGVO, 2017, Art. 9 Rn. 2.
4 Däubler, Gläserne Belegschaften?, 7. Aufl. 2017, Rn. 194.

Biometrische Daten – wie der Fingerabdruck – unterliegen einem besonderen Datenschutzstandard.

»Der Beschäftigtendatenschutz bleibt bis auf Weiteres eine der größeren Baustellen des Datenschutzrechts.«

BENEDIKT BUCHNER, TIM SPERLICH

ber. In Ausfüllung dieses Regelungsspielraums erlaubt § 26 Abs. 3 BDSG 2018 eine Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses, »wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist«. Damit wiederholt § 26 Abs. 3 BDSG 2018 zunächst einmal das, was schon Art. 9 Abs. 2 lit. b DSGVO in dieser Allgemeinheit normiert, ergänzt lediglich durch die Vorgabe einer Interessenabwägung (»und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt«). Noch minimalistischer präsentiert sich der Gesetzgeber mit der Vorschrift des § 22 BDSG 2018, die den Inhalt der in Art. 9 Abs. 2 DSGVO normierten Öffnungsklauseln zum Teil fast wortgetreu wiedergibt.[5] § 22 Abs. 1 lit. b BDSG 2018 erlaubt (in Umsetzung des Art. 9 Abs. 2 lit. h DSGVO) eine Verarbeitung besonders schutzwürdiger Daten u.a. »für die Beurteilung der Arbeitsfähigkeit des Beschäftigten«. Ebenso soll die Datenverarbeitung zur Beurteilung der Arbeitsfähigkeit aber ausweislich der Begründung des Gesetzesentwurfs zum neuen BDSG auch unter die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses nach § 26 Abs. 3 BDSG 2018 fallen.[6] Sonderlich durchdacht wirkt dies alles nicht.

Insbesondere: Einwilligung als Erlaubnistatbestand

So oder so wird aber auch in Zukunft in vielen Konstellationen die Verarbeitung von besonders schutzwürdigen Daten wie Gesundheitsdaten nur auf Grundlage einer Einwilligung der betroffenen Person erfolgen können. Grundsätzlich kommt der Einwilligung auch im Beschäftigungsverhältnis die Rolle eines Erlaubnistatbestands für die Verarbeitung personenbezogener Daten zu – obwohl dies im Gesetzgebungsprozess zur DSGVO keineswegs unumstritten war. So hieß es im Kommissionsentwurf zur DSGVO noch, dass aufgrund eines klaren Ungleichgewichts im Verhältnis zwischen Arbeitgeber und Arbeitnehmer die Einwilligung »keine rechtliche Handhabe für die Verarbeitung personenbezogener Daten« liefern könne (s. ErwGr 34 des Entwurfs der Kommission). In die endgültige Fassung der DSGVO hat diese Sichtweise dann allerdings keinen Eingang mehr gefunden. Vielmehr beschränkt sich stattdessen ErwGr 155 auf die Feststellung, dass das mitgliedstaatliche Recht und Kollektivvereinbarungen im Rahmen des nach Art. 88 DSGVO bestehenden Regelungsspielraums insbesondere auch »Vorschriften über die Bedingungen, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen«, vorsehen können.

In Ausfüllung dieses Regelungsspielraums regelt § 26 Abs. 2 BDSG 2018 (der nach Abs. 3 Satz 2 Hs. 1 auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten gilt), dass für die Beurteilung der Freiwilligkeit einer Einwilligung »insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen« sind. Viel gewonnen scheint mit dieser Aufforderung, die hinlänglich bekannte Abhängigkeit im Beschäftigungsverhältnis bei der Beurteilung der Freiwilligkeit zu berücksichtigen, nicht. Auch schon vor Geltung der DSGVO und des BDSG 2018 war ein bestehendes Ungleichgewicht zwischen Datenverarbeiter und Betroffenem bei der Frage nach der Freiwilligkeit einer Einwilligung zu berücksichtigen. An dem Umstand, dass die Freiwilligkeit einer datenschutzrechtlichen Einwilligung in vielen Fällen eine bloße Fiktion ist, hat dies kaum etwas geändert – egal, ob es um Schufa-Klausel, Schweigepflicht-Entbindungsklauseln oder eben auch um eine Einwilligung im Beschäftigungskontext geht. Verwiesen sei hier nur auf das Beispiel der Einstellungsuntersuchungen, die stets einer wirksamen Einwilligung des Bewerbers bedürfen.[7] Zu Recht wird in der Begründung des Gesetzesentwurfs zum neuen BDSG darauf hingewiesen, dass insbesondere vor Abschluss eines (Arbeits-)Vertrages Beschäftigte »regelmäßig einer größeren Drucksituation ausgesetzt« sind, ihre Einwilligung in eine Datenverarbeitung zu erteilen.[8] Gleichwohl wird auch künftig gelten, dass Einstellungsuntersuchungen zur Beurteilung der Arbeitsfähigkeit eines Arbeitsplatzbewerbers datenschutzrechtlich zulässig sind, wenn ein Bewerber eine entsprechende Einwilligung erteilt hat.[9] Der Widerspruch zwischen datenschutzrechtlicher Idealvorstellung und arbeitsvertraglicher Realität tritt hier offen zutage, weil auch künftig gilt, was in der Kommentarliteratur in fast schon entwaffnender Offenheit auf den Punkt gebracht wird: »Der Bewerber ist nicht verpflichtet, die Untersuchung durchführen zu lassen. Die Untersuchung kann nur auf freiwilliger Basis durchgeführt werden. Mit der Verweigerung der Einwilligung riskiert der Bewerber freilich seine sofortige Ablehnung.«[10]

Pauschale Informationsverbote

Art. 9 Abs. 2 lit. a DSGVO sieht für den Fall der Verarbeitung besonders schutzwürdiger Daten die Möglichkeit vor, dass der nationale Gesetzgeber die Einwilligung als Legitimationsgrundlage für eine Datenverarbeitung ausschließt. Auch unter der DSGVO hat daher eine Regelung wie die des § 19 Gendiagnostikgesetz (GenDG) weiterhin Bestand, nach der für den Arbeitgeber ein umfassendes, pauschales Verbot der Verarbeitung von genetischen Daten gilt. Selbst wenn hier beispielsweise ein Bewerber seine informationelle Selbstbestimmung im Sinne einer bewussten und gewollten Entscheidung für eine Offenbarung »seiner« genetischen Daten ausüben wollte, bleibt eine Verwendung dieser Daten untersagt. Rechtfertigen lässt sich dieser Ausschluss der informationellen Selbstbestimmung vor allem damit, dass dadurch ein »Wettlauf nach unten« vermieden werden kann: Derjenige, der seine genetischen Daten nicht preisgeben möchte, soll auch nicht dadurch unter Druck geraten, dass andere – beispielsweise Mitbewerber – ihre Daten freiwillig preisgeben. Ein Schweigen soll dem Einzelnen nicht faktisch dadurch zum Nachteil gereichen, dass andere von ihrem Recht zum Schweigen keinen Gebrauch machen. Dass bei genetischen Daten (ebenso wie bei biometrischen und bei Gesundheitsdaten) im nationalen Recht nochmals ein höherer Datenschutzstandard normiert werden darf als in der DSGVO vorgesehen, stellt auch Art. 9 Abs. 4 DSGVO nochmals ausdrücklich klar.

Beschäftigtendatenschutz als Dauerbaustelle

Der Beschäftigtendatenschutz bleibt bis auf Weiteres eine der größeren Baustellen des Datenschutzrechts. Aufgrund der weitreichenden Öffnungsklauseln der DSGVO zur Datenverarbeitung im Beschäftigungskontext liegt der Ball hier weiterhin beim nationalen Gesetzgeber. Gleich doppelt gefordert ist dieser beim Schutz besonders sensibler Beschäftigtendaten, da die DSGVO auch bei den sog. besonderen Kategorien personenbezogener Daten den mitgliedstaatlichen Gesetzgebern die Normierung spezifischer Vorgaben überlässt. Die Bedeutung der Einwilligung als Legitimationsgrundlage für eine Datenverarbeitung ist dabei nur einer von vielen offenen Punkten im Bereich des Beschäftigtendatenschutzes, der noch immer einer Klärung bedarf. ◁

Prof. Dr. Benedikt Buchner LL.M. (UCLA), Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen.

Tim Sperlich, Wissenschaftlicher Mitarbeiter Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen.

5 Weichert, DuD 2017, 538 (542).

6 BT-Drs. 18/11325, S. 98.

7 Kort, NZA-Beilage 2016, 62 (70).
8 BT-Drs. 18/11325, S. 97.
9 Kort, NZA-Beilage 2016, 62 (70).
10 Preis in Erfurter Kommentar zum Arbeitsrecht, 18. Aufl. 2018, § 611a BGB Rn. 294.

»Einsame Rufer in der Wüste!«

INTERVIEW *Warum Betriebsräte bis zum 25.5.2018 einsame Rufer in Punkto neuer Datenschutz waren und wieso sich das bei der Leistungs- und Verhaltenskontrolle immer noch nicht verändert hat. Ein Interview mit den Datenschutzexperten Matthias Wilke und Mattias Ruchhöft von dtb.*

VON **EVA-MARIA STOPPKOTTE**

DARUM GEHT ES

1. Der Datenschutz rückte erst im Jahr 2018 spürbar in den Fokus der Geschäftsleitungen und dann musste es schnell gehen.

2. Bei der Anpassung bestehender Betriebsvereinbarungen auf die DSGVO sollten Betriebsräte genau auf die Einhaltung von Mitbestimmungsrechten achten.

3. Betriebsräte müssen auch auf Datenschutz im Betriebsratsbüro achten. Dabei ist es wichtig, die Datenverarbeitung auf die Zweckbestimmung hin zu überprüfen.

Das Büro für Datenschutz- und Technologieberatung (dtb) mit Sitz in Kassel berät seit 1999 Betriebs- und Personalräte bei der Planung und Umsetzung von Technikeinsatz und entwickelt Datenschutzkonzepte. Im Auftrag von Interessenvertretungen prüft dtb auch die innerbetriebliche Einhaltung des nun neu normierten Datenschutzes und bestehende Betriebsvereinbarungen. Wir befragten zu den aktuellen Neuerungen Matthias Wilke und Mattias Ruchhöft.

Viele klagen über die neuen Regeln zum Datenschutz durch die Datenschutz-Grundverordnung (DSGVO). Könnt Ihr diese Klagen nachvollziehen?

Matthias Wilke: Nein diese Klagen kann ich nicht nachvollziehen. Die Regeln des Datenschutzes sind vor allem für die großen Datensammler geschaffen worden. Firmen wie Facebook, Google und andere. Ein Beispiel: Wenn ich im Internet ein Ticket für die Bahn buche und anschließend ein Hotelzimmer, muss ich für dieses Zimmer mehr bezahlen. Gleiches gilt für Preisangebote im Internet, wenn ich vorher auf einer sogenannten Lifestyle-Webseite gesurft bin. Dieses Verhalten, selbstverständlich mit den Daten der Nutzer zu handeln und daraus Profit zu schlagen, hat nichts mehr mit einem »ehrlichen kaufmännischen Verhalten« zu tun.

Mattias Ruchhöft: Außerdem muss gesagt werden, dass sich in Deutschland an den Grundsätzen des Datenschutzes, also keine Verarbeitung personenbezogener Daten ohne einen Zweck, nichts geändert hat. Man muss sich wundern, wenn in namhaften Zeitungen dies nun als komplett neu definiert wird. Beim Datenschutz geht es um die Einhaltung unseres Rechts auf informationelle Selbstbestimmung gerade gegenüber den Firmen, die mein Kollege gerade genannt hat.

Ihr habt ja schon während der 2-jährigen Übergangsfrist zur DSGVO zahlreiche Betriebsratsgremien geschult. Wo hat der Schuh die Kolleginnen und Kollegen datenschutzrechtlich am meisten gedrückt?

Mattias Ruchhöft: In unseren Beratungen war ein interessantes Phänomen zu beobachten. Die Betriebs- und Personalräte waren lange Zeit »einsame Rufer in der Wüste«, wenn es um die Vorbereitung ihrer Arbeitgeber auf die neuen Datenschutzregeln ging. Der Datenschutz rückte erst im Jahr 2018 spürbar in den Fokus der Geschäftsleitung und dann sollte es ganz schnell gehen. Und Betriebs- und Personalräte kämpften auch um die Einhaltung der Grundlagen des Datenschutzes und um ihre Mitbestimmung bei technischen Systemen zum Schutz der Arbeitnehmer vor einer allumfassenden Leistungs- und Verhaltenskontrolle. Dies insbesondere in den Zeiten von Big Data und künstlicher Intelligenz.

Matthias Wilke: Ja, und dabei drückte der Schuh in vielen Unternehmen insbesondere bei der Einhaltung der Grundsätze zum Datenschutz. Gerade bei der Erforderlichkeit der Datenverarbeitung liegen Arbeitgeber und Arbeitnehmervertretungen im Clinch. Die vielen Dashboards und Auswertungen zu einzelnen Beschäftigten werden in vielen Fällen mit dem Arbeitsverhältnis erklärt, obwohl diese detaillierte Auswertung des Arbeitsverhaltens und der Leistungsbeurteilung nicht dazu gehört. Betriebs- und Personalräte haben schon lange auf diese Grundsätze des Datenschutzes hingewiesen und darauf, dass eine kollektivrechtliche Vereinbarung als Erlaubnis für die Verarbeitung personenbezogener Daten von Beschäftigten dienen kann. Dieses Ansinnen blieb in vielen Fällen unbeachtet und gewann dann im Frühjahr 2018 an Brisanz in vielen Unternehmen und öffentlichen Stellen. Der Schutz vor Leistungs- und Verhaltenskontrolle als zentraler Ansatz der Mitbestimmung bei IT-Systemen ist auch eine der Grundlagen des Datenschutzes. Da drückt der Schuh auch nach dem 25.5.2018 und nach den zwei Jahren Übergangsfrist.

Worauf sollten Betriebsräte bei der Anpassung von Betriebsvereinbarungen auf die DSGVO und das neue BDSG genau achten?

Matthias Wilke: Bei der Anpassung bestehender Betriebsvereinbarungen oder Dienstvereinbarungen auf die DSGVO sollten Betriebsräte insbesondere auf die Einhaltung der Mitbestimmungsrechte achten. Einige Arbeitgeber versuchten über allgemein gültige Rahmenvereinbarungen zum Beschäftigtendatenschutz diese Anpassungen vorzunehmen. Dabei rücken die Mitbestimmungsrechte in den Hintergrund. Außerdem sollten die Betriebs- und Personalräte die technische Umsetzung der Betriebs- und Dienstvereinbarungen direkt am System überprüfen. Wir haben in den vergangenen Jahren über 300 Systeme im Auftrag der Arbeitnehmervertretung auditiert und nur ein einziges Mal feststellen können, dass alle gesetzlichen und durch Betriebs- und Dienstvereinbarungen vereinbarten Anforderungen wie beispielsweise Zugriffsberechtigungen oder Auswertungen nicht entsprechend technisch umgesetzt waren.

Mattias Ruchhöft: Bei der Anpassung bestehender Dienst- und Betriebsvereinbarungen muss auf die Darlegung der Zwecke, für die personenbezogene Daten der Beschäftigten verarbeitet werden sollen, geachtet werden. Sind diese in den bestehenden Vereinbarungen klar aufgezeigt und formuliert, ist der Anpassungsbedarf nicht mehr sehr groß. Dazu gehört auch ein belastbares Berechtigungskonzept, in dem die Rollen beispielsweise von Führungskräften auf die Datenfelder eines Systems dargelegt sind. Ist dann noch ein Löschkonzept in der Betriebsvereinbarung beinhaltet, beschränkt sich aus meiner Sicht der Anpassungsbedarf auf eventuell vorhandene Zitate aus dem alten Bundesdatenschutzgesetz (BDSG).

Viele Arbeitgeber nutzen die DSGVO ja auch dazu, Informationspflichten, die der Betriebsrat einfordert, beispielsweise zum Betrieblichen Eingliederungsmanagement, zu negieren. Es verstoße gegen den Datenschutz, wird dann lapidar gesagt. Was könnt Ihr den Betriebsräten hier empfehlen?

Mattias Ruchhöft: Die Regelungen des BDSG 2018 hierzu sind eindeutig. Die Datenverarbeitung der Betriebs- und Personalräte zum Zweck der Mitbestimmungsrechte aus dem BetrVG, den unterschiedlichen Personalvertretungsgesetzen sowie zur Kontrolle von Vereinbarungen oder aus Tarifverträgen ist ausdrücklich erlaubt. Damit sind auch die Informationsrechte des Betriebs- und Personalrats abgedeckt.

Matthias Wilke: Nach meiner Erfahrung wird nach einer Prüfung, die der Betriebsrat beim betrieblichen Datenschutzbeauftragten anfordert, und nach dem Hinweis auf die Informations- und Beteiligungsrechte dann der Anfrage des Betriebsrats häufig auch stattgegeben. Wir empfehlen den Betriebs- und Personalräten in unseren Seminaren, dass sie sich den Zweck ihrer Anfragen im Sinne des Datenschutzes klarmachen. Welcher Bereich des Vertretungs- oder Betriebsverfassungsgesetzes deckt die konkrete Anfrage oder das Beteiligungsrecht ab? Und auf diesen sollten sie bei der Anfrage direkt hinweisen.

Und wenn es um den Datenschutz im Betriebsratsbüro geht, welche zwei Tipps könnt Ihr den Interessenvertretungen mit auf den Weg geben?

Matthias Wilke: Wie eben bereits erwähnt, sind im BDSG 2018 die Rechte der Interessenvertretung, personenbezogene Daten der Beschäftigten zu verarbeiten, hinterlegt. Wir empfehlen den Kolleginnen und Kollegen, ihre Datenverarbeitung auf die Zweckbestimmung hin zu überprüfen. Dazu sollten sie ein Verzeichnis von Verarbeitungstätigkeiten entsprechend dem früheren Verfahrensverzeichnis über ihre Datenverarbeitung erstellen, um diese zu dokumentieren.

Matthias Wilke
Geschäftsführer Datenschutz- und Technologieberatung (dtb), Kassel.

Mattias Ruchhöft
Technologieberater bei dtb und Fachautor beim Bund-Verlag.

Mattias Ruchhöft: Und als zweiten Tipp geben wir den Betriebs- und Personalräten mit auf den Weg, dass sie einen Beauftragten des Gremiums für den Datenschutz ernennen sollten. Der betriebliche Datenschutzbeauftragte darf als Vertreter des Arbeitgebers das Büro der Interessenvertretung nicht kontrollieren. Somit ist ein Mitglied des Gremiums, das für den Datenschutz zuständig ist, der richtige Weg. Dieser ist dann entsprechend zu schulen und muss für seine Tätigkeiten den zeitlichen Freiraum haben.

Wie sieht es mit der Videoüberwachung aus? Worauf müssen Betriebsräte hier jetzt besonders achten?

Mattias Ruchhöft: Die Videoüberwachung stellt aus der Sicht des Datenschutzes eine umfassende Leistungs- und Verhaltenskontrolle dar. Für diese systematische Überwachung, die ein besonderes Risiko für die Rechte und Freiheiten der Betroffenen darstellen kann, sieht die DSGVO eine Datenschutz-Folgenabschätzung vor, in der diese Risiken durch geeignete Maßnahmen minimiert werden sollen. Die DSGVO sieht diese Folgenabschätzung für die Videoüberwachung in öffentlich zugänglichen Bereichen vor. Im Gesetz ist vorgesehen, dass die Betroffenen im Verfahren der Folgenabschätzung gehört werden sollen. Dies sollten die Interessenvertretungen einfordern. Zumal durch eine Datenschutz-Folgenabschätzung auch Informations- und Beteiligungsrechte berührt sein können, wenn beispielsweise eine Software für die Umsetzung der Folgenabschätzung genutzt wird.

Matthias Wilke: Neben der Folgenabschätzung bleiben auch nach neuem Recht die Grundlagen des Beschäftigtendatenschutzes bei der Videoüberwachung erhalten: Keine Überwachung von dauerhaften Arbeitsplätzen der Arbeitnehmer. Diese Bereiche sind entsprechend auszupixeln und unkenntlich zu machen. Zudem dürfen die Videobilder nur diejenigen anschauen, die für den Zweck der Videoüberwachung, zum Beispiel Wahrung des Hausrechts, zuständig sind. Das sind dann die Vertreter einer Sicherheitsfirma, nicht jedoch die Geschäftsleitung oder andere Führungskräfte des Arbeitgebers, was wir auch in unseren Beratungen schon erlebt haben. ◁

Eva-Maria Stoppkotte,
Assessorin jur.,
verantwortliche Redakteurin
Arbeitsrecht im Betrieb.

IMPRESSUM

Arbeitsrecht im Betrieb EXTRA
Sonderausgabe für dtb – Kassel

Redaktion
Eva-Maria Stoppkotte
eva-maria.stoppkotte@bund-verlag.de

Anschrift für Redaktion und Verlag
Heddernheimer Landstraße 144, 60439 Frankfurt/Main
Tel. +49 (0)69/79 50 10 – 0
Fax +49 (0)69/79 50 10 – 18

Verlag
Bund-Verlag GmbH
Geschäftsführer
Rainer Jöde

Geschäftsbereich Zeitschriften
Bettina Frowein

Leser- und Aboservice
Bund-Verlag GmbH, 60424 Frankfurt/Main
Tel. +49 (0) 69/79 50 10 – 96
Fax +49 (0)69/79 50 10 – 12
E-Mail: abodienste@bund-verlag.de

Gestaltung und Satz
fsvk.design

Druck
alpha print medien AG, Darmstadt

Mit Namen gezeichnete Beiträge sowie Beilagen und Anzeigen geben nicht unbedingt die Meinung der Redaktion oder des Verlages wieder.

Redaktionsschluss
27.6.2018

Bildnachweise
Titelbild, S. 4, 6: © gettyimages.com, Emrah Turudu | S. 8, 14, 18, 23, 26, 33, 34, 36, 39, 52, 56, 58: © iStock.com, Jorisvo, AndreyPopov, TommL, pagadesign, Predrag Vuckovic, IPGGutenbergUKLtd, monsitj, vm, Nikada, mediaphotos, alvarez, Irina Vodneva | S. 30: LfDI BW, Kristina Schäfer | S. 29: Wikimedia Commons: Public Domain, Kasselklaus | S. 43: Fotolia.com, © freshidea

Datenschutz
Die zur Abwicklung des Abonnements erforderlichen Daten werden nach den Bestimmungen der EU-DSGVO und des BDSG verwaltet.

Herausgeber
dtb – Datenschutz- und Technologieberatung
Matthias Wilke
Theaterstr. 1, 34117 Kassel
Tel.: 0561 / 70 575 70
Fax.: 0561 / 70 575 71
Mail: info@dtb-kassel.de
Web: www.dtb-kassel.de

verantwortlich
Matthias Wilke
dtb – Datenschutz- und Technologieberatung
Mail: matthias.wilke@dtb-kassel.de
Web: www.dtb-kassel.de

Redaktionelle Bearbeitung
Dr. Eberhard Kiesche
www.aob-bremen.de

Weiterbildung für Betriebs- und Personalräte

Nur bei uns:

Weiterbildung zur

Zertifizierte Fachkraft für Datenschutz bei IT-Systemen

Weitere Informationen zu Terminen und Preisen finden Sie auf unserer Internetseite:
www.dtb-kassel.de/datenschutzfachkraft
oder scannen Sie den QR-Code:

dtb – Datenschutz- und Technologieberatung
Theaterstraße 1 • 34117 Kassel • Telefon (05 61) 70 575 70 • Telefax (05 61) 70 575 71
E-Mail: info@dtb-kassel.de • www.dtb-kassel.de