Hans Böckler Stiftung
Mitbestimmung · Forschung · Stipendien

STUDY

Nr. 328 · Juni 2016

DATENSCHUTZ IM KONZERN DER DEUTSCHEN BAHN AG

Reihe Praxiswissen Betriebsvereinbarungen

Eberhard Kiesche

MF MITBESTIMMUNGS-FÖRDERUNG

BETRIEBS-VEREINBARUNGEN

Die Reihe Betriebsvereinbarungen wird herausgegeben
von Dr. Manuela Maschke, Hans-Böckler-Stiftung.

Die Hans-Böckler-Stiftung ist das Mitbestimmungs-, Forschungs- und Studienförderungswerk des DGB. Sie ist in allen ihren Aufgabenfeldern der Mitbestimmung als Gestaltungsprinzip einer demokratischen Gesellschaft verpflichtet. Sie wirbt für diese Idee, unterstützt Mandatsträger in Mitbestimmungsfunktionen und tritt für erweiterte Mitbestimmungsrechte ein.

Hans Böckler Stiftung
Mitbestimmung · Forschung · Stipendien

STUDY

Nr. 328 · Juni 2016

DATENSCHUTZ IM KONZERN DER DEUTSCHEN BAHN AG

Reihe Praxiswissen Betriebsvereinbarungen

Eberhard Kiesche

MF MITBESTIMMUNGS-FÖRDERUNG

BETRIEBS-VEREINBARUNGEN

Der Autor

Dr. Eberhard Kiesche, AoB Bremen
Berater für Arbeits- und Gesundheitsschutz, Betriebsverfassungsrecht, Betriebliches Eingliederungsmanagement und Beschäftigtendatenschutz

Redaktion
Dr. Manuela Maschke, Hans-Böckler-Stiftung

Kontakt
Telefon +49 211 7778-167
betriebsvereinbarung@boeckler.de

ISBN 978-3-86593-236-5

Lektorat: Anne Gampert, Berlin
Satz: DOPPELPUNKT, Stuttgart

INHALT

ABKÜRZUNGSVERZEICHNIS

BAG	Bundesarbeitsgericht
BDS	Beschäftigtendatenschutz
BGB	Bürgerliches Gesetzbuch
BKU	Bürokommunikationslösung
BvD	Berufsverband der Datenschutzbeauftragten Deutschlands
BYOD	Bring your own device
CDA	Organisationseinheit Konzerndatenschutz Audit
DB	Deutsche Bahn
DS	Datenschutz
DSB	Datenschutzbeauftragte/r
DV	Datenverarbeitung
FDS	Fachkräfte für Datenschutz
GDD	Gesellschaft für Datenschutz und Datensicherheit
GG	Grundgesetz
IT	Informationstechnik
JFD	Jour Fixe Datenschutz
KBV	Konzernbetriebsvereinbarung
KBR	Konzernbetriebsrat
KDSB	Konzerndatenschutzbeauftragte/r
KID	Konzerninterne Datenflüsse
RKBV	Rahmenkonzernbetriebsvereinbarung
VbV	Vertrauensperson Datenschutz beim Vorstand C
VPDS	Vertrauenspersonen für den Datenschutz

VORWORT

Zu Beginn des Jahres 2009 geriet die Deutsche Bahn AG in eine datenschutzrechtliche Krisensituation. Als Konsequenz aus Verstößen gegen das Datenschutzrecht wurde eine Konzernbetriebsvereinbarung Beschäftigtendatenschutz entwickelt, verhandelt und abgeschlossen mit dem Ziel, einen transparenten und vorbildlichen Datenschutz zu verwirklichen.

Der Konzern und seine Mitbestimmungsakteure haben auf die Verfehlungen umfassend reagiert und neue Verfahrensweisen entwickelt. Die KBV Beschäftigtendatenschutz geht im DB-Konzern allen anderen internen Regelungen vor, in denen die Verarbeitung von Beschäftigtendaten geregelt wird. Auf diese Weise wird der Datenschutz konkret, setzt pragmatisch die Rechte der Beschäftigten im Beschäftigtendatenschutz um. Ein vorbildliches Datenschutzmanagementsystem wurde ins Leben gerufen bestehend aus Transparenz, Nachhaltigkeit und Vertrauen. Das ist nicht selbstverständlich.

Das Ziel der Publikation ist, die Veränderungen im Konzern durch diese Regelungen ausführlich zu dokumentieren und einzuordnen. Dafür wurden Hintergründe recherchiert und die gesammelten Erfahrungen maßgeblich beteiligter Akteure dokumentiert. Expertinnen und Experten des Betriebsrats, der Arbeitgeberseite und des Datenschutzes kamen zu Wort wie auch beteiligte externe Berater der Arbeitnehmerseite.

An dieser Stelle geht ein sehr herzlicher Dank an alle Beteiligten, besonders an die Interviewpartner für ihr Vertrauen und ihre Offenheit. Die Interviews wurden zwischen Sommer 2013 und Frühjahr 2014 geführt.

Weil einzelne Regelungen ausführlich kommentiert sind, kann diese Fallstudie anderen Akteuren als Handlungshilfe dienen für die Gestaltung eigener Datenschutzkonzepte und Betriebsvereinbarungen. Den Erfahrungen und Lösungswegen wird daher ausführlich Platz eingeräumt.

Wir wünschen eine anregende Lektüre!

Dr. Manuela Maschke

1 EINE DATENAFFÄRE KOMMT AN DIE ÖFFENTLICHKEIT

Anfang 2009 wurde eine Datenschutzhavarie im Konzern Deutsche Bahn AG offenkundig, die das Vertrauen der Beschäftigten in das Unternehmen schlagartig erschütterte.

1.1 Verstöße gegen den Datenschutz

Was war passiert? Im Zuge der Prävention von Korruption und Betrug im Unternehmen wurden im DB-Konzern 173.000 Beschäftigte einem Screening unterzogen – unrechtmäßig und heimlich, ohne konkreten Anlass oder Verdacht. Um Korruption zu bekämpfen wurde untersucht, inwieweit ihre Daten – hier: Bankverbindungen – mit Lieferantendaten übereinstimmten und somit Beschäftigte von der Auftragsvergabe durch die Bahn profitierten. Nahezu alle Mitarbeiter und Mitarbeiterinnen sowie ihre Angehörigen wurden von 2002 bis 2005 dem automatisierten systematischen Datenabgleich unterworfen, das heißt auch Gleisarbeiter, Handwerker und Reinigungskräfte, die nichts mit dem Einkauf zu tun hatten. Das Screening führte zu 300 Treffern und in 150 Fällen zu verschärfter Beobachtung (Däubler 2015, Rdnr. 2g, Kock/Francke 2009, S. 646).

In konkreten Verdachtsfällen wurden Mitarbeiter bzw. Führungskräfte vollständig durchleuchtet, indem Festplatten und E-Mail-Dateien am Arbeitsplatz kopiert, Büros durchsucht, private Geld- und Kontobewegungen aufgelistet und Reisetätigkeit und Familienverhältnisse festgehalten wurden. Zudem wurden Detekteien eingeschaltet, um den privaten Lebensstil der Mitarbeiter einschließlich der Ehe- oder Lebenspartner und deren Kontodaten zu überprüfen.

Die Ermittlungsberichte wurden unsystematisch in Akten aufbewahrt, auch in Fällen, in denen sich die Vorwürfe nicht bestätigten.

Nachdem der Stern einen Bericht zu den Vorkommnissen bei der Bahn veröffentlicht hatte, gab es helle Empörung bei den Beschäftigten im Konzern und in der Medienöffentlichkeit. Sonderermittler wurden eingesetzt. Bis Juni 2009 erstellten sie einen Bericht darüber, wie die durchgeführten Compliance-Maßnahmen datenschutzrechtlich zu bewerten waren. Der Bericht zeigte erhebliche Datenschutzverstöße auf. Auch die Aufsichtsbehörde

bewertete die Überwachung als zu umfangreich, massiv und datenschutzrechtlich unzulässig (Dix 2009, S. 118 f.; Kock/Francke 2009, S. 651). Im Einzelnen wurden folgende Verstöße angeführt:

- Die Untersuchungen wurden ohne wirksame gesetzliche Grundlage durchgeführt. Es fehlten zu dokumentierende tatsächliche Anhaltspunkte für einen Verdacht (Mähner 2010, S. 379, 383).
- Die Maßnahmen wurden heimlich bzw. verdeckt durchgeführt, das heißt weder die Beschäftigten noch die Interessenvertretungen wurden im Vorfeld informiert.
- Die Compliance-Maßnahmen waren unverhältnismäßig: Nahezu alle Beschäftigten wurden überprüft, die Maßnahmen wurden nicht auf besonders gefährdete Mitarbeitergruppen beschränkt.
- wDie latente Dauerüberwachung verstieß gegen das Grundrecht auf informationelle Selbstbestimmung (Dix 2009, S. 119).

Die zuständige Aufsichtsbehörde für den Datenschutz in Berlin – der Beauftragte für Datenschutz und Informationsfreiheit – verhängte ein Bußgeld in Höhe von 1.123.503,50 Euro. Der Konzernbetriebsrat rief eine Sondersitzung ein, zu der der gesamte damalige Vorstand erschien. Letzten Endes führten die Ereignisse dazu (vgl. Steinkühler 2009, S. 1294 f.), dass fast der gesamte Vorstand ausgetauscht und ein neuer Konzern-Vorstandsvorsitzender berufen wurde.

1.2 Ursachen der Datenschutzhavarie

Im Folgenden wird der Frage nachgegangen: Welche Gründe für die Datenschutzkrise führen die betrieblichen Akteure heute an? Vor den Ereignissen verfügte der DB-Konzern bereits über eine Datenschutzorganisation, über Konzernrichtlinien zum Datenschutz sowie über Betriebsvereinbarungen. Dennoch kam es zu diesem Verstoß gegen Gesetze, konzerninterne Richtlinien, Betriebsvereinbarungen und bahninterne Vorgaben. Wie war das möglich?

Unzureichende Strukturen, Prozesse und Ressourcen für den Datenschutz

Offensichtlich war das für den im gesamten DB-Konzern zuständige Personal allein angesichts der Ressourcen – das heißt angesichts der organisatorischen Ausprägung und personellen Ausstattung – klar überfordert. In der DB-Hol-

ding bestand für die zentrale Datenschutzorganisation eine sehr kleine Organisationseinheit: Nur ein Konzerndatenschutzbeauftragter war für ca. 100 DB-Gesellschaften bestellt und für ca. 200.000 Beschäftigte zuständig. Er wurde von drei Mitarbeitern und einem Sekretariat mit zwei Halbtagskräften unterstützt. Zudem konzentrierte sich der damalige Datenschutzbeauftragte vermutlich auf den Kundendatenschutz. In den einzelnen DB-Gesellschaften gab es vereinzelt Datenschutzbeauftragte und zusätzliche Ansprechpartner vor Ort. Diese bekamen aber für ihre Aufgaben im Datenschutz keine zeitliche Entlastung.

Verselbstständigung der Konzernfunktionen Konzernsicherheit und Revision

Zudem war der Bereich Datenschutz vor der Datenaffäre (Fritz 2012, S. 197) auf Vorstandsebene dem Bereich der Konzernsicherheit – und nicht mit der Konzernrevision und Konzernsicherheit gleichrangig einem gemeinsamen Vorstand untergeordnet.

Seit 2007 wurde ein eigenständiger Bereich Compliance aufgebaut. Konzernsicherheit und Konzernrevision verselbständigten sich offenbar mit eigenen internen Ermittlungen, ohne die anderen zentralen Bereiche einzubeziehen und zu informieren. Wer welche Compliance-Maßnahmen ergriff, war intransparent und blieb verdeckt. Allen Mitarbeitern wurde Misstrauen entgegengebracht, indem sie beim Screening unter Generalverdacht gestellt wurden. Der lautere Zweck, dadurch die Einhaltung der gesetzlichen Vorschriften sicherzustellen, heiligt nicht alle Mittel (Fritz 2012, S. 198). Das Datenscreening insgesamt war offenkundig nicht compliant und nicht datenschutzkonform (Mähner 2010).

1.3 Vertrauensverlust seitens der Mitarbeiter

Der Datenschutzskandal führte zu einem tiefen Misstrauen und vor allem zur Verunsicherung bei den Mitarbeitern und Führungskräften im Konzern. Die Informationen aus dem Konzern über die Reichweite des Skandals waren zu Beginn nur spärlich, da die Aufklärung noch andauerte. In dieser Situation musste der Konzernbetriebsrat entscheiden, wie er reagieren sollte und was aus seiner Sicht zu tun war.

2 AUF DEM WEG ZUR KONZERNBETRIEBSVEREINBARUNG BESCHÄFTIGTENDATENSCHUTZ (KBV BDS)

Nachfolgend wird der Prozess beschrieben, der mit der Unterschrift unter der Konzernbetriebsvereinbarung Beschäftigtendatenschutz (KBV BDS) endete. Hier interessieren insbesondere die Sichtweisen der beteiligten Akteure und das gemeinsame Vorgehen bei den Verhandlungen.

2.1 Neuer Vorstand signalisiert vorbildlichen Datenschutz – der Konzernbetriebsrat reagiert

Zu Beginn der datenschutzrechtlichen Krise war das Ausmaß der Datenschutzverstöße noch unklar. Der Konzernbetriebsrat (KBR) musste sich zunächst umfassend informieren. Er rief zu diesem Zweck eine Sondersitzung ein, an der der gesamte damalige Vorstand teilnahm.

Noch während die eingesetzten Sonderermittler tätig waren und das Ausmaß der Affäre noch unklar war, entwickelte der KBR die Idee, eine Konzernbetriebsvereinbarung „Persönlichkeitsrechte" vom damaligen Personalvorstand zu fordern – zumal der neue Vorstand bzw. der neue Konzern-Vorstandsvorsitzende nach wenigen Monaten öffentlich versprach, einen „transparenten und vorbildlichen Datenschutz" zu schaffen und eine Vorbildfunktion zu übernehmen. Der neue Konzernvorstand akzeptierte und bezahlte nicht nur die Geldbuße der Aufsichtsbehörde; er erklärte darüber hinaus den Datenschutz zu einer seiner obersten Prioritäten und übernahm damit eine Modellfunktion für die gesamte deutsche Wirtschaft (Dix 2009, S. 4).

Nachdem der Bericht der Sonderermittler vorlag, entschied der KBR, sich auf die Verwirklichung des Grundrechts auf informationelle Selbstbestimmung im Sinne des Volkszählungsurteils von 1983 (Bundesverfassungsgericht, auch BVerfG 1 BvR 256/08 vom 2.3.2010, Rdnr. 226 ff.) zu konzentrieren. Er wollte den Arbeitnehmerdatenschutz im Konzern komplett im Sinne des Persönlichkeitsschutzes mit Bezug auf Art. 2 Grundgesetz (GG) sowie die stärkere Gewährleistung von Mitbestimmungsrechten der Interessenvertretungen neu regeln und vorbildlich aufstellen. Dies wird letztlich in § 1 Abs. 2 KBV BDS ausdrücklich als Zielvorstellung formuliert: „Mit dieser Vereinbarung sollen Persönlichkeitsrechte der Beschäftigten und zugleich die

Rechte der Interessenvertretungen gewahrt und geschützt werden. Beides ist gleichermaßen entscheidend für die hiermit erklärte Zielstellung eines vorbildhaften Beschäftigtendatenschutzes im DB-Konzern."

2.2 Das Eckpunktepapier „Arbeitnehmerdatenschutz": Der erste Schritt zu einem vorbildlichen Datenschutz im DB-Konzern

Arbeitgeber und KBR bildeten ein Verhandlungsgremium, das sich auf den Weg machte zu einem vorbildlichen Datenschutz. Die Interviews mit den beteiligten Akteuren zeigen: In den intensiven Verhandlungen bildete sich ein gemeinsames Verständnis eines vorbildlichen Datenschutzes heraus, das aus Sicht aller Akteure heute noch gelebt wird und hilft, aktuelle Datenschutzherausforderungen und -probleme zu lösen. An der entscheidenden abschließenden Verhandlung nahm der Vorstand Compliance, Datenschutz, Recht und Konzernsicherheit (nachfolgend Vorstand C genannt) persönlich teil.

Zum Verhandlungsteam des KBR gehörten überwiegend Betriebsräte aus dem KBR-Ausschuss „Datenschutz und Neue Technologien" sowie ein externer Sachverständiger gemäß § 80 Abs. 3 BetrVG, der sowohl im Arbeits- als auch im Datenschutzrecht als ausgewiesener Experte galt. Das KBR-Gremium erstellte Eckpunkte zu einem vorbildlichen Arbeitnehmerdatenschutz, erarbeitete ein grundlegendes Verständnis von Datenschutz im Betrieb und initiierte in dem Verhandlungsgremium mit dem Arbeitgeber die Erstellung eines gemeinsamen Eckpunktepapieres zum Arbeitnehmerdatenschutz. Letzteres galt als wichtigster Meilenstein des Projektes „Vorbildlicher Datenschutz". Es sollte aus Sicht der Akteure vor allem der Befriedung im Konzern dienen und möglichst zügig den Worten Taten folgen lassen. Vorbild für die Strategie des KBR war ein ähnlich gelagertes Vorgehen in Tarifverhandlungen.

Aus Sicht des KBR ergab sich die Notwendigkeit, vor Beginn der Verhandlungen den vorhandenen Datenschutz auf null zu stellen und grundlegend neu zu beginnen. Gespräche über den Datenschutz zum Beispiel mit Führungskräften zeigten deutlich: Ihnen war vielfach ihre Verantwortung für die Integrität der Daten ihrer Mitarbeiter nicht bewusst.

Das Eckpunktepapier wurde am 24.11.2009 abgeschlossen. Es findet sich in fast allen Punkten vollständig in der letztlich abgeschlossenen KBV Beschäftigtendatenschutz wieder. Daher erwies sich das Vorgehen mit dem Eckpunktepapier aus Sicht der Verhandlungsführerin auf Seiten der Betriebsräte als äußerst nützlich: Es diente dazu, Ziele, Begriffe und Inhalte des betriebli-

chen Datenschutzes zu klären, und legte das datenschutzrechtliche Grundverständnis fest, auf das sich die Verhandlungspartner geeinigt hatten. Das gemeinsame Ziel formuliert §1 Abs. 1 Satz 2 KBV BDS letztendlich bündig wie folgt: „Diese Vereinbarung ist die verbindliche Basis aller Regelungen zum Beschäftigtendatenschutz im DB-Konzern. Ihr Ziel ist es, einen rechtskonformen, sicheren und nachhaltigen Beschäftigtendatenschutz im gesamten DB-Konzern zu gewährleisten." Dabei darf nicht verkannt werden: Die datenschutzrechtliche Krisensituation im Jahr 2009, sowie der öffentliche Druck hielten die Verhandlungspartner zur Einigung an und förderten so tatsächliche Kompromiss- und Lernbereitschaft. In der deutlichen personellen Stärkung des Datenschutzes waren Arbeitgeber und Konzernbetriebsrat sich schnell einig.

Einige inhaltliche Punkte im Prozess zur Verabschiedung des Eckpunktepapiers waren jedoch umstritten. Eine große Herausforderung aus der Sicht der Betriebsräte und des neuen Vorstands C bestand darin, dass der Skandal zu einem enormen Vertrauensverlust im DB-Konzern geführt hatte. Das Vertrauen musste wieder aufgebaut werden, insbesondere zwischen den Betriebsparteien. Beim Eckpunktepapier gab es insbesondere bei der dezentralen Datenschutzorganisation und bei der Sachverhaltsaufklärung im Wege der doppelten Verhältnismäßigkeitsprüfung inhaltliche Streitpunkte. Mitglieder des KBR verdeutlichen in den Interviews, dass der KBR einige seiner ursprünglichen Ziele im Laufe der Verhandlungen modifizierte und etwa der Bildung einer zentralen sowie einer dezentralen Datenschutzorganisation zustimmte. Damit ließ er letzten Endes die Forderung nach ausschließlich dezentraler Organisation des Datenschutzes fallen. Auch das Ziel, regelmäßige Datenschutzaudits durch externe Stellen zu vereinbaren, musste der KBR aufgeben. Durchsetzen konnte er jedoch, dass überhaupt eine dezentrale Datenschutzorganisation gebildet wurde.

Aufgrund der vielen Datenschutzskandale in der Privatwirtschaft, die ab 2008 die Öffentlichkeit regelmäßig aufschreckten, reagierte die Politik kurz vor der Bundestagswahl 2009 und schuf mit §32 Bundesdatenschutzgesetz (BDSG) eine erste Rechtsgrundlage zum Arbeitnehmerdatenschutz. Die Bedeutung des §32 BDSG wurde durch den Gesetzgeber relativiert: Er sollte nur vorläufig gelten, gleichzeitig wurde ein eigenständiges Arbeitnehmerdatenschutzgesetz in Aussicht gestellt. Zudem sollte sich laut Gesetzesbegründung am Stand des Beschäftigtendatenschutzes, wie er bislang von der Rechtsprechung geprägt war, nichts ändern.

Die Novellierung des BDSG im Jahr 2009 war für die betrieblichen Akteure nach ihren Aussagen eher irrelevant und deshalb für die Betriebspartei-

en keine große Hilfe. Als die schwarz-gelbe Koalition ihr Vorhaben ankündigte, ein Beschäftigtendatenschutzgesetz zu verabschieden, und 2010 die Bundesregierung einen Gesetzentwurf dazu vorlegte, einigte sich das gemeinsame Verhandlungsgremium darauf, gesetzliche Änderungen nicht abzuwarten. Der Gesetzentwurf Beschäftigtendatenschutz ist im Jahr 2013 endgültig gescheitert.

2.3 Vorgehensweise des KBR beim Abschluss der KBV BDS

Der KBR setzte bei der Entwicklung KBV BDS auf Arbeitsteilung. In regelmäßigen Abständen wurde der Verhandlungsstand dem KBR-Ausschuss Datenschutz und Neue Technologien insgesamt vorgestellt und darüber berichtet. Im Gesamtgremium wurde auch an einem gemeinsamen Verständnis von Datenschutz gearbeitet. Von Beginn an zog der KBR einen Sachverständigen hinzu und ernannte für das KBR-Verhandlungsgremium eine Verhandlungsführerin.

Der Vorstand C hatte einen zu diesem Zeitpunkt noch externen Sachverständigen mit der Erstellung eines KBV-Entwurfes beauftragt, den die Arbeitgeberseite dann dem KBR-Verhandlungsgremium vorlegte. Dem KBR kam es entscheidend darauf an, dass sowohl Aufbau als auch Inhalt der KBV das zugrunde liegende Eckpunktepapier deutlich erkennen ließen. Daher verfasste die KBR-Verhandlungsführerin auf Basis des Eckpunktepapieres einen KBV-Entwurf als „Arbeitspapier“. Er wurde mit dem KBR-Sachverständigen und dem KBR-Verhandlungsgremium abgestimmt und diente als Grundlage weiterer Verhandlungen mit der Arbeitgeberseite.

Die Verhandlungspartner waren sich darin einig, das final verhandelte „KBV-BDS-Papier“ vor der KBR-Beschlussfassung und Unterzeichnung der zuständigen Aufsichtsbehörde vorzulegen und durch diese bewerten zu lassen. Nach Vorlage des Entwurfes bei der Aufsichtsbehörde klärte diese erste Rückfragen mit dem KBR-Sachverständigen. Die KBR-Verhandlungsführerin nahm einen Termin bei der zuständigen Aufsichtsbehörde wahr und berichtete hierzu im Anschluss den Verhandlungspartnern. Die Anregungen der Aufsichtsbehörde wurden kurzfristig im KBV-BDS-Entwurf umgesetzt, der dann in dieser Fassung dem KBR zur Beschlussfassung vorgelegt wurde.

Der jeweilige Stand der KBV-Verhandlungen wurde vom KBR regelmäßig ins Intranet gestellt und allen Betriebsräten per Mail zugesandt. Es ist vermutlich heute noch eine Herausforderung, interessierte Betriebsräte für die Arbeit zum Thema Datenschutz zu gewinnen, zumal sich durch die KBV BDS

viele neue Aufgaben für den KBR im Beschäftigtendatenschutz ergeben haben. Der KBR hofft, dem hohen Arbeitsaufkommen insgesamt durch intensive interne und externe Vernetzung begegnen zu können, vor allem durch die Zusammenarbeit mit externen Sachverständigen und Betriebsräten.

2.4 Ziele der KBV BDS

Bei den Verhandlungen mit dem Arbeitgeber zum Eckpunktepapier und zur KBV BDS mussten sich alle Beteiligten über die gemeinsamen Ziele verständigen, die sie mit der KBV BDS insgesamt erreichen wollten. Aus allen Interviews wird erkennbar: Die Betriebsparteien wollten aus der Erfahrung der Datenhavarie lernen und sahen den erzwungenen Neustart als Chance an. Die Weichen im Beschäftigtendatenschutz sollten so gestellt werden, dass sich zukünftig Ähnliches nicht mehr ereignen kann.

Die KBD BDS sollte dazu beitragen, möglichst weitgehend Transparenz zu schaffen hinsichtlich der Verwendung von personenbezogenen Daten der Beschäftigten und der automatisierten Datenverarbeitung im DB-Konzern, um seitens der Mitarbeiter und Interessenvertretungen verlorengegangenes Vertrauen wiederzugewinnen. Jede Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten bedarf nach der KBV BDS einer klaren Rechtsgrundlage. Sie verbietet in § 11 eine rechtsgrundlose Datenverwendung:

> „Die Verwendung personenbezogener Beschäftigtendaten darf nur erfolgen, wenn hierfür eine klare Rechtsgrundlage gegeben ist. Handelt es sich um besondere Arten personenbezogener Daten, muss die Rechtsgrundlage gesondert geprüft und dargelegt werden“ (KBV BDS Anlage 1 Nr. 2, siehe Anhang).

Diese Regelung spielt auf das Verbot mit Erlaubnisvorbehalt in § 4 Abs. 1 BDSG an:

> „§ 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung (1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.“

Die KBV BDS stellt aber auch fest, wann die Verarbeitung personenbezogener Daten der Beschäftigten erlaubt ist. Entweder gibt es bereits eine Rechtsgrundlage (z. B. durch eine gesetzliche Regelung, Betriebsvereinbarung oder eine Einwilligung). Fehlt sie, muss durch die Einbeziehung der zuständigen Interessenvertretung in Form einer Rechtsvorschrift eine Rechtsgrundlage geschaffen werden. Im Zweifelsfall muss der Arbeitgeber die Notwendigkeit oder Erforderlichkeit der Datenverwendung und deren Rechtsgrundlage nachweisen (§ 11 KBV BDS) und hat somit eine Nachweispflicht:

> „Verwendung ist jede Erhebung, Verarbeitung und Nutzung von Daten" (KBV BDS Anlage 1 Nr. 6).

Die Information der zuständigen Interessenvertretung, z. B. in § 27 Abs. 6 KBV BDS durch eine jährliche Übersicht über IT-Systeme und Verfahren, dient ebenfalls dem Ziel der Transparenz:

> „Dem zuständigen Betriebsrat wird einmal jährlich eine Übersicht der Systeme und Verfahren, in denen personenbezogene Daten seiner Beschäftigten verwendet werden, zur Verfügung gestellt."

Vorbildlich bei diesen Regelungen in der KBV BDS ist die strikte Ausrichtung auf einen ganz wesentlichen Datenschutzgrundsatz: auf die Transparenz durch Informationen und Benachrichtigung der betroffenen Beschäftigten und der Interessenvertretungen. Nur wenn Transparenz über die Datenverarbeitung im Betrieb als ein wichtiges Grundprinzip des Datenschutzes gewährleistet ist, können betroffene Beschäftigte, Datenschutzbeauftragte und Interessenvertretungen ihre gesetzlich zugewiesenen Kontrollaufgaben im Datenschutz wahrnehmen.

Der betriebliche Datenschutz sollte auf Nachhaltigkeit und kontinuierliche Verbesserung ausgerichtet werden. Hierzu sollte eine transparente und dem DB-Konzern mit ca. 120 eigenständigen Unternehmen (2012) angemessene Organisationsstruktur geschaffen werden, die als Ganzes zentral und dezentral ein funktionierendes System von Datenschutzstrukturen bildet. Für den geplanten Neustart des Datenschutzes sollte vor allem mehr Personal im Datenschutz eingestellt werden.

Aus Sicht der Konzernbetriebsräte, des Vorstands C und der Abteilung Arbeitsrecht, Mitbestimmung, Arbeitsvertragliche Grundsätze bei der Deut-

schen Bahn AG (im Folgenden Abteilung Arbeitsrecht) bestand ein zweites wichtiges Ziel: Rechtssicherheit herzustellen, um Führungskräften und den übrigen Beschäftigten im Konzern Sicherheit zu vermitteln bei der Erhebung, Verarbeitung und Nutzung von Beschäftigten- bzw. Kundendaten sowie um ihnen die Angst vor Datenschutz und möglichen Datenschutzverstößen zu nehmen. Von daher sind, so deutlich die Aussage der KBV BDS, klare Gebote und Verbote im Datenschutz erforderlich. Gebote sind handlungsanweisend, Verbote zielen auf das Unterlassen von Handlungen ab.

Die KBV BDS sollte weiterhin dazu beitragen, die mit dem neuen Vorstandsressort Compliance, Datenschutz, Recht und Konzernsicherheit geschaffene Struktur des gleichberechtigten kooperativen Verhältnisses der drei Bereiche deutlich zu unterstützen. Darüber hinaus sollte sie als verbindliche Richtschnur dazu dienen, bereits vorhandene Konzernvereinbarungen zu Informations- und Kommunikationstechnologien zu überarbeiten, anzupassen und entsprechende Vereinbarungen für neue IT-Systeme zu strukturieren. Die KBV BDS sollte sozusagen das „Arbeitnehmerdatenschutzgrundgesetz" für die Gewährleistung des Rechts auf informationelle Selbstbestimmung im DB-Konzern bilden (§ 32 Abs. 2 KBV BDS):

> „Die hier getroffenen Regelungen sind zugleich Richtschnur bei Interpretation und Auslegung des DB-internen Regelwerkes. Insbesondere bei Unklarheiten und Regelungslücken gelten sie als verbindlicher Maßstab. Das Regelwerk ist so auszulegen, dass es dieser KBV BDS entspricht."

3 DAS PRINZIP „VORBILDLICHER DATENSCHUTZ“ IN DER KBV BDS VOM 24.11.2010

Die KBV BDS wurde am 24.11.2010 unterzeichnet. Es wurden alle Regelungen des Eckpunktepapiers übernommen und vor allem etliche Regelungen noch präzisiert bzw. neue aufgenommen. Sie setzt konzernweite Standards für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten der Beschäftigten.

In fünf Abschnitten werden folgende Punkte geregelt: Grundsätzliches, der Umgang mit Beschäftigtendaten, technische, organisatorische und gesetzliche Aspekte des Datenschutzes, Rechte von betroffenen Beschäftigten und Interessenvertretungen sowie Schlussbestimmungen einschließlich der Anlagen. Der Abschnitt Grundsätzliches enthält Bestimmungen zu Ziel und Bedeutung der KBV, zum Geltungsbereich, zu den Begriffsbestimmungen, den Zwecken der Datenverarbeitung, zum Grundsatz der engen Auslegung der Zwecke, zur Zweckänderung, zum Trennungsgebot, zu Vorgaben für IT-Systeme und zur Nebendatenverarbeitung.

Die Regelungen der Konzernbetriebsvereinbarung Beschäftigtendatenschutz gehen allen anderen betrieblichen Regelungen vor, die Bezug zum Beschäftigtendatenschutz haben. An ihr haben sich somit alle anderen Regelungen mit Bezug zum Datenschutz im Konzern auszurichten. Die KBV BDS ist die verbindliche Basis aller Regelungen zum Beschäftigtendatenschutz im DB-Konzern (vgl. § 32 Abs. 1 und 2 KBV BDS):

> „Diese Vereinbarung ist die verbindliche Basis aller Regelungen zum Beschäftigtendatenschutz im DB-Konzern. Sie entfaltet ihre Wirkung ohne einen expliziten Verweis oder eine ausdrückliche Inbezugnahme auf sämtliche zukünftige Vereinbarungen zwischen den Parteien oder anderen Betriebspartnern, soweit diese eine Verwendung personenbezogener Beschäftigtendaten im DB-Konzern betreffen.“

Sie entfaltet ihre Wirkung ohne einen expliziten Verweis oder eine ausdrückliche Inbezugnahme auf sämtliche zukünftige Vereinbarungen, soweit diese eine Verwendung personenbezogener Beschäftigtendaten im DB-Konzern betreffen. Sollten sich Widersprüche mit vorhandenen Vereinbarungen und

konzerninternen Regelungen ergeben, gehen die Bestimmungen der Konzernbetriebsvereinbarung Beschäftigtendatenschutz vor (§ 32 Abs. 1, 3 KBV BDS).

3.1 Die KBV BDS und das novellierte Bundesdatenschutzgesetz 2009 (BDSG)

Aus Sicht des Konzernbetriebsrats soll die KBV BDS das BDSG konkretisierend umsetzen. Sie reflektiert das Gesetz, geht jedoch an wesentlichen Stellen über das gesetzliche Schutzniveau zugunsten der Beschäftigten hinaus, um den Beschäftigtendatenschutz nachhaltig und transparent im gesamten DB-Konzern zu verankern und passgenaue Lösungen für alle DB-Gesellschaften zu finden. Sie verwirklicht das Zweckbindungsgebot gemäß § 32 Abs. 1 Satz 1 BDSG:

> „§ 32 BDSG Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses
> „1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.“

Die KBV BDS bezieht sich des Weiteren auf die Regelung zu Straftaten im Beschäftigungsverhältnis (§ 32 Abs. 1 Satz 2 BDSG), die Bestimmungen zur Auftragsdatenverarbeitung in § 11 BDSG und die Pflicht zur Direkterhebung bei dem betroffenen Beschäftigten nach § 4 Abs. 2 Satz 1 BDSG.

3.2 Herausragende Regelungen in der KBV BDS

Betriebsräte, Mitarbeiter der Abteilung Arbeitsrecht, Datenschützer und Sachverständiger sehen die Stärken der KBV BDS ziemlich gleichlautend. Genannt werden die folgenden Regelungsfragen aus der KBV BDS:

– Sachverhaltsaufklärung (interne Ermittlungen) mit der doppelten Verhältnismäßigkeitsprüfung (§§ 18, 19)

- Verbot der Nebendatenverarbeitung (§ 9)
- Datenschutzaudits für die Nachhaltigkeit (§ 23)
- Bewerberdatenschutz: Gebot der Direkterhebung (§§ 15, 16)
- Einwilligung der Beschäftigten gekoppelt mit einem Zustimmungsvorbehalt der Betriebsräte (§ 25)
- Dezentrale Datenschutzorganisation (Anlage 3 B Datenschutzorganisation im DB-Konzern)
- Vertrauensperson beim Vorstand C (§ 28)
- Vorrang des Beschäftigtendatenschutzes vor Budgetzwängen (§ 1 Abs. 1 Satz 2)
- enge Auslegung der Zweckbindung (§ 5)
- Datenübersicht als Erleichterung des Rechts auf Auskunft (§ 24 Abs. 1)
- Jour fixe (Anlage 3, B 2.5)
- vorbildliches Datenschutzniveau auch im Ausland (§ 2 Abs. 4 Satz 3)
- Auftragsdatenverarbeitung/Funktionsübertragung (§ 17).

Sachverhaltsaufklärung

Die Sachverhaltsaufklärung (§§ 18, 19 KBV BDS) bezieht sich auf interne Ermittlungen einschließlich Prävention und Aufdeckung von Straftaten oder schwerwiegenden Gesetzesverstößen im Rahmen privatrechtlicher Befugnisse. Die Einschaltung von öffentlichen Stellen wie z. B. der Staatsanwaltschaft bleibt hiervon unberührt. Hier geht es grundsätzlich um die Fragestellungen, die auch in der Datenschutzkrise von 2009 eine Rolle gespielt haben. Die nach intensiver Diskussion im gemeinsamen Verhandlungsgremium gefundene Lösung zu einem transparenten Ablauf von zulässigen internen Ermittlungen ist eine Folge des unverhältnismäßigen und anlasslosen Mitarbeiter-Screenings.

Grundsätzlich sollen demnach präventive und repressive Maßnahmen zur Vorbeugung und zur Aufdeckung von Straftaten oder schwerwiegenden Gesetzesverstößen möglich sein, aber stets nur unter „genauer Beachtung der Datenschutzvorschriften“. Hierzu zählt inzwischen § 32 Abs. 1 Satz 2 BDSG (vgl. Wybitul 2009, S. 1583 f.), auf den in § 19 KBV BDS und im dazugehörigen Schaubild in Anlage 2 der KBV BDS ausdrücklich Bezug genommen wird:

> „§ 32 Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses
> (1) […] Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder ge-

> nutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind."

Gekoppelt ist die Sachverhaltsaufklärung mit einer doppelten Verhältnismäßigkeitsprüfung im Sinne eines abgestuften Verfahrens. In einer ersten Stufe wird geprüft, ob sich aus den vorliegenden und dokumentierten tatsächlichen Anhaltspunkten der Verdacht auf eine Straftat oder einen schwerwiegenden Gesetzesverstoß ergibt. Ist dies der Fall, so wird in einem ersten arbeitsrechtlichen Prüfschritt gemeinsam mit den zuständigen Interessenvertretungen bewertet, ob der angenommene Sachverhalt, seine Beweisbarkeit unterstellt, nur zu arbeitsrechtlichen Maßnahmen unterhalb einer Abmahnung führen würde. Diese erste arbeitsrechtliche Prüfung soll dazu beitragen, dass nicht jede kleine Verfehlung bzw. jeder Bagatellfall Gegenstand einer arbeitsrechtlichen Maßnahme wird und somit zusätzlich eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Beschäftigten erforderlich macht. Die Beteiligten in der Verhandlungskommission wollten nach ihren eigenen Worten nicht „mit Kanonen auf Spatzen schießen".

Das Ziel der 1. Prüfungsstufe ist demnach die Abgrenzung von Fällen, die nur zu arbeitsrechtlichen Maßnahmen unterhalb einer Abmahnung führen würden (Bagatellfälle), von Straftaten und schwerwiegenden Gesetzesverstößen (§ 19 Abs. 1 KBV BDS). Ist diese Schwelle nicht erreicht, bricht die Prüfung ab, es sei denn, der Betroffene fordert die Einleitung weiterer Schritte.

Ist das in Frage stehende Verhalten kein Bagatellfall, so entscheidet der Arbeitgeber gemeinsam mit der zuständigen Interessenvertretung, ob und welche weiteren Maßnahmen hinsichtlich der Datenverarbeitung zielführend bzw. erforderlich werden, unter Berücksichtigung der schutzwürdigen Interessen des Betroffenen. In diesem zweiten datenschutzrechtlichen Prüfschritt, der sich an § 32 Abs. 1 Satz 2 BDSG orientiert, wird überprüft, inwieweit eine weitere Datenerhebung erforderlich und damit datenschutzrechtlich verhältnismäßig ist. In Bagatellfällen ist eine zusätzliche Datenerhebung nicht erforderlich, so die ausdrückliche Regelung der Betriebsparteien in § 19 KBV BDS.

Die Betroffenen sind so bald wie möglich zu informieren, wenn der Erfolg der durchgeführten Maßnahmen nicht mehr gefährdet ist (§ 18 Abs. 1 KBV BDS). Die vorherige Information über die Ziel- und Zweckänderung der ursprünglich erhobenen Daten kann in den Fällen des § 18 KBV BDS ausnahmsweise unterbleiben, wenn hierdurch eine gesetzlich legitimierte Sachverhaltsaufklärung gefährdet wird (§ 6 KBV BDS). In diesen Fällen erfolgt die Information der Betroffenen gemäß § 18 Abs. 3 KBV BDS „so bald als möglich". Insofern kann dann von dem Grundsatz der Direkterhebung von Daten bei den betroffenen Beschäftigten in § 15 KBV BDS abgewichen werden.

Compliance lässt sich nach Aussagen der bahninternen Datenschützer, der Betriebsräte und der Abteilung Arbeitsrecht nur mit Datenschutz und Mitbestimmung verwirklichen. Die Betriebsräte müssen hinzugezogen werden. Beide Prüfungen müssen mit einem einvernehmlichen Ergebnis der Betriebsparteien enden, ansonsten wird eine Eskalationsinstanz eingeschaltet (§ 19 Abs. 2 KBV BDS). Die Regelung in § 18 KBV BDS zur Sachverhaltsaufklärung kann damit insgesamt als einzigartig und vorbildlich in der Privatwirtschaft und im öffentlichen Dienst bezeichnet werden.

Die Konzernbetriebsräte wollten ausdrücklich mit dieser Regelung keinen Täterschutz betreiben, sondern einer ungebremsten Verfolgung von Beschäftigten auch bei kleinsten Vergehen oder Vorkommnissen Einhalt bieten. Es sollte zudem berücksichtigt werden, dass der Arbeitgeber kein Staatsanwalt ist. Vor allem sollte ein geregeltes Verfahren zur internen Ermittlung installiert werden, das ausdrücklich der Mitbestimmung der Interessenvertretungen unterliegt (ablehnend Wybitul 2014, S. 230). Die Regelung stellt, so ausdrücklich die KBV BDS, keine Duldung der in Frage kommenden Sachverhalte durch den Arbeitgeber oder den Betriebsrat dar.

Die *doppelte Verhältnismäßigkeitsprüfung* wird in der Regel durch den jeweiligen Personalverantwortlichen angestoßen. Die zuständigen Interessenvertretungen werden ebenso wie Mitarbeiter des Datenschutzes und des Arbeitsrechts bei der Auswahl und Ausgestaltung der erforderlichen Prozesse, Instrumente und Methoden zur Sachverhaltsprüfung einbezogen (§ 18 Abs. 2 KBV BDS). Bei konzernrelevanten Sachverhalten wird die Konzernsicherheit eingeschaltet, die die Prüfung koordiniert. Kommt es nicht zu einem Einvernehmen bzw. zu einem Dissens bei beiden Schritten der Verhältnismäßigkeitsprüfung, so kann eine paritätisch besetzte Kommission als Eskalationsinstanz auf der jeweils zuständigen betrieblichen Ebene angerufen werden. Dies ist bislang noch nie vorgekommen.

Der Arbeitgeber im Verhandlungsgremium, hier der Vorstand C, hat diesen Ansatz gemeinsam mit dem KBR-Sachverständigen entwickelt und un-

terstützt. Vorher wurde allerdings seitens des Arbeitgebers die Befürchtung geäußert, dass aufgrund des Verfahrens z. B. die Ausschlussfristen gemäß § 626 Abs. 2 BGB von zwei Wochen (vgl. Müller-Glöge et al. 2012, § 626 BGB Rdnr. 200 ff.) nicht einzuhalten wären. In § 19 Abs. 2 KBV BDS werden die zuständigen Betriebsparteien verpflichtet, die gesetzlichen Fristen bei der Einleitung von arbeitsrechtlichen Maßnahmen einzuhalten. Die Abteilung Arbeitsrecht hat hervorgehoben, dass die paritätisch besetzte Kommission als Eskalationsinstanz bislang nicht einberufen wurde und erforderliche Verfahren schnell durchgeführt werden konnten (Fritz 2012, S. 207). Alle notwendigen Termine konnten innerhalb von 48 Stunden gefunden werden.

Nebendatenverarbeitung

Ein weitere herausragende Regelung aus Sicht der beteiligten Akteure ist die klare Begrenzung der Verarbeitung personenbezogener Daten der Beschäftigten auf zentrale bzw. kollektivrechtlich geregelte IT-Systeme (vgl. § 9 KBV BDS):

> „§ 9 Nebendatenverarbeitung
> Eine Verwendung personenbezogener Beschäftigtendaten außerhalb führender und kollektivrechtlich geregelter Systeme und Verfahren (z. B. wenn dies in oder aus Excel-Tabellen, Access-Datenbanken etc. erfolgen soll) ist verboten, es sei denn, sie ist ausdrücklich kollektivrechtlich vereinbart.“

Nebendatenverarbeitung wird als die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten außerhalb von führenden und kollektivrechtlich geregelten Systemen verstanden (KBV BDS Anlage 1 Nr. 13). Mit dem Verbot soll verhindert werden, dass Daten aus verschiedenen individuellen IT-Systemen zusammengeführt bzw. verknüpft und außerhalb der führenden IT-Systeme weiterverarbeitet werden. Das würde gegen das Gebot der Zweckbestimmung (§ 32 BDSG), gegen Transparenz (u. a. § 33 ff. BDSG), gegen Datenvermeidung und Datensparsamkeit (§ 3a BDSG) und nicht zuletzt gegen Datensicherheit (§ 9 und Anlage zu § 9 BDSG) verstoßen.

Diese klare Regelung ist insoweit vorbildlich, als der Transfer oder die Verarbeitung von personenbezogenen Daten in Bürokommunikationssoftware oder auf mobilen Geräten ansonsten nicht mehr zu unterbinden bzw. rechtsklar zu regeln wäre. Mit dem Verbot der Nebendatenverarbeitung ohne ausdrückliche vorherige Zustimmung der zuständigen Interessenver-

tretung wird die notwendige Transparenz geschaffen, damit einerseits Beschäftigte ihre Rechte (§ 33 ff. BDSG) überhaupt wahrnehmen können und andererseits die Mitbestimmung der Interessenvertretung nicht per se ins Leere läuft. Datenschutzrechtlich soll damit das Gebot der Zweckbindung eingehalten werden, damit es nicht zu einer ungeregelten Zweckänderung kommt. Hier zeigt sich, dass der Zweckbindungsgrundsatz die heilige Kuh des Datenschutzrechts ist (Wolff/Brink-Brink 2013, System A, Rn. 11 f).

Das *Verbot der Nebendatenverarbeitung* dient zudem dazu, die Gebote der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) und der Erforderlichkeit (§ 32 Abs. 1 Satz 1 BDSG) zu verwirklichen. Die Verwendung personenbezogener Beschäftigtendaten ist stets auf das für die konkrete Zweckbestimmung objektiv Erforderliche zu beschränken. Sie hat grundsätzlich nur unter Nutzung derjenigen Verarbeitungsprozesse zu geschehen, die eigens zu diesem Zweck unter Beachtung bestehender kollektivrechtlicher Regelungen aufgesetzt worden sind (§ 13 KBV BDS). Ausdrücklich wird verboten, dieselben personenbezogenen Beschäftigtendaten für denselben Zweck aus parallelen Dateien und anderen Formen der Nebendatenverarbeitung zu verarbeiten (ebd.).

Durch diese Regelung soll nach Aussagen der befragten Konzernbetriebsräte nicht die Arbeit der Beschäftigten erschwert werden, sondern rechtskonform die erforderliche Transparenz geschaffen werden, ob und wo es zur Verarbeitung und Nutzung von Beschäftigtendaten in dezentralen IT-Systemen kommt. Vor Ort wird dann überprüft und gegebenenfalls in einer Betriebsvereinbarung geregelt, inwieweit diese dezentralen Anwendungen in führende IT-Systeme überführt werden können bzw. noch erforderlich sind.

Audits für die Nachhaltigkeit von Datenschutz

Das Bundesdatenschutzgesetz sieht in § 9a die Möglichkeit von Datenschutzaudits vor. Zu einem endgültigen Ausführungsgesetz ist es jedoch in 2009 bei der Novellierung des BDSG nicht mehr gekommen. Es besteht also kein gesetzlicher Zwang zur Auditierung eines Datenschutzmanagementsystems, spezieller IT-Systeme oder IT-Produkte.

Bei der Deutschen Bahn gibt es zentral bei der Konzerndatenschutzbeauftragten eine eigene Organisationseinheit Konzerndatenschutz Audit (CDA), die in enger Zusammenarbeit mit der IT/TK-Revision Audits in den DB-Konzerngesellschaften und bei IT-Dienstleistern durchführt. Die Mitarbeiter von CDA verstehen sich als Berater und nicht als Kontrolleure. CDA ist unabhängig und weisungsfrei. Audits in anderen Handlungsfeldern wie z. B. im Qualitätsmanagement sind beim DB-Konzern üblich bzw. eingeführt. Jetzt kom-

men mit der KBV BDS Datenschutz-Audits hinzu, die aus Sicht der Konzern-Datenschützer besonders wichtig und nützlich sind. Dies sehen sowohl die Betriebsräte als auch die Mitarbeiter der Abteilung Arbeitsrecht.

Die Audits sorgten zuerst nicht unbedingt für einhellige Begeisterung, sondern anfänglich für Skepsis, da die Datenschutzaudits zusätzliche Arbeit bedeuten. Inzwischen wird jedoch das Audit als „Hilfe zur Selbsthilfe“ akzeptiert und Auditberichte als wichtiges Instrument zur kontinuierlichen Verbesserung (§ 23 Abs. 1 KBV BDS) bzw. zum „Selbstdatenschutz“ angenommen. Die Mitglieder der Auditabteilung bei der Konzerndatenschutzbeauftragten müssen die Qualifikation zum betrieblichen Datenschutzbeauftragten und/oder zertifizierten Fachauditor vorweisen.

Die Audits sind in § 23 KBV BDS geregelt. Um sie wurde lange in den Verhandlungen zur KBV BDS gerungen. Sie dienen zur Überprüfung der „relevanten Datenschutzprozesse“ in den Konzerngesellschaften und beziehen sich unter anderem auf die Kontrolle der Einhaltung von Rollen und Zugriffsberechtigung (§ 20 Abs. 4 KBV BDS). Ziele der Audits sind die nachhaltige kontinuierliche Verbesserung des Datenschutzes, die Herstellung von Rechtssicherheit und die Sicherung des erreichten Datenschutzniveaus. Die Ziele sollen aus Sicht des zentralen Datenschutzes partnerschaftlich mit den DB-Gesellschaften erreicht werden. Die Audits sollen zudem möglichst zu einem Kulturwandel im Datenschutz beitragen.

Es geht also nicht nur ausschließlich um Kontrolle; es geht insbesondere um Beratung und darum, für Datenschutzprobleme gemeinsam nachhaltige Lösungen zu finden, die Rechtssicherheit gewährleisten. Im Audit werden hohe Anforderungen an das Datenschutzniveau im Allgemeinen, die Datensparsamkeit und die Transparenz der IT-Systeme und Verfahren im Besonderen gestellt. Unterschieden werden die drei Formen Basis-Audits, Projekt-Audits und Ad-hoc-Audits, z. B. bei einer vermuteten Datenpanne im Sinne von § 42a BDSG „Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten.“

Besonders hervorzuheben ist die Teilnahme der dezentralen Datenschutzfachkräfte an den Audits. Die Fachkräfte für Datenschutz (FDS) und/oder die Vertrauenspersonen für den Datenschutz (VPDS) werden in die Audits einbezogen. Methodisch gehen die Datenschutz-Auditoren bei der Ist-Aufnahme des Datenschutzniveaus bzw. des Datenschutzmanagementsystems folgendermaßen vor: Die notwendigen Dokumente zum Datenschutz werden geprüft und strukturierte Checklisten, Fragebögen, Interviews, Ortsbegehungen und Tests als Instrumente eingesetzt (§ 23 Abs. 3 KBV BDS).

In § 23 Abs. 4 und 5 KBV BDS wird zudem festgelegt, dass zuständige In-

teressenvertretungen über Anlass, Inhalt und Termine der Audits rechtzeitig informiert werden, daran teilnehmen und jederzeit Auditvorschläge bei der Auditabteilung CDA einreichen können. Auch jeder Beschäftigte kann Vorschläge einreichen. Diese sollen möglichst zeitnah in der Auditplanung von CDA und Revision berücksichtigt werden. Aktuell ist ein Online-Tool-Datenschutz-Monitoring zur Selbsteinschätzung für die Geschäftsführung der Einzelgesellschaften fertiggestellt, damit die Konzerngesellschaften ihren erreichten Stand im Datenschutz und Verbesserungsmöglichkeiten selbst überprüfen können.

Zu jedem durchgeführten Audit ist ein umfangreicher Bericht von CDA gemäß §23 Abs. 7 KBV BDS zu fertigen, der den Ist-Zustand des Datenschutzniveaus, die Risikoeinschätzung, Lücken des Datenschutzes und Umsetzungsmaßnahmen mit Terminsetzung für Verfahrensverantwortliche beschreibt:

> „Verfahren ist eine Verarbeitung von Daten oder ein Bündel von Datenverarbeitungen, die über eine von der verantwortlichen Stelle definierte Zweckbestimmung verbunden sind“ (KBV BDS Anlage 1 Nr. 19). Verfahren, die Bezug zu Beschäftigtendaten aufweisen können, sind z. B. Personalverwaltungssystem, Zeiterfassungssystem, Lohn- und Gehaltsabrechnung, Bewerberdatenbank, Skilldatenbanken, Videoüberwachung, Zugriffskontrollsystem, E-Mail-System, Virenscanner, Spamfilter, Verarbeitung von Internet Log Files oder Verwaltung von Dienstreisen“ (Hallermann 2013, S. 175).

Der Audit-Bericht dient der Herstellung von Transparenz und Sicherung der Nachhaltigkeit des Datenschutzes. Auch die jeweils zuständige Interessenvertretung empfängt diesen elektronisch verschlüsselten und passwortgeschützten Bericht, ebenso wie die Konzerndatenschutzbeauftragte. Die im Bericht vorgeschlagenen Maßnahmen müssen durch die verantwortliche Stelle umgesetzt werden:

> „Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt“ (KBV BDS Anlage 1 Nr. 7).

Die CDA überprüft bzw. kontrolliert die termingerechte Umsetzung der vorgeschlagenen Maßnahmen und führt gegebenenfalls ein weiteres Audit durch, wenn die vorgeschlagenen Umsetzungsmaßnahmen größeren Umfangs sind:

> „Ein Audit ist endgültig abgeschlossen, wenn alle im Bericht festgelegten Maßnahmen umgesetzt sind“ (§ 23 Abs. 7 KBV BDS).

Bei den Audits werden den zuständigen Interessenvertretungen weitgehende Informations-, Beratungs- und Initiativrechte eingeräumt. Der Konzernbetriebsrat erhält alle Auditpläne. Betriebsräte können Audits anmelden. So sind dem zuständigen Betriebsrat alle Unterlagen über durchgeführte Auditverfahren und deren Ergebnisse auf Verlangen unverzüglich zur Verfügung zu stellen (§ 27 Abs. 2 KBV BDS). Wurden bislang für geplante Systeme oder Verfahren keine Audits durchgeführt, sind diese auf Verlangen des zuständigen Betriebsrates unverzüglich einzuleiten. Wird die Durchführung eines Audits verweigert, darf das IT-System oder Verfahren erst nach Zustimmung des Betriebsrates eingesetzt oder verändert werden (§ 27 Abs. 3 KBV BDS).

Bewerberdatenschutz: Bewerberdaten müssen direkt beim Bewerber erhoben werden

Neben aktiven Beschäftigten werden Bewerberinnen und Bewerber im personellen Geltungsbereich von der KBV BDS wie in § 3 Abs. 11 BDSG unter dem Begriff Beschäftigte nach § 2 Abs. 2 KBV BDS erfasst, ebenso wie ehemalige Beschäftigte.

> „(11) Beschäftigte sind: […] 7. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist […].“

Beschäftigtendaten müssen, auch bei Bewerbern, direkt beim Betroffenen erhoben werden. Für Bewerber bedeutet dies, dass der Arbeitgeber nur solche Bewerberdaten (auch solche von Azubis) verwenden darf, die unmittelbar und persönlich von ihm stammen. Dazu gehören auch Daten, die der Bewerber zwecks Abrufes seitens des Arbeitgebers in eine Jobbörse eingestellt hat oder aber eigens zur Weitergabe an den Arbeitgeber einem Personalvermittler übergeben hat. Unzulässig ist es jedoch, den Bewerber „zu googeln“, ins-

besondere in sozialen Netzwerken, die der privaten Kommunikation dienen (z. B. Facebook) oder diesbezüglich Daten von Auskunfteien anzufordern. Die Daten müssen unmittelbar und persönlich vom Bewerber stammen und dürfen nicht mit anderen Daten zu einem Profiling verarbeitet und genutzt werden (§ 15 KBV BDS). Zu diesem so aktuellen Thema gab es im Vorfeld der KBV BDS intensive Verhandlungen.

Der Beschäftigtendatenschutz wird nach § 16 Abs. 1 KBV BDS umfassend von der Anbahnung bis zur Beendigung des Beschäftigungsverhältnisses gewährleistet und umfasst somit die Phase der Bewerbung als Begründung des Beschäftigungsverhältnisses (analog § 32 Abs. 1 Satz 1 BDSG). Unter anderem wird für die Begründung des Beschäftigungsverhältnisses geregelt, dass bei Nichteinstellung die Unterlagen zurückzureichen und die Bewerberdaten *unverzüglich zu löschen sind:*

> „Löschen ist das Unkenntlichmachen gespeicherter personenbezogener Daten, um deren weitere Verwendung auszuschließen“ (KBV BDS Anlage 1 Nr. 16).

Abweichungen hiervon sind nur möglich, wenn die Betroffenen einer längerfristigen Speicherung für eine eventuelle spätere Einstellung zugestimmt haben (§ 16 Abs. 2 KBV BDS). Bei Initiativbewerbungen müssen die betroffenen Bewerber informiert werden und eine Widerspruchsfrist eingeräumt bekommen. Das indirekte Verbot des Googelns von Bewerbern und Bewerberinnen bzw. das Gebot der Direkterhebung beim Betroffenen (siehe § 4 Abs. 2 und 3 BDSG) lässt sich dem folgenden Gebot in § 16 Abs. 2 KBV BDS entnehmen:

> „Der Arbeitgeber verpflichtet sich, nur diejenigen Bewerberdaten (auch solche von Azubis) zu verwenden, die unmittelbar und persönlich vom jeweiligen Bewerber stammen.“

Das *Gebot der Direkterhebung* in diesem Zusammenhang bedeutet, dass Beschäftigtendaten direkt beim Betroffenen erhoben werden müssen (§ 15 KBV BDS):

> „Eine Erhebung von personenbezogenen Daten aus anderen Quellen (z. B. aus dem Internet oder von Auskunfteien) ist ohne zwingendes gesetzliches Erfordernis oder einschlägige kollektivrechtliche Vereinbarungen ebenso verboten wie die anschließende Verarbeitung und Nutzung im Rahmen von Profilings etc."

Diese Regelung geht über das gesetzliche Schutzniveau zugunsten der Beschäftigten hinaus. Sie soll wiederum dabei helfen, im DB-Konzern einen vorbildlichen Beschäftigtendatenschutz zu installieren. Sicherlich ist es in der Praxis schwierig, die Einhaltung des Verbots zu kontrollieren. Aber alle Führungskräfte im DB-Konzern wissen aufgrund der KBV BDS, dass es bei Bewerbern das Gebot der Direkterhebung gibt – und darauf kommt es nach Aussagen der Betriebsräte wesentlich an.

Begrenzung der Wirksamkeit der Einwilligung im Beschäftigungsverhältnis (§ 25 KBV BDS)

Die Aufsichtsbehörden für den Datenschutz und engagierte Datenexperten sehen seit langem die Einwilligung im Beschäftigungsverhältnis als kritisch an (Kiesche/Wilke 2012, S. 9; Däubler 2015, Rdnr. 152 ff.; Gola/Wronka 2013, Rdnr. 396). Denn sie ist nicht notwendigerweise als freiwillig zu qualifizieren. § 4 Abs. 1 BDSG nennt die Einwilligung als eine mögliche Erlaubnis für die Zulässigkeit der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten:

> „1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat."

Die umstrittene Einwilligung des Betroffenen kann nur dann eine Erlaubnisnorm nach § 4 Abs. 1 und § 4a Abs. 1 BDSG und wirksam sein, wenn sie frei und informiert erfolgt, der Betroffene keine Sanktionen oder ungerechtfertigte Nachteile zu befürchten hat, die Einwilligung auch versagen bzw. widerrufen kann und kein Zweifel an der freien Entscheidung des Betroffenen besteht. Zusätzliche Anforderungen an die Einwilligung werden in § 4a BDSG gestellt. Im Arbeitsverhältnis kann demnach die notwendige Freiwilligkeit nicht per se unterstellt werden (§ 25 Abs. 1 KBV BDS, Kock-Francke 2009, S. 647; Däubler 2013, Rdnr. 332a). In der Praxis von Unternehmen

spielt die Einwilligung eher eine geringe Rolle, da sie nur dann aus Konzern- bzw. Unternehmenssicht zum Ziel führt, wenn alle Beschäftigten wirklich mitmachen würden. Das ist aber unwahrscheinlich (Däubler 2013, Rdnr. 334).

Die Betriebsparteien im DB-Konzern finden für dieses Problem eine besondere Lösung. Die KBV BDS regelt die Einwilligung der Betroffenen im Arbeitsverhältnis und geht auch hierbei über das gesetzlich verlangte Schutzniveau hinaus, indem sie die Einwilligung als Ausnahmefall mit einer vorherigen Zustimmung des Betriebsrats koppelt. Zum Schutz der Beschäftigten muss der zuständige Betriebsrat jeweils bezogen auf einen konkreten Regelungstatbestand der Bitte um Einholung einer Einwilligung zu einer Erhebung, Verarbeitung oder Nutzung personenbezogener Daten der Beschäftigten zustimmen. Gleichzeitig sind noch zusätzlich festgelegte datenschutzrechtliche Bedingungen für eine rechtskonforme Einwilligung einzuhalten:

- Für den betroffenen Beschäftigten muss es tatsächlich möglich sein, seine Einwilligung zu verweigern bzw. diese später ohne Angabe von Gründen ohne für ihn negative Konsequenzen zu widerrufen.
- Der Beschäftigte muss vor Abgabe seiner Einwilligung auf die Freiwilligkeit seiner Erklärung sowie auf die Folgen der Verweigerung hingewiesen werden; dies muss protokolliert werden.
- Die Einwilligung muss schriftlich erfolgen (Schriftformerfordernis).

Dezentrale Datenschutzorganisation

Alle befragten Akteure des betrieblichen Datenschutzes bei der Deutschen Bahn AG betonen immer wieder die enorme Bedeutung der dezentralen Datenschutzorganisation, die aufgrund der Verhandlungsprozesse zur KBV BDS und eines Vorstandsbeschlusses eingeführt wurde. Zudem wurde die zentrale Datenschutzorganisation wesentlich ausgebaut. Die Konzerndatenschutzbeauftragte führt verschiedene Abteilungen zum zentralen Datenschutz: so den Kundendatenschutz, den Mitarbeiterdatenschutz, Globales Datenschutzmanagement (Konzernleitung, Ressorts Personal, Informationstechnik, Transport), Globales Datenschutzmanagement (Transport & Logistik) und Audit. Die Aufgaben der zentralen Datenschutzorganisation sind unter anderem die Strategie- und Konzeptentwicklung, die Bearbeitung übergeordneter Datenschutzthemen und die Vorhaltung von vertieftem Datenschutzfachwissen.

Zur dezentralen Datenschutzorganisation gehören die Beauftragten für Datenschutz in insgesamt sechs DB-Konzerngesellschaften, die Fachkräfte für Datenschutz und die Vertrauenspersonen für Datenschutz in den DB-Konzerngesellschaften vor Ort. Ihre Aufgabe ist es, die jeweilige datenverantwort-

liche Stelle zu unterstützen. Sie wirken auf die Einhaltung des Datenschutzes hin (siehe § 4g Abs. 1 Satz 1 BDSG).

Des Weiteren werden zusätzlich in der Regel auf Geschäftsfeldebene sogenannte *Fachkräfte für Datenschutz* (im Folgenden FDS) eingesetzt, die speziell für diese Aufgabe ausgebildet worden sind. In anderen Unternehmen der Privatwirtschaft werden sie oft, wenn sie berufen sind, Koordinatoren genannt. Die FDS werden ständig fortgebildet und erhalten, wie betriebliche Datenschutzbeauftragte seit 2009, einen erweiterten Kündigungsschutz. Das heißt, sie können nur aus wichtigem Grunde gemäß § 626 BGB gekündigt werden. Dieser Kündigungsschutz wirkt ein Jahr nach Beendigung der Tätigkeit als FDS nach. Die FDS erhalten eigene Kontrollrechte für ihren Verantwortungsbereich. Sie stehen im Rahmen ihrer Arbeitszeit dem Datenschutz voll zur Verfügung.

Zusätzlich sind *Vertrauenspersonen für den Datenschutz* (im Folgenden VPDS) bestellt und qualifiziert worden, die vor Ort für den Datenschutz verfügbar sind. Sie sollen beraten, qualifizieren, kontrollieren und mit Unterstützung des zentralen Datenschutzes Lösungen für Probleme vor Ort organisieren. Ähnlich wie im Arbeitsschutz bei den Sicherheitsbeauftragten dienen sie vor allem in den Arbeitsbereichen als Ansprechpartner für Betroffene bei Datenschutzvorfällen und -problemen.

Jährlich wird ein Treffen veranstaltet, an dem alle dezentralen und zentralen Datenschutzakteure (KDSB, DSB, FDS, VPDS) teilnehmen. FDS und VPDS sind umfassend qualifiziert worden. Sie nehmen zudem an den Datenschutzaudits teil. Ihre Aufgaben sind in der KBV BDS in B. 2.2 detailliert normiert. Sie sind insbesondere Ansprechpartner für Beratung, Schulung und Information im jeweils zugeordneten Geschäftsbereich und für die Sensibilisierung für den Datenschutz vor Ort. Sie stellen weiterhin die Erarbeitung und Pflege bzw. Aktualisierung von dezentralen Verfahrensverzeichnissen bei den verantwortlichen Stellen sicher (zum Verfahrensverzeichnis Kiesche/Wilke 2011). Auswahl und Bestellung der FDS und VPDS erfolgt maßgeblich unter fachlichen Gesichtspunkten durch die betreffenden Konzernunternehmen in Abstimmung mit den fachlich Verantwortlichen sowie unter Beteiligung der zuständigen Arbeitnehmervertreter. Dies gilt inhaltsgleich für eine Abberufung einer FDS oder einer VPDS (B 2.4.5 KBV BDS).

Die Beteiligung der Betriebsräte bei der dezentralen Datenschutzorganisation ist weitgehender als das Betriebsverfassungsgesetz, in dem Datenschutz und Datenschutzbeauftragte nicht erwähnt werden. Ein Mitentscheidungsrecht der Betriebsräte über § 99 BetrVG entsteht im Fall der Bestellung eines nicht leitenden Angestellten als internen Datenschutzbeauftragten

dann, wenn die Bestellung mit der Einstellung oder einer Versetzung verknüpft wird (ausführlich Gola 2013, S. 368 f.; Gola/Jaspers 2011, S. 67).

Die Vertrauensperson Datenschutz beim Vorstand C (VbV)

In § 28 KBV BDS wird die Position einer Vertrauensperson Datenschutz beim Vorstand C (im Folgenden VbV) geregelt, die vor allem eine Unterstützungsfunktion für den Datenschutz hat. Diese Stelle war vom KBR bereits bei den Verhandlungen zum Eckpunktepapier angeregt worden und konnte bei den KBV-Verhandlungen durchgesetzt werden.

Die VbV ist in Ergänzung zur zentralen und dezentralen Datenschutzorganisation eine unabhängige Vertrauensinstanz und Ansprechpartner für die Beschäftigten und Interessenvertretungen in Datenschutzangelegenheiten. Sie ist außerhalb der Datenschutzorganisation (Linie) angesiedelt, weisungsunabhängig und zur Verschwiegenheit verpflichtet. Die Rechte der betrieblichen Datenschutzbeauftragten nach §§ 4f und 4g BDSG bleiben durch ihre Tätigkeit unberührt.

Eine derartige Position im Sinne eines Datenschutznetzwerksknoten ist in der Wirtschaft bislang unbekannt, aber unbedingt für größere Unternehmen zur Nachahmung zu empfehlen. Die Vertrauensperson nimmt an Treffen der Datenschutzbeauftragten teil, berät und schult Beschäftigte und Interessenvertretungen und setzt wichtige Impulse bei Vorhaben mit Datenschutzrelevanz. Sie hat ein Initiativrecht in allgemeinen Datenschutzbelangen (z. B. Vorschläge zur Verbesserung prozessualer und organisatorischer Strukturen und Abläufe) und erstattet dem Vorstand C und dem KBR einen jährlichen Tätigkeitsbericht.

Vorrang des Beschäftigtendatenschutzes vor wirtschaftlichen Interessen und Budgetzwängen

Die Betriebsräte sind optimistisch, dass das hohe Niveau des Beschäftigtendatenschutzes jetzt und in naher Zukunft gehalten werden kann. Sollte im Zuge von Einsparungen im DB-Konzern der Datenschutz davon betroffen sein, so erlangt die folgende zentrale Regelung große Bedeutung:

> „Diese Vereinbarung ist die verbindliche Basis aller Regelungen zum Beschäftigtendatenschutz im DB-Konzern. Ihr Ziel ist es, einen rechtskonformen, sicheren und nachhaltigen Beschäftigtendatenschutz im gesamten DB-Konzern zu gewährleisten. Diesem Ziel dürfen Budgetzwänge oder wirtschaftliche Interessen nicht entgegengestellt werden“ (§ 1 Abs. 1 KBV BDS).

Der vorbildliche Datenschutz kann somit, so die KBV BDS, heute und zukünftig nicht an Budgetzwängen oder übermächtigen wirtschaftlichen Interessen scheitern.

Enge Auslegung der Zweckbindung

Als besonders wichtige Säule des Datenschutzrechts ist die Zweckbestimmung bzw. -bindung hervorzuheben, die detailliert in § 5 KBV BDS geregelt ist:

> „§ 5 Grundsatz enger Auslegung der Zweckbestimmung
> (1) Die Zweckbestimmung ist eng auszulegen.
> (2) Jede konkrete Verwendung personenbezogener Beschäftigtendaten muss sich einer dokumentierten Zweckbestimmung zweifelsfrei zuweisen lassen können. Ist dies nicht mit hinreichender Sicherheit möglich, so ist davon auszugehen, dass die Zweckbestimmung diese Verwendung nicht erfasst und damit das Gebot der Zweckbindung verletzt wird.“

Die *Zweckbindung in Verbindung mit einer eindeutigen Zweckbestimmung* (§ 4 KBV BDS) und dem Gebot der Datensparsamkeit und Datenvermeidung ist eines der wichtigsten Datenschutzprinzipien zur Gewährleistung der informationellen Selbstbestimmung der Betroffenen. Zwecke und Ziele der Datenverarbeitung *müssen vor der Erhebung von Daten* abschließend und verbindlich festgelegt und dokumentiert sein (§ 4 Abs. 1 KBV BDS, § 3a und § 28 Abs. 1 Satz 2 BDSG).

In der Praxis der Privatwirtschaft sind die Zwecke der Datenverarbeitung längst nicht immer eindeutig und abschließend bestimmt und damit für Beschäftigte und Betriebsräte in aller Regel nicht transparent. Deshalb müssen nach der KBV BDS Zwecke und Ziele der Datenverarbeitung allen Beschäftigten und deren zuständigen Interessenvertretungen verdeutlicht werden.

An Zwecke und Ziele der Datenverarbeitung werden konkrete Anforderungen gestellt. Das heißt, sie dürfen gesetzlichen Bestimmungen nicht widersprechen und müssen die Persönlichkeitsrechte der Beschäftigten maximal wahren (§ 4 Abs. 3 KBV BDS und § 75 Abs. 2 BetrVG):

> „§ 75 Abs. 2 BetrVG Grundsätze für die Behandlung der Betriebsangehörigen

> […] (2) Arbeitgeber und Betriebsrat haben die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Sie haben die Selbständigkeit und Eigeninitiative der Arbeitnehmer und Arbeitsgruppen zu fördern."

Die Verwendung von Daten auf *Vorrat, das heißt ohne konkrete Zweckbindung,* ist – wie im Volkszählungsurteil von 1983 bereits als wichtiges Datenschutzprinzip in Zusammenhang mit Zweckbindung und Datenvermeidung ausgeführt – ausdrücklich verboten (§ 4 Abs. 5 KBV BDS). *Vorratsdatenverarbeitung* wird wie folgt definiert:

> „Vorratsdatenverarbeitung im Sinne dieser Vereinbarung liegt vor, wenn personenbezogene Daten ohne abschließende Festlegung von Ziel und Zweck erhoben, verarbeitet oder genutzt werden" (KBV BDS Anlage 1 Nr. 12).

In § 5 der KBV BDS wird an dem wichtigen Grundsatz der engen Auslegung der Zweckbestimmung festgehalten. Jede konkrete Verwendung personenbezogener Beschäftigtendaten muss sich einer dokumentierten Zweckbestimmung zweifelsfrei zuweisen lassen können. Ansonsten wird als klare Rechtsfolge festgehalten:

> „Ist dies nicht mit hinreichender Sicherheit möglich, so ist davon auszugehen, dass die Zweckbestimmung diese Verwendung nicht erfasst und damit das Gebot der Zweckbindung verletzt wird."

Will der Arbeitgeber die Zweckbestimmung für die erhobenen Beschäftigtendaten ändern, muss er gemäß § 6 KBV BDS bei einer Zweckänderung zuvor die Betriebsräte kollektivrechtlich beteiligen und die Beschäftigten informieren. Die Zweckänderung muss zudem unstreitig datenschutzrechtlich im Sinne des § 32 Abs. 1 Satz 1 BDSG „erforderlich" sein. Streitig wäre die *Erforderlichkeit*, wenn z. B. der Betriebsrat widerspricht. Die vorherige schriftliche Information der betroffenen Beschäftigten über die Zweckänderung, z. B. auch per E-Mail, kann im Fall der gesetzlich legitimierten Sachverhaltsaufklärung gemäß § 18 Abs. 3 KBV BDS ausnahmsweise unterbleiben, wenn der Zweck der Ermittlung dadurch gefährdet wird.

Datenübersicht zur Erleichterung eines Auskunftsersuchens der Beschäftigten

Die Akteure bei der Deutschen Bahn AG heben die Datenübersicht als Bestandteil eines vorbildlichen Datenschutzes hervor. Sie ist im DB-Intranet im „C-Portal“ unter „Beschäftigtendatenschutz“ eingestellt und dokumentiert bezogen auf die Konzerngesellschaften, in welchen IT-Systemen und Papierdatenverarbeitungen wie z. B. Personalakten personenbezogene Daten der Beschäftigten verarbeitet und genutzt werden.

Im Fall des DB-Konzerns ist festzuhalten: Nur 70.000 Beschäftigte haben einen Zugang zum Intranet und damit zum Portal Beschäftigtendatenschutz. Insofern ergab sich die Notwendigkeit einer *Datenschutzbroschüre*, die umfassend über den Datenschutz informiert. Sie wurde inzwischen erstellt, gedruckt und verteilt.

Um den Beschäftigten die Wahrnehmung der Auskunftsrechte zu erleichtern und um Transparenz herzustellen, wird der Arbeitgeber in § 24 Abs. 2 der KBV BDS dazu verpflichtet, für die Beschäftigten eine *jährliche Datenübersicht* online zu veröffentlichen. Darin werden die über sie als Mitarbeiter gespeicherten Daten in den zentralen und dezentralen Systemen und Verfahren in elektronischer Form oder in Papierform aufgeführt. Die Datenübersicht listet differenziert nach Funktionsgruppen (Jobcodes) die zentralen IT-Systeme und Verfahren vollständig auf, in denen personenbezogene Daten verarbeitet werden. Ein Muster der Datenübersicht mit Mindestangaben ist der KBV BDS als Anlage 4 beigefügt. Die Online-Datenübersicht wird zurzeit benutzerfreundlicher gestaltet. Eine solche Übersicht ist ansonsten in der Privatwirtschaft unüblich. Aus Sicht der Herstellung von Transparenz eignet sie sich dazu, die Beschäftigten über die Art der Daten und den Umfang der Datenverarbeitung zunächst grob zu informieren und ggf. ihr Verlangen nach detaillierteren Auskünften im Sinne von Bestimmtheit vorzustrukturieren.

In § 24 Abs. 3 KBV BDS verpflichtet sich der Arbeitgeber zusätzlich, innerhalb von maximal 4 Wochen auf Anfrage eine *detaillierte Datenauskunft nach § 34 BDSG* zu erteilen, die in Anlage 5 der KBV BDS näher spezifiziert ist. Aus aktuellem Anlass müssen die Beschäftigten über datenschutzrelevante Änderungen im Umgang mit ihren personenbezogenen Daten informiert werden (§ 24 Abs. 2 KBV BDS).

In der betrieblichen Datenschutzpraxis sind konkrete Wünsche nach Auskunft gemäß § 34 BDSG eher selten. Daher sollte noch stärker intern in Betrieben und Dienststellen sensibilisiert und dafür geworben werden, dass betroffene Beschäftigte ihre wichtigen Rechte auch wirklich nutzen. Ansonsten können sie ihre wichtige Rolle als interne datenschutzrechtliche Kontrol-

linstanz und ihre Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung, Löschung und Widerspruch nicht effektiv wahrnehmen.

Jour Fixe Datenschutz als Mittel der Prozessgestaltung

Die KBV BDS legt nicht nur eine wirksame Struktur der Datenschutzorganisation fest, sondern ermöglicht auch wichtige Prozesse der Kommunikation und Interaktion zum betrieblichen Datenschutz. In den Interviews werden diesbezüglich insbesondere der Jour Fixe Datenschutz (im Folgenden JFD) und Telefonkonferenzen bei Bedarf genannt.

Am Jour Fixe Datenschutz (vgl. KBV BDS, Anlage 3, Datenschutzorganisation im DB-Konzern, B. Dezentrale Datenschutzorganisation und ihr Zusammenwirken mit der zentralen Datenschutzorganisation, 2.5) wirken der Konzerndatenschutz, die Leitungen der Organisationseinheiten und die Fachkräfte für den Datenschutz mit. Als ständiger Gast nimmt die Vertrauensperson Datenschutz beim Vorstand C teil. Weitere Gäste können einstimmig hinzugezogen werden. Beschlüsse bzw. Ergebnisse werden einstimmig gefasst (2.5.3). Aufgabe des Jour Fixe Datenschutz (2.5.1) ist es, ein einheitliches, angemessenes Datenschutzniveau im Gesamtkonzern sicherzustellen. Hierzu ist ein regelmäßiger und systematischer Informationsfluss zwischen der Konzerndatenschutzbeauftragten (entspricht Leitung „Konzerndatenschutz CD“), den Beauftragten für den Datenschutz gemäß § 4f BDSG in einzelnen Konzernunternehmen sowie den Fachkräften für Datenschutz des DB-Konzerns erforderlich.

Alle Mitwirkenden sind gleichberechtigt und inhaltlich weisungsfrei, so wie in § 4f Abs. 3 Satz 2 BDSG für den betrieblichen Datenschutzbeauftragten geregelt. Die Sitzungen des Jour fixe Datenschutz dienen dazu, ein abgestimmtes und transparentes Vorgehen des Konzerndatenschutzes mit den Beauftragten für den Datenschutz gemäß § 4f Abs. 1 BDSG in den Konzerngesellschaften sowie Fachkräften für Datenschutz des DB-Konzerns zu beraten und zu erzielen. Die detaillierten Aufgaben des Jour Fixe Datenschutz, eines Treffens der zentralen und dezentralen Datenschützer alle zwei Monate, lassen sich wie folgt beschreiben:

- Abstimmung über aktuelle Themen des Datenschutzes aufgrund der Einführung neuer gesetzlicher und betrieblicher Regelungen und Normen
- strukturierter Informations- und Erfahrungsaustausch zu Geschäftsmodellen, Prozessen und Umgang mit Kunden-/Mitarbeiterdaten, Ergebnissen der Datenschutzaudits und Datensicherheit.

Vorbildliches Datenschutzniveau auch im Ausland

Eine Konzernbetriebsvereinbarung kann Regelungen nur für inländische Betriebe eines Unternehmens treffen. Im DB-Konzern arbeiten weltweit 300.000 Beschäftigte, 107.000 davon im Ausland. Damit auch dort ein vorbildlicher Datenschutz erreicht wird, hat die Deutsche Bahn AG sich verpflichtet, für die jeweilige Landesgesetzgebung den bestmöglichen Beschäftigtendatenschutz im Ausland zu gewährleisten (vgl. § 2 KBV BDS):

> „Es wird sichergestellt, dass individuelle Rechte der Beschäftigten ebenso wie die Einhaltung der Regelungen aus kollektivrechtlichen Vereinbarungen uneingeschränkt gewährleistet sind.“

Personenbezogene Daten aus Deutschland nehmen bei der Verarbeitung im Ausland den in Deutschland bestehenden bzw. vereinbarten Schutzstandard mit, so das Ziel der KBV BDS. Vorzugsweise soll die Datenverarbeitung im Inland erfolgen (ebd.):

> „Hierbei wird nicht allgemein der deutsche Datenschutz in das Ausland exportiert, personenbezogene Daten aus Deutschland nehmen aber bei der Verarbeitung im Ausland den in Deutschland bestehenden bzw. vereinbarten Schutzstandard mit. Der DB-Konzern wird zur Vermeidung von Beeinträchtigung oder Umgehung des datenschutzrechtlichen Standards geeignete Maßnahmen ergreifen. Vorzugsweise sind die Daten der in der Bundesrepublik Deutschland Beschäftigten im Inland zu verarbeiten.“

In Zweifelsfällen wird eine problematische Datenverwendung unterlassen, wenn keine Rechtssicherheit erreicht werden kann. Beim Datentransfer in Drittstaaten außerhalb der EU wird in § 17 Abs. 5 KBV BDS festgelegt:

- Eine Datenverwendung im Ausland darf nur durchgeführt werden, wenn sie datenschutzrechtlich zulässig ist und wenn hierbei die Rechte der Betroffenen (Information, Berichtigungsansprüche etc.) und der zuständigen Betriebsräte umfassend garantiert werden.
- Insbesondere muss hierfür ein Vertrag entsprechend der Vorgaben in § 11 BDSG abgeschlossen werden.
- Eine Datenverwendung außerhalb der EU ist nur zulässig, wenn die hierfür einschlägigen datenschutzrechtlichen Vorgaben gemäß § 4 und §§ 4b,

4c BDSG eingehalten werden. Bei derartigen Verwendungen werden zusätzlich zu einem Vertrag entsprechend § 11 BDSG EU-Standardvertragsklauseln zu Grunde gelegt.

Zur Abgrenzung der Auftragsdatenverarbeitung von Funktionsübertragung

Ein wichtiger Punkt der KBV BDS aus Sicht der Abteilung Arbeitsrecht und der Betriebsräte ist die *Regelung zur Auftragsdatenverarbeitung einschließlich Funktionsübertragung* in § 17 KBV BDS. Damit wurde eine erste Grundlage für die rechtskonforme Gestaltung von konzerninternen Datenflüssen geschaffen, die 2013 durch die KBV Konzerninterne Datenflüsse (KBV KID; dazu Bussche/Voigt 2014, S. 199) ergänzt wurde.

In den Begriffsbestimmungen in Anlage 1 der KBV BDS (siehe Anhang) werden Auftragsdatenverarbeitung und Funktionsübertragung nach dem aktuellen Stand der datenschutzrechtlichen Diskussion mit exakten Erkennungsmerkmalen unterschieden. Eine Übermittlung von Beschäftigtendaten an andere Stellen kann auf Grundlage einer Auftragsdatenverarbeitung nach § 11 BDSG erfolgen. Die anschließende Verarbeitung durch den Auftragnehmer, der nicht Dritter ist, muss sich auf Hilfsfunktionen beschränken. Er unterliegt dem Weisungsrecht des Auftraggebers. Für die Regelung von Auftragsdatenverarbeitung im DB-Konzern wird in § 17 Abs. 5 KBV BDS ausdrücklich auf § 11 BDSG Bezug genommen.

Außerhalb der Auftragsdatenverarbeitung nach § 11 BDSG ist eine eigenständige Verarbeitung von Beschäftigtendaten durch andere Konzernunternehmen auch durch eine „Funktionsübertragung" möglich. Dabei erhalten die beauftragten Stellen eine eigenständige Kompetenz zur Datenverarbeitung (KBV BDS Anlage 1 Nr. 9 und 10, mit Erkennungsmerkmalen zur Unterscheidung, siehe Anhang). Funktionsübertragung wird in § 17 Abs. 6 KBV BDS analog zur Auftragsdatenverarbeitung geregelt:

> „Funktionsübertragungen dürfen nur erfolgen, wenn hierbei die Rechte der Betroffenen und der Betriebsräte uneingeschränkt gewahrt werden."

Die Regelung ist insoweit Vorbild, weil sie Interessenvertretungen umfassend und rechtzeitig bei Funktionsübertragungen in Form von Beratungen beteiligt. Mit den Arbeitnehmervertretungen findet also eine umfassende Beratung vor jeder Vergabe von Auftragsdatenverarbeitung und Funktionsüber-

tragung statt. Insbesondere werden die Interessenvertretungen bei dem Vertrag zur Auftragsdatenverarbeitung hinzugezogen. Diese Regelung hatte anschließend Auswirkungen auf die abzuschließende KBV KID, da es sich um beauftragte Stellen innerhalb des Konzerns handeln kann.

In § 11 BDSG wird für jede Auftragsdatenverarbeitung *ein schriftlicher Vertrag* verlangt, dessen Bestandteile in § 11 Abs. 2 Satz 2 BDSG festgelegt sind. In der Novellierung von 2009 wurden diese Bestimmungen noch ergänzt und vor allem eine sorgfältige Auswahl und eine fortlaufende Kontrolle des Auftragnehmers durch den jeweiligen Auftraggeber verlangt. Den Auftraggeber trifft eine Kontrollpflicht, die in 2009 vom Gesetzgeber noch verschärft wurde.

Der Vertrag, der im DB-Konzern bei der Auftragsdatenverarbeitung zu schließen ist, muss sowohl die kollektiven Mitbestimmungstatbestände als auch die Rechte der Beschäftigten wahren (§ 17 Abs. 1 KBV BDS). Ohne Beratung mit Interessenvertretungen darf ein Vertrag zur Auftragsdatenverarbeitung nicht abgeschlossen werden:

> „Besteht keine Einbeziehung der Interessenvertretung, darf eine Datenverarbeitung im Auftrag nicht stattfinden.“

Die Regelung, dass Funktionsübertragungen nur erfolgen dürfen, wenn hierbei die Rechte der Betroffenen und der Betriebsräte uneingeschränkt gewahrt werden, ist von besonderer Bedeutung (§ 17 Abs. 6 KBV BDS).

Den Betriebsräten wird „unabhängig von ihren Beteiligungsrechten nach dem BetrVG“ zugestanden, die Vorlage des Vertrags nach § 11 BDSG zu verlangen (§ 17 Abs. 3 KBV BDS). In der Datenschutzpraxis in Unternehmen wird dies eher selten praktiziert. Schon gar nicht werden Rechte der Interessenvertretungen im jeweiligen Vertrag zur Auftragsdatenverarbeitung eingearbeitet und während seiner Laufzeit eine Kontrolle des Datenschutzes unter Einbeziehung des Datenschutzbeauftragten und des Betriebsrats vereinbart.

Hingegen formuliert die KBV BDS in § 17 Abs. 2 KBV BDS als explizite Anforderung an den Vertrag zur Auftragsdatenverarbeitung: Sowohl die Ausübung des Kontrollrechtes durch die verantwortliche Stelle sowie durch die dortigen Datenschutzbeauftragten als auch die Umsetzung der bestehenden Rechte der zuständigen Interessenvertretungen sind im Vertrag sicherzustellen.

Werden Auftragnehmer außerhalb des Konzerns ausgewählt, so sind bei der Auswahl der Auftragnehmer Anforderungen gestellt, die vor allem auf

die Zuverlässigkeit der Auftragnehmer abzielen. Zudem wird in § 17 Abs. 4 KBV BDS verlangt, dass die *sorgfältige Auswahl des Auftragnehmers* zu dokumentieren ist. Die folgenden Anforderungen an die Auswahl von Auftragnehmern sind als Checkliste für andere Unternehmen zu empfehlen:

- fachliche Eignung des Auftragnehmers für die konkret zu beauftragende Datenverwendung
- technische und organisatorische Maßnahmen zur Datensicherheit
- Erfahrung und Stellung des Auftragnehmers
- Seriosität des Auftragnehmers (ggf. unter Prüfung zur Verfügung gestellter Referenzen)
- Professionalität des Auftragnehmers (ggf. unter Befragung des Datenschutzbeauftragten des Auftragnehmers und Prüfung zur Verfügung gestellter Datensicherheitskonzepte, Notfallpläne und anderer relevanter Dokumentationen sowie von bestehenden Zertifizierungen).

3.3 Sichtweisen der betrieblichen Akteure bezüglich der KBV BDS

Einhellig wird die KBV BDS von den Beschäftigten der Abteilung Arbeitsrecht, den Konzernbetriebsräten und den Bahn-Datenschützern als Grundlage für einen rechtskonformen und nachhaltigen Datenschutz geschätzt.

Die Mitarbeiter der Abteilung Arbeitsrecht gewichten vor allem den Aspekt hoch, dass die KBV BDS Verfahren zur Mitbestimmung und Mitbestimmungstatbestände transparent und vertrauensvoll regelt. Sie hat offensichtlich ein Grundvertrauen zwischen Arbeitgeber, Interessenvertretungen und Belegschaft wiederhergestellt, das die Basis für weitere KBV-Verhandlungen und die vertrauensvolle Zusammenarbeit nach § 2 Abs. 1 BetrVG bildet. Des Weiteren sehen sie die Transparenz der Prozesse und Strukturen im Datenschutz als besonders wichtiges Element eines nachhaltigen Beschäftigtendatenschutzes an.

Sie schätzen zudem die gegenseitige Information, Beratung und Vernetzung von Arbeitsrecht, Datenschutz und Mitbestimmung (KBR), weil im Datenschutzrecht als Querschnittsmaterie oftmals Datenschutzfragen nicht eindeutig mit dem Gesetz (insbesondere mit dem BDSG) zu entscheiden sind. In vielen Fällen müssen Interessenabwägungsprozesse im Sinne von Verhältnismäßigkeitsprüfungen vorgenommen werden, die nur gemeinsam mit den internen Beteiligten und manchmal noch zusätzlich mit der zuständigen Aufsichtsbehörde durchzuführen sind.

Die Datenschützer, hier mit Schwerpunkt auf den Beschäftigtendatenschutz, sehen die KBV BDS als besonders hilfreich an und verstehen sich in dem Netzwerk der beteiligten Führungskräfte, Abteilungen und Betriebsräte in erster Linie als Berater. Sie nehmen eine neutrale Position ein, praktizieren Offenheit und stehen für Beratung, Schulung, Information, Vernetzung und in schwierigen Abwägungsprozessen zur Verfügung. Das erscheint als wesentliche Voraussetzung für eine kooperative und vertrauensvolle Zusammenarbeit aller Beteiligten im DB-Konzern, die festzustellen ist und von den Befragten auch so gesehen wird.

Die Konzernbetriebsräte und andere Betriebs- bzw. Gesamtbetriebsräte sind in etlichen Fragen des Datenschutzes und der Einführung von IT-Systemen auch über das gesetzlich Notwendige hinaus einbezogen. Sie erhalten vor allem aufgrund der KBV BDS vollständige Transparenz über eingeführte oder geänderte IT-Systeme, Datenverarbeitungsprozesse, IT-gestützte Personalprozesse und sonstige Prozesse der Erhebung, Verarbeitung und Nutzung der Beschäftigtendaten.

Auch wenn die Anpassung bestehender KBVs an die KBV BDS mühselig ist und neue KBVs zu weiteren Themen wie z. B. Social Media, Telefonie und Smartphones zu entwickeln sind, nutzen die Konzernbetriebsräte die KBV BDS als betriebliches Grundgesetz des Datenschutzes. Sie können weiterhin auf die in der KBV BDS beschriebenen kontrollierbaren und nachvollziehbaren Prozesse und Strukturen eines nachhaltigen Beschäftigtendatenschutzes bauen. Sie betonen, dass zu den Datenschutzfunktionsträgern ein Vertrauensverhältnis besteht und ihre Beratung für die Betriebsräte Gewicht hat.

In der Einschätzung der Stärken der KBV BDS und der nachfolgenden Regelungen wie z. B. der KBV KID (Konzerninterne Datenflüsse) manifestiert sich bei allen Akteuren offenkundig ein *gemeinsames Datenschutzgrundverständnis.* Denn unter anderem werden die Stärken der KBV BDS von den Interviewpartnern weitgehend identisch benannt. Alle Akteure sind zudem zuversichtlich, dass die KBV BDS, die erreichte Stärkung des konzerninternen Datenschutzes und der deutlich feststellbare Kulturwandel hinsichtlich der Bedeutung des Rechts auf informationelle Selbstbestimmung langfristig helfen, das vorbildliche Datenschutzniveau im DB-Konzern zu halten. Insbesondere die Konzernbetriebsräte sehen hierfür jedoch Schwierigkeiten, wenn Einsparungen für die Bahn notwendig werden und Budgetzwänge eventuell auf die zentrale und dezentrale Datenschutzorganisation zukommen könnten.

3.4 Das Prinzip „Vorbildlicher Datenschutz" umsetzen, leben und weiterentwickeln

Datenschutz ist nie abgeschlossen, sondern muss beständig gelebt werden. Betrieblicher Datenschutz funktioniert dann gut, wenn er nicht mehr sichtbar ist. So kann die Bedeutung des Datenschutzes im Bewusstsein der Akteure eines Unternehmens oder Konzerns jedoch schnell abnehmen. Datenschutz als gelebte informationelle Selbstbestimmung muss in die alltägliche Praxis der Beschäftigten Eingang finden und immer wieder neu aktualisiert werden, wenn sich neue Fragen ergeben. Hierfür ist insbesondere eine entsprechende Schulung für Datenschutz-Multiplikatoren wichtig, ebenso wie eine stets offene Kommunikation zwischen allen beteiligten Stellen, Akteuren und Betriebsparteien. Vor allem Datenpannen oder Beinahe-Datenpannen sollten bzw. können dazu genutzt werden, das Bewusstsein für das Grundrecht auf informationelle Selbstbestimmung als Menschenrecht auch im Betrieb wachzuhalten. Durch technologische Entwicklungen, gesetzliche Änderungen und neue Instrumente eines modernen Datenschutzes im Sinne von Selbstdatenschutz und Selbstregulierung ist der Beschäftigtendatenschutz nicht nur in einem Konzern wie der Deutschen Bahn AG im Grundsatz nie abgeschlossen. Datenschutz muss, wie ein Betriebsrat der Deutschen Bahn AG anschaulich verdeutlicht, in Bewegung bleiben, sich dynamisch weiterentwickeln und darf möglichst niemals stillstehen. Denn für den Daten- und Persönlichkeitsschutz im Beschäftigungsverhältnis gibt es immer neue Herausforderungen.

Beim Umsetzen und Leben des Prinzips „Vorbildlicher Datenschutz" ist im konkreten Fall noch zu berücksichtigen: Der Vorstand der Deutschen Bahn hat, ähnlich wie die Deutsche Telekom, *im Jahr 2010 einen Datenschutzbeirat* gegründet, der die internen Datenschutzmaßnahmen und aktuellen Herausforderungen mit Hilfe von anerkannten Sachverständigen des Datenschutzes begleitet. Das unabhängige Gremium soll vor allem datenschutzrechtliche Transparenz schaffen und dem Vorstand Anregung und Unterstützung in datenschutzrechtlichen Fragen bieten, wie z. B. hinsichtlich der Videoüberwachungen auf Bahnhöfen. Die Gründung des Datenschutzbeirates bei der Deutschen Bahn AG ist ein wichtiger Baustein im Mosaik für die konsequente Umsetzung eines vorbildlichen Datenschutzes. Das Gremium ist weisungsunabhängig, kann frei handeln und setzt sich aus zwölf Mitgliedern zusammen. Besonderer Schwerpunkt der Arbeit des Datenschutzbeirates liegt in dem vertrauensvollen und kooperativen Dialog mit dem Vorstand des DB-Konzerns. Er hält sich aus dem operativen Datenschutzgeschäft her-

aus. An den Sitzungen nehmen verschiedene Vorstände und die Konzerndatenschutzbeauftragte teil. Der Datenschutzbeirat tagt an vier halben Tag im Jahr. Er ist mit Arbeitnehmervertretern sowie Datenschutzexperten aus Wissenschaft und Wirtschaft besetzt.

4 AUSWIRKUNGEN AUF BESCHÄFTIGUNGSDATENSCHUTZ IN WEITEREN HANDLUNGSFELDERN

4.1 Auswirkungen auf die KBV Hinweismanagement

Die Deutsche Bahn AG hat mit der KBV BDS und weiteren Maßnahmen wie der KBV Hinweismanagement aus dem Datenschutzskandal gelernt und Compliance, Datenschutz und Mitbestimmung rechtskonform miteinander verbunden. Die Konzernbetriebsvereinbarung zum Hinweismanagement im DB-Konzern (KBV Hinweismanagement) wurde am 13.3.2013 unterzeichnet.

Daher ist die Sachverhaltsaufklärung in der KBV BDS auch für das Hinweismanagement von größter Bedeutung: Sie unterwirft interne Ermittlungen im Konzern einem transparenten Verfahren, bezieht dabei die Mitbestimmung der Arbeitnehmervertretung ein und führt vor allem wieder zu einer doppelten arbeits- und datenschutzrechtlichen Verhältnismäßigkeitsprüfung (vgl. § 19 KBV BDS).

In einem weiteren Schritt wurden zusätzliche Mitarbeiter in der zentralen Abteilung Compliance (CC) eingestellt, dezentral in DB-Konzerngesellschaften Einheiten für Compliance geschaffen und schon vor der KBV BDS ein eigenes Vorstandsressort für „Compliance, Datenschutz, Recht und Konzernsicherheit“ gebildet. Damit ist der Datenschutz in einem eigenen Vorstandsressort angesiedelt. Zudem ist wegweisend festgelegt, dass die Abteilung Compliance keine ermittelnde Tätigkeit durchführt und hier eine deutliche „Gewaltentrennung“ besteht zwischen den Abteilungen Compliance und Konzernsicherheit.

Den Beschäftigten wird zusätzlich ein breites *Schulungsangebot zum Thema Compliance* angeboten, insbesondere Führungskräften und Mitarbeitern in Compliance-sensiblen Bereichen wie z. B. dem Konzerneinkauf. Die Aufklärung der Mitarbeiter soll vor allem durch Schulung erfolgen. Zusätzlichen zu den Schulungsmaßnahmen wurde bei der DB ein Compliance-Helpdesk eingerichtet, das als Informationsstelle auf Fragen zum richtigen Verhalten leicht erreichbar und kompetent Auskunft gibt (Fritz 2012, S. 205 f.). Mitarbeitern, die sich an das Compliance-Helpdesk wenden, wird auf Wunsch Vertraulichkeit zugesichert. Dies wurde in der KBV Hinweismanagement geregelt.

Der DB-Konzern geht den Hinweisen auf mögliche Verstöße nach. Die KBV Hinweismanagement vom 13.3.2013 begründet für Arbeitnehmer aber

keine Rechtspflicht, auf Compliance-Verstöße hinweisen zu müssen. Auf Wunsch wird den Hinweisgebern auch hier Vertraulichkeit zugesichert. Alle Beschäftigten werden darüber informiert, wie der Prozess verläuft, wenn ein entsprechender Hinweis von oder über einen Mitarbeiter eingeht. Das dient dazu, auch für das Hinweismanagement im DB-Konzern die datenschutzrechtlich erforderliche Transparenz herzustellen. Bei dem sich anschließenden Prüfprozess in Form interner Ermittlungen werden wieder die Vorgaben zur Sachverhaltsaufklärung mit der doppelten Verhältnismäßigkeitsprüfung in der KBV BDS genutzt. Der bzw. die Betroffene wird spätestens dann benachrichtigt, wenn das Ziel der Ermittlungen nicht mehr gefährdet ist. Das technische System zur Übermittlung von Hinweisen wurde von den Konzernbetriebsräten in der KBV Hinweismanagement einschließlich der Datensicherheitsbestimmungen mitbestimmt.

4.2 Auswirkungen auf die Rahmenkonzernbetriebsvereinbarung Beschäftigtendatenverarbeitung (RKBV Beschäftigten-DV)

Die KBV BDS führte dazu, dass die RKBV zur Verarbeitung von Beschäftigtendaten geändert und der KBV BDS angepasst wurde. Die neue Rahmen-Konzernbetriebsvereinbarung über Einführung und Betrieb von Verfahren zur Verarbeitung personenbezogener Beschäftigtendaten im DB-Konzern (RKBV Beschäftigten-DV) wurde am 24.8.2011 unterzeichnet. Sie umfasst Verfahren der Verarbeitung von Beschäftigtendaten sowohl in elektronischer Form als auch in Papierform und verweist damit auf § 32 Abs. 2 BDSG, der seit 2009 gilt und die Verarbeitung von Beschäftigtendaten in Papierform einbezieht.

§ 2 Abs. 1 RKBV Beschäftigten-DV definiert die Verantwortlichkeiten der einzelnen Konzerngesellschaften als verantwortliche Stellen, das heißt ihre Pflichten wie z. B. Löschen der Daten, wenn die Genehmigungsgrundlage weggefallen ist. Ziel der RKBV Beschäftigten-DV ist es, die Beschäftigtendaten vor Missbrauch zu schützen (§ 2 Abs. 3 RKBV Beschäftigten-DV): und zwar durch Wahrung und Förderung des Persönlichkeitsschutzes (vgl. § 75 Abs. 2 BetrVG) und durch Erhöhung der datenschutzrechtlich geforderten Transparenz, z. B. durch die Einrichtung von Datenausschüssen (§ 4 RKBV Beschäftigten-DV).

Das einzelne Konzernunternehmen ist weiterhin verantwortlich dafür, die zuständige Arbeitnehmervertretung und die Funktionsträger der Datenschutzorganisation frühzeitig einzubinden: ab der Investitionsentscheidung

bzw. mit Beginn der Planung zur Einführung oder Änderung von IT-Verfahren. Nur so können sie sich frühzeitig ein Bild machen sowohl von Zweck und Erforderlichkeit des beabsichtigten Verfahrens als auch von den damit verbundenen Datenflüssen. In der sonst üblichen Praxis von Unternehmen wird die frühzeitige und umfassende Information der Betriebsräte oftmals zur Farce und Transparenz letzten Endes für Betriebsräte oftmals eine Holschuld.

Die Erhebung, Verarbeitung oder Nutzung von Beschäftigtendaten ist nur mit Genehmigung der Unternehmensleitung zulässig (§ 3 Abs. 1 RKBV Beschäftigten-DV). In dem Antrag an das zuständige Mitglied der Unternehmensleitung, das für Personal zuständig ist, müssen Mindestangaben enthalten sein, die weitgehend übereinstimmen mit den Angaben im Verfahrensverzeichnis nach § 4e und 4g BDSG und Regelungsgegenständen, die in der Regel in Betriebsvereinbarungen enthalten sind (vgl. § 4 Abs. 3 RKBV Beschäftigten-DV). Die Angaben in dem zu genehmigenden Antrag beziehen sich unter anderem auf den Verwendungszweck, den betroffenen Personenkreis, die Art der Beschäftigtendaten, die Datenquellen, die Verfahrensbeschreibung, die Auswertungen, die Zugriffsberechtigungen, die Daten- und Informationsempfänger, die konkreten Löschfristen, die technisch-organisatorischen Schutzmaßnahmen, die Beschreibung der Rechtsgrundlagen der geplanten Verarbeitung, die Benennung des Auftragnehmers und eventueller Unterauftragnehmer bei Auftragsdatenverarbeitung sowie auf die Schnittstellen zu anderen Verfahren.

Der Antrag kommt anschließend in den zuständigen Datenausschuss (§ 3 Abs. 4 RKBV Beschäftigten-DV) und unterliegt einem Standard-Prozessablauf (RKBV Beschäftigten-DV, Anlage 2). Die datenschutzrechtliche Zulässigkeitsprüfung erfolgt somit in Datenausschüssen, die auf Konzern-, Unternehmens-, Geschäftsfeld- und Spartenebene gebildet sind. Hierfür werden die ständigen Mitglieder benannt, zu denen auch zwei Vertreter des zuständigen Betriebsratsgremiums gehören. Diese Anzahl variiert bei den verschiedenen Arten der Datenausschüsse.

Die Leitung der Datenausschüsse in den zugeordneten Konzernunternehmen haben die Fachkräfte für Datenschutz (FDS) unter Mitwirkung der Vertrauenspersonen für den Datenschutz (VPDS) in den „verantwortlichen Stellen“ (KBV BDS, Anlage 2, B 2.2). Die Konzerndatenschutzbeauftragte leitet den Konzerndatenschutzausschuss zur Behandlung von konzernweiten Pilot-Verfahren gemäß § 4 Abs. 6 RKBV Beschäftigten-DV und kann zu den anderen Datenausschüssen beratend hinzugezogen werden, ebenso wie externe Sachverständige.

Zur Arbeitsweise der Datenausschüsse wurde eine *Muster-Geschäftsordnung* in Anlage 4 der RKBV Beschäftigten-DV beigefügt, in der unter anderem die Hauptaufgaben beschrieben werden. Dem Datenausschuss obliegt es, die Interessen der Unternehmensleitung und den sicheren Schutz der Persönlichkeitsrechte der Beschäftigten in Einklang zu bringen, um ein abgestimmtes Verfahren herbeizuführen. Im Sinne von Transparenz sind die Datenausschüsse gehalten, *einen Jahresbericht* zu erstatten. Der Datenausschuss führt ein Verzeichnis der genehmigten Anträge über Einführung und Änderung von Datenverarbeitungsverfahren, Dateien/Datenbanken und Beschäftigtendaten.

Die entscheidungsvorbereitende Beteiligung der *Datenausschüsse* im Sinne einer Prüfung und der Abgabe einer Empfehlung ersetzt nicht die Rechte der Arbeitnehmervertretungen. Die Empfehlungen der Ausschüsse präjudizieren nicht die Entscheidungen der Arbeitnehmervertretungen (§ 4 Abs. 8 RKBV Beschäftigten-DV). Die Einbindung und Beteiligung der zuständigen Betriebsräte erfolgt parallel zur Arbeit der Datenausschüsse. Die Empfehlungen an den zuständigen Vorstand Personal können Zustimmung, Auflagen, Ablehnung oder auch ein abweichendes Votum enthalten. Empfehlungen im Sinne von Zustimmungen bedürfen einer Zwei-Drittel-Mehrheit der Stimmen. Die Funktionsträger der Datenschutzorganisation wirken im Vorfeld bei dem Entwurf der Verfahrensmeldung mit und führen die Vorabkontrolle nach § 4d Abs. 5 und 6 BDSG durch.

Die Datenausschüsse müssen mit allen Stellen zusammenzuarbeiten, die für die Kontrolle der Einhaltung von Datenschutzvorschriften zuständig sind – das heißt auch mit den Betriebsräten (§ 5 Abs. 1 RKBV Beschäftigten-DV). Hier wird eine Pflicht der Datenschutzfunktionsträger zur *Kooperation* mit dem Betriebsrat festgehalten (Simitis 2011, § 4g, Rdnr. 8). Die Mitglieder der Datenausschüsse werden durch die Muster-Geschäftsordnung auf Verschwiegenheit verpflichtet.

Hervorzuheben ist die Bestimmung in § 7 Abs. 2 RKBV Beschäftigten-DV: Demnach sind *heimliche Kontrollen* untersagt, denn „ohne Wissen der Benutzer einer DV-Anlage bzw. ohne Wissen des von der Datenverarbeitung Betroffenen darf keine Vorrichtung zu deren qualitativer und/oder quantitativer Kontrolle verwendet werden." Das erinnert stark an den Anhang der Bildschirmarbeitsverordnung (BildscharbV, Anhang Nr. 22). Ebenso dürfen keine rein automatisierten Entscheidungen getroffen werden, die für betroffene Beschäftigte eine Rechtsfolge nach sich ziehen oder sie erheblich beeinträchtigen (§ 7 Abs. 3 RKBV Beschäftigten-DV).

4.3 Auswirkungen auf die KBV IT

Angesichts des in der KBV BDS enthaltenen Auftrags zur gemeinsamen Weiterentwicklung des Regelwerks wurde auch die Konzernbetriebsvereinbarung zum Einsatz, zur Nutzung und zur Zulässigkeit von Auswertungen bei Bürokommunikationslösungen (KBV IT) überarbeitet. Dabei geht es wesentlich um die Kontrolle der E-Mail- und Internet-Nutzung bei zugelassener privater Nutzung in geringfügigem Umfang.

Die in einer früheren Fassung der KBV IT vorgesehene Kontrolle der Nutzung von Internet und E-Mails erwies sich als zu weitgehend. Zur Anpassung wurde frühzeitig der Berliner Beauftragten für den Datenschutz hinzugezogen. Hervorzuheben ist, dass der frühere Prüfprozess nie zur Anwendung kam, da die Verhandlungen zur konkreten Umsetzung angesichts der Entwicklungen zum Datenschutzskandal zurückgestellt wurden. Privatnutzung wird nur in geringfügigem Umfang gestattet, soweit der Nutzer den Nutzungsbedingungen zustimmt. Die Kontrolle der *Verkehrsdaten* durch den Arbeitgeber wird datenschutzrechtlich durch die vorliegende KBV IT einschließlich einer nachvollziehbaren Einwilligung der Beschäftigten rechtssicher gestaltet.

Ausdrücklich ausgenommen von den Kontrollen der E-Mail-Accounts wird die Kommunikation von und mit den Interessenvertretungen sowie Einrichtungen der betrieblichen Gesundheits- und Sozialfürsorge. Der Schutz vor Zugriff und Kontrolle muss durch *geeignete technische und organisatorische Maßnahmen* erfolgen (§ 4 Abs. 1, 2 KBV IT).

Die Nutzungsentscheidung der Beschäftigten im Sinne einer *Einwilligung* wird vom Verfahrensadministrator protokolliert. Zur Auswertung der Kontrolldaten wird eine paritätisch besetzte Kommission (§ 3 KBV IT) gebildet, mit je drei Vertretern des Konzernbetriebsrats und drei Vertretern des Arbeitgebers DB AG/DB Mobility Logistics AG. Die Konzerndatenschutzbeauftragte oder ihr Vertreter nimmt beratend ohne Stimmrecht teil. Die Mitglieder der Kommission sind zu schulen.

Die Kontrollmöglichkeiten der nur *eingeschränkt zugelassenen Privatnutzung* von E-Mail und Internet wurden begrenzt und an die Vorgaben der *Sachverhaltsaufklärung* mit der doppelten Verhältnisprüfung in der KBV BDS angepasst. Die gespeicherten Daten werden verringert, die Mitarbeiter umfassend informiert, und es wird ein stufenweises Verfahren im Sinne eines Eskalationsmodells (vgl. ULD 2010) eingeführt. Dabei wird zunächst eine Kontrolle mit anonymisierten Daten und erst nach der doppelten Verhältnismäßigkeitsprüfung eine Kontrolle mit personalisierten Daten durchgeführt.

Besondere Ereignisse, die § 2 Abs. 6 KBV IT definiert sind, können zunächst einer anonymisierten Analyse und in einem zweiten Schritt einer pseudonymisierten Stichprobenkontrolle unterworfen werden (§ 8 KBV IT). *Pseudonymisieren* ist laut der KBV BDS das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren (KBV BDS Anlage 1 Nr. 18 und § 3 Abs. 6a BDSG).

Eine detaillierte Auswertung mit Personenbezug darf dann nur unter Kontrolle durch eine paritätisch besetzte KBV IT-Kommission mit strikter Beachtung der Vorgaben der doppelten Verhältnismäßigkeitsprüfung gemäß §§ 18, 19 KBV BDS erfolgen. Als letztes Mittel können dann auch die *Inhaltsdaten* kontrolliert werden. Nach erfolgter Untersuchung muss ein Bericht erstellt und der Betroffene so früh wie möglich gehört werden (§ 9 Abs. 5 KBV IT). Die Mitglieder der IT-Kommission müssen über die erforderliche *Fachkunde und Zuverlässigkeit* verfügen und nach einer Belehrung eine Verpflichtung auf das Datengeheimnis nach § 5 BDSG und das Fernmeldegeheimnis nach § 88 Telekommunikationsgesetz unterschreiben.

Die KBV IT legt zudem konkret die *Löschfristen* für die protokollierten Daten fest. Die Verkehrsdaten von Internet- und E-Mail-Kommunikation dürfen für drei Monate gespeichert werden (§ 4 Abs. 7 KBV IT).

Einbezogen wird in § 10 KBV IT bei unzulässiger Datenauswertung *ein rechtssicheres Beweisverwertungsverbot,* das ansonsten in der Praxis von Betriebs- und Dienstvereinbarungen oft vernachlässigt bzw. fehlerhaft formuliert wird. Bislang fehlt ein gesetzliches Beweisverwertungsverbot. Zudem ist bisher die Rechtsprechung zu heimlichen Kontrollen und Beweisverwertung eher uneinheitlich. Von daher sollte ein rechtssicheres Beweisverwertungsverbot in derartigen Betriebsvereinbarungen zum Beschäftigtendatenschutz nie fehlen:

> „Die Verwendung von Tatsachen, die aufgrund einer unzulässigen Datenauswertung gewonnen werden, ist unzulässig. Der Arbeitgeber darf auf solche Maßnahmen keine personellen Maßnahmen stützen, die zu einer Veränderung der Beschäftigungsbedingungen, zur Beendigung des Arbeitsverhältnisses oder zu Er- oder Abmahnungen oder sonstigen Sanktionen gegenüber dem Beschäftigten führen. Der Arbeitgeber ist verpflichtet, eine derartig personelle Maßnahme zurückzunehmen und keinerlei Rechte aus dieser abzuleiten“ (§ 10 KBV IT).

4.4 Auswirkungen auf die KBV Konzerninterne Datenflüsse (KBV KID)

Die KBV KID ist die erste neu geschaffene Konzernbetriebsvereinbarung, die von der KBV BDS ausgehend als Basis-KBV vwerhandelt und im Juni 2013 unterzeichnet wurde. Es fehlt zum Zeitpunkt der Interviews also noch die praktischen Erfahrungen mit der KBV KID. Übermittlungen von Beschäftigtendaten an zentrale Konzernfunktionen wie z. B. Recht oder Personal sind grundsätzlich erforderlich (Vogt 2014). Die Übermittlung von Beschäftigtendaten ist das Zugänglichmachen oder Weitergeben an eine Person oder Stelle außerhalb der verantwortlichen Stelle. Dabei sind die Vorgaben der KBV BDS zu beachten und die Persönlichkeitsrechte der Beschäftigten zu wahren (§ 8 Abs. 2 KBV KID).

Im Mittelpunkt der KBV KID stehen konzernerhebliche Übermittlungen und die konzernweite Verarbeitung von Beschäftigtendaten, die als *Funktionsübertragungen* zwischen Konzernunternehmen und zentralen Konzernfunktionen datenschutzrechtlich einzuordnen sind. Die Antragsteller müssen diese Funktionsübertragungen (KBV BDS Anlage 1 Nr. 10, siehe Anhang) begründen, weshalb sie nicht als Auftragsdatenverarbeitung gemäß § 11 BDSG gestaltet werden können. Auftragsdatenverarbeitung geschieht im DB-Konzern nach Konzernstandardvertragsmustern. Beispiele dafür sind Dienstleistungen durch Service-Center-Personal wie z. B. Führung der Personalakte, Gehaltsabrechnung, Zeiterfassung, Abwicklung von Standardprozessen wie z. B. Urlaub und Jobtickets.

Bei einer konzerninternen bzw. -weiten Funktionsübertragung, die datenschutzrechtlich eine Übermittlung von personenbezogenen Daten der Beschäftigten darstellt, wechselt mit den Daten auch die *verantwortliche Stelle* nach § 3 Abs. 7 BDSG. Für jede Übermittlung zwischen den DB-Konzerngesellschaften bedarf es somit einer eigenen Rechtsgrundlage nach § 4 Abs. 1 BDSG (KBV KID, Präambel). Beispiele hierfür sind unter anderem Dienstreisebuchung über das Travel Management oder die Rechtsberatung des Konzernunternehmens bei Verfahren mit Personenbezug.

Die KBV KID regelt konzerninterne Datenflüsse für *Zwecke des integrierten Bahn-Konzerns* per Funktionsübertragung innerhalb des Bahn-Konzerns und schafft dafür klare und transparente Regeln. Ein konzerninterner Datenfluss ist die Übermittlung personenbezogener Beschäftigtendaten nach einheitlichen Kriterien zwischen Konzernunternehmen des DB-Konzerns und zentralen Konzernfunktionen aufgrund der Wahrnehmung einer Funktion des zentralen Konzernunternehmens für andere Konzernunternehmen (§ 2

Abs. 2 KBV KID). Bei den konzerninternen Datenflüssen müssen die Persönlichkeitsrechte der Beschäftigten und die Rechte der zuständigen Arbeitnehmervertretungen uneingeschränkt gewahrt bleiben (§ 3 Abs. 1 KBV KID). Die KBV KID reagiert damit auf die Tatsache, dass das Datenschutzrecht bisher für die Verarbeitung von Beschäftigtendaten innerhalb eines Konzerns *kein Konzernprivileg* kennt (siehe Bussche/Voigt 2014, S. 93 f.). Jedes Konzernunternehmen, das personenbezogene Beschäftigtendaten erhebt, verarbeitet, nutzt oder damit Dritte beauftragt, ist eine datenschutzrechtlich verantwortliche Stelle und Konzernunternehmen verhalten sich zueinander wie *Dritte* (§ 3 Abs. 8 Satz 2 BDSG). Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle:

> „Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten für die verantwortliche Stelle im Auftrag erheben, verarbeiten oder nutzen" (KBV BDS Anlage 1 Nr. 8).

Datentransfers zwischen Konzernunternehmen und zentralen Konzernfunktionen erfordern somit eine eigene legitimierende Rechtsgrundlage (§ 4 Abs. 1 BDSG). Das BDSG kann gemäß § 28 Abs. 1 Nr. 2 BDSG die Übermittlung erlauben, eine Einwilligung des Betroffenen kann eine Erlaubnis sein oder eine einschlägige Betriebsvereinbarung als andere Rechtsvorschrift kann die Übermittlung datenschutzrechtlich zulässig machen. Die Anwendbarkeit von § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist allerdings strittig. Damit die notwendigen konzerninternen Datenflüsse, die als Datenübermittlung auch im Interesse der Beschäftigten sein können, rechtssicher, transparent und jederzeit kontrollierbar gestaltet werden können, ist der Abschluss einer Konzernbetriebsvereinbarung KID als Rechtsgrundlage gemäß § 4 Abs. 1 BDSG ein wichtiger Schritt, der bereits in der KBV BDS in Aussicht gestellt worden ist.

Mit der KBV KID wird der hohe Schutzstandard, der für *die Auftragsdatenverarbeitung* nach § 11 BDSG vorgesehen ist, auch für die *Funktionsübertragung* sichergestellt. Einer Funktionsübertragung wird nur dann zugestimmt, wenn beide Betriebsparteien sie für konzernrelevant halten und eine Auftragsdatenverarbeitung nach § 11 BDSG nicht möglich ist.

Die Prüfung, ob der beantragte Datenfluss nach der KBV KID empfohlen, in die Anlage zur KBV KID aufgenommen und damit anerkannt wird,

läuft gemäß §1 Abs. 3 KBV KID parallel zum Mitbestimmungsverfahren nach §87 Abs. 1 Nr. 6 BetrVG, in dem es um die betriebsverfassungsrechtliche Legitimation des Verfahrens und der eingesetzten IT-Systeme geht. *§87 Abs. 1 Nr. 6 BetrVG* eröffnet Betriebsräten bekanntermaßen umfassende Regelungsmöglichkeiten, wenn technische Kontrolleinrichtungen eingeführt und angewendet werden:

> „§87 Mitbestimmungsrechte: (1) Der Betriebsrat hat, soweit eine gesetzliche oder tarifliche Regelung nicht besteht, in folgenden Angelegenheiten mitzubestimmen: […] 6. Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen."

Die Daten dürfen erst übermittelt werden, wenn das betriebsverfassungsrechtliche Verfahren abgeschlossen ist (§3 Abs. 3 KBV KID) und der KBR zugestimmt hat. Betriebsräte anderer Unternehmen sollten insbesondere die Angaben in dem Antrag, die Dokumentation und die Prüfkriterien nutzen, die in §4 Abs. 3, §5 und §6 Abs. 1 KBV KID dokumentiert sind, wenn sie Funktionsübertragungen regeln müssen. Ganz wichtig erscheint die allgemeine Regel in §3 Abs. 4 KBV KID, wonach die datenabgebende Stelle gemeinsam mit der datenaufnehmenden Stelle weiterhin verantwortlich für die ordnungsgemäße Datenverarbeitung und die Einhaltung der im DB-Konzern geltenden Datenschutzvorschriften bleibt.

Das Beratungsgremium auf Konzernebene ist paritätisch mit je zwei Vertretern des Konzernbetriebsrats der DB AG und der Arbeitgeberseite besetzt; der Konzerndatenschutz nimmt wiederum beratend teil (§4 Abs. 1, 2 KBV KID). Den jeweils betroffenen Datenausschüssen im DB-Konzern wird innerhalb von zwei Monaten Gelegenheit zur Stellungnahme gegeben. Die Empfehlung des Gremiums dient zur betriebsverfassungsrechtlichen Beurteilung durch den Konzernbetriebsrat DB AG und legt die Prüfkriterien gemäß §5 Abs. 1–6 KBV KID zugrunde.

Der aufgenommene Datenfluss wird von den beteiligten Konzernunternehmen und den zuständigen Datenschutzbeauftragten alle zwei Jahre in einem Audit auf Erforderlichkeit und Übereinstimmung mit den Prüfkriterien der KBV KID (§5 KBV Abs. 1–6 KID) überprüft. Für diese Audits wird in der KBV KID auf §23 KBV BDS verwiesen (§6 Abs. 1 KBV KID). Das Ergebnis wird dem Ausschuss des KBR Datenschutz & Neue Technologien des Konzernbetriebsrats mitgeteilt.

Alle fünf Jahre werden die in der Anlage aufgenommenen konzerninternen Datenflüsse von den Betriebsparteien auf Erforderlichkeit, Gesetzeskonformität und Anpassungsbedarf von den verantwortlichen Stellen mit dem Konzerndatenschutz evaluiert und das Ergebnis dem Beratungsgremium vorgelegt. Folge des Audits kann dann auch sein, dass die Anerkennung des konzerninternen Datenflusses erlischt. Die verantwortlichen Personen erhalten ein Einsichtsrecht in IT-Verfahren, in sämtliche gespeicherten Beschäftigtendaten und in die Dokumentation, das auch unangekündigt ausgeübt werden kann (§ 6 Abs. 2 KBV KID). Die aufgenommen, geänderten oder aufgehobenen konzerninternen Datenflüsse sind in dem jährlichen Datenschutzbericht für den DB-Konzern aufzuführen (§ 7 Abs. 3 KBV KID), den der KBR vom Arbeitgeber erhält (§ 27 Abs. 7 KBV BDS).

In § 1 Abs. 3 Satz 4 KBV KID wird der Vorrang der in der Anlage zur KBV KID dokumentierten konzerninternen Datenflüsse vor eventuell schlechteren gesetzlichen Regelungen festgeschrieben, falls doch einmal gesetzlich auf nationaler oder europäischer Ebene ein Konzernprivileg eingeführt wird:

> „Soweit in der Zukunft eine gesetzliche Regelung des Konzernprivilegs in Kraft treten sollte, so sollen dieser die Regelungen der KBV zu den in der Anlage geregelten Datenflüssen vorgehen."

Für andere Unternehmen sind insbesondere die umfassenden und abschließenden Prüfkriterien in der Anlage zur KBV KID zu empfehlen.

5 HEUTE UND MORGEN: DATENSCHUTZ FÜR DIE ZUKUNFT GESTALTEN

Im DB-Konzern kam es 2009 zu einer öffentlichkeitswirksamen Datenschutzhavarie, zu einem Imageschaden und zu einem hohen Bußgeld durch die Aufsichtsbehörde für den Datenschutz in Berlin. Das Großunternehmen hat daraus gelernt und einen Neustart im Datenschutz als Chance unternommen. Dadurch kam es zur Erarbeitung und Verabschiedung der KBV BDS und somit zu einer Stärkung des gesamten Konzerndatenschutzes und der Mitbestimmung im Konzern. Die KBV BDS, die KBV IT und die KBV KID gehen zum Teil über das gesetzliche Schutzniveau hinaus und haben gerade dadurch wesentlich dazu beigetragen, dass das verlorengegangene Vertrauen der Mitarbeiter zurückgewonnen werden konnte.

Heute wird der Beschäftigtendatenschutz von allen Beteiligten, das heißt auch den Führungskräften, im Konzern positiv gesehen und als Wettbewerbs- und Imagefaktor gewertet, der gerade in Zeiten des Fachkräftemangels durchaus zur Personalgewinnung beitragen kann. Beschäftigtendatenschutz kann helfen, den Kampf um die Talente zu gewinnen, so ausdrücklich die Überzeugung der Mitarbeiter der Abteilung Arbeitsrecht. Er dürfe auch zukünftig als wichtiger Faktor der Unternehmenskultur nicht vernachlässigt werden.

5.1 Kulturwandel in Bezug auf die gelebte Mitbestimmung

Die vertrauensvolle Zusammenarbeit der Abteilung Arbeitsrecht mit den Interessenvertretungen hat sich im Rahmen der Prozesserfahrung mit der KBV BDS und deren Inhalten nach Aussagen der interviewten Mitarbeiter bewährt. Ein gangbarer und anzustrebender vorbildlicher Beschäftigtendatenschutz lebt vor allem davon, dass sich die Verhandlungspartner gegenseitig vertrauen können. Das gegenseitige Vertrauen und das gemeinsame Verständnis davon, was Datenschutz ist und wie dieser im Konzern zu gewährleisten ist, erleichtern aktuelle und zukünftige Verhandlungen zu Konzernbetriebsvereinbarungen, die den Beschäftigtendatenschutz wesentlich betreffen. Voraussetzung ist hierfür immer eine *umfassende Transparenz für Betriebsräte*, was die Einführung von IT-Systemen und die Verarbeitung, Nutzung und Erhebung von Beschäftigtendaten betrifft. Das bedeutet ein wirkliches

Informationsrecht für Betriebsräte als Bringschuld des Arbeitgebers, wobei die Information frühzeitig in der Planungsphase einsetzen soll und alle vorhandenen Datenschutzunterlagen den Betriebsräten zur Verfügung stehen (§ 80 Abs. 2 BetrVG) müssen.

Der Mitbestimmungsprozess im DB-Konzern im Hinblick auf den Beschäftigtendatenschutz wird nie abgeschlossen sein. Weitere erforderliche Regelungen warten. Eins ist jedoch bei der Bahn offenbar: Eine Basissicherheit im Umgang der Betriebsparteien untereinander ist erreicht und hilft allen Beteiligen dabei, guten Beschäftigtendatenschutz zu verwirklichen. Hinzu kommt, dass *die Datenschützer* sich neutral verstehen, kooperativ mit Interessenvertretungen, der Abteilung Arbeitsrecht und Führungskräften zusammenarbeiten und jederzeit für Beratung und fachlichen Austausch bereitstehen. Durch Prozess- und Strukturvorgaben in der KBV BDS ist offenkundig ein kooperativer und vertrauensvoller Suchprozess zur Gewährleistung eines vorbildlichen Beschäftigtendatenschutzes im DB Konzern entstanden, der immer wieder zu guten Verhandlungsergebnissen beiträgt.

5.2 Aktuelle Themen des Beschäftigtendatenschutzes im DB-Konzern

Social Media

Der DB-Konzern beschäftigt sich aktuell mit den Möglichkeiten von *Social Media* und insbesondere mit der Frage: Wie lassen sich soziale Netzwerke für das Unternehmen nutzen? Hier sind wieder die Grundprinzipien der KBV BDS zu beachten. Der Konzernbetriebsrat beschäftigt sich aktuell ebenfalls mit dem Thema und hat hierfür ein Grundsatzpapier mit Anforderungen aus Sicht der Beschäftigten und der Interessenvertretungen entwickelt. Das Thema *BYOD* (bring your own device) – das heißt, dass Beschäftigte immer stärker ihre eigenen privaten mobilen Geräte in der Arbeit einsetzen wollen – hat die Deutsche Bahn AG bislang noch nicht auf die Tagesordnung gesetzt. Die Auswirkungen in Bezug auf Datenschutz und Datensicherheit, die BYOD mit sich bringt, erscheinen bislang aus Sicht der Datenschützer und Betriebsräte nicht handhabbar.

AEO-Terrorlisten-Screening

Das Screening von Mitarbeitern, ob sie in *EU-Anti-Terrorlisten* erfasst sind, wird zurzeit nur bei den DB-Konzerngesellschaften durchgeführt, die mit

Außenwirtschaft zu tun haben und den zollrechtlichen Status eines zugelassenen Wirtschaftsbeteiligten (Authorised Economic Operator – AEO) erlangen wollen. Die international tätigen Unternehmen erlangen den AEO-Status nur, wenn sie einen flächendeckenden und systematischen Abgleich der Mitarbeiter- und Bewerberdaten mit den Listen verdächtiger Personen nach den EG-Verordnungen vornehmen.

Von daher wurde der datenschutzgerechte Umgang mit den EU-Anti-Terrorlisten und dem geforderten Mitarbeiterscreening im DB-Konzern bislang nur dort von zuständigen Gesamtbetriebsräten in Gesamtbetriebsvereinbarungen geregelt, wo es unbedingt erforderlich ist. Die Anti-Terrorlisten sind datenschutzrechtlich aus Sicht der Aufsichtsbehörden für den Datenschutz äußerst umstritten, insofern bezog der DB-Konzern auch bei diesem Thema frühzeitig die zuständige Datenschutzbehörde in Berlin ein (siehe auch Gola/Wronka 2013, Rdnr. 1215). Aus Sicht der Datenschutzbehörden ist das Mitarbeiter-Screening nicht erforderlich, weil Kreditinstitute ohnehin bei Gehaltszahlungen nach § 25c Kreditwesengesetz einen Abgleich mit den Terroristenlisten vornehmen müssen (ebd., Rdnr. 1217).

Personalinformations- und Personalverwaltungssystem

Der DB Konzern setzt PeopleSoft als *Personalinformationssystem* ein, als Software für die Personalverwaltung. Die KBV PeopleSoft wurde von den Betriebsparteien im August 2014 neu vereinbart.

Gesetzliche Änderungen

Im DB-Konzern haben die Betriebsparteien frühzeitig entschieden, sich auf dem Weg zur KBV BDS von dem Entwurf der Bundesregierung zu einem Beschäftigtendatenschutzgesetz im Jahr 2010 abzukoppeln. Auch die gesetzlichen Änderungen, die die Verabschiedung einer EU-Datenschutzgrundverordnung mit sich bringen könnte, werden von den Betriebsparteien erst einmal abgewartet bzw. die Deutsche Bahn AG bringt sich in den aktuellen Prozess ein und nutzt vorhandene Spielräume. Auf den europäischen oder nationalen Gesetzgeber will die Deutsche Bahn AG nach Aussagen der Arbeitsrechtsabteilung lieber nicht warten, sondern den Prozess zu einem vorbildlichen Datenschutz weiter voranbringen und auch neue Themen wie z. B. Social Media oder Mobile Telefonie im Geist der KBV BDS angehen.

6 SCHLUSSFOLGERUNGEN UND TIPPS FÜR INTERESSENVERTRETUNGEN

Die Entstehung der KBV BDS im DB-Konzern ist sicherlich wesentlich der Ausnahmesituation und der datenschutzrechtlichen Vertrauenskrise geschuldet, in der sich der Konzern 2009 befand. Der öffentliche Druck auf den Arbeitgeber war groß, zudem wurde er an seinem Wort zum Prinzip „Vorbildlicher Datenschutz" gemessen.

Nicht überall kann oder muss der Beschäftigtendatenschutz komplett neu aufgestellt und von Null begonnen werden. Dennoch lassen sich aus dem Bahn-Beispiel wichtige Erkenntnisse für andere Unternehmen und Betriebsräte für einen vorbildlichen Beschäftigtendatenschutz gewinnen, die im Folgenden auf Übertragbarkeit geprüft werden. Die konkrete Umsetzung des Beschäftigtendatenschutzes ist unter anderem abhängig von der Größe des Unternehmens, der IT-Infrastruktur der verantwortlichen Stellen und der Sensibilität der Daten. Nachfolgend werden Tipps für Betriebsräte aus anderen Unternehmen und Konzernen zusammengestellt, wie Beschäftigtendatenschutz in der Praxis erfolgreich durchgesetzt und gelebt werden kann.

Wille zum Datenschutz

Das Beispiel DB-Konzern zeigt: Ein vorbildlicher Beschäftigtendatenschutz kann auch gegen Widerstände umgesetzt werden, wenn dies vom Vorstand als Machtpromotor und von den Interessenvertretungen gemeinsam getragen wird. Es muss ein klarer Wille zum Datenschutz bestehen. Dies gilt für den Vorstand oder die Geschäftsführung ebenso wie für Führungskräfte und Interessenvertretungen. Es sollte sich bei der Implementierung des Prinzips „Vorbildlicher Datenschutz" immer um einen Top-down-Ansatz handeln, der durch einen Bottom-up-Ansatz, das heißt durch die Beteiligung der Beschäftigten und ihrer Führungskräfte, unbedingt ergänzt werden sollte. Ohne Zweifel zeigt das untersuchte Beispiel DB Konzern: Die Umsetzung des gesetzlich geforderten Beschäftigtendatenschutzes in eine gute Praxis braucht viele Multiplikatoren, insbesondere Machtpromotoren, die ganz oben in der Hierarchie angesiedelt sind.

Datenschutz nicht nur als Kostenfaktor sehen

Datenschutz darf nicht ausschließlich als Kostenfaktor angesehen werden. Personalabteilung, Datenschützer und Interessenvertretungen sollten gemeinsam den Nutzen eines guten und vorbildlichen Beschäftigtendatenschutzes systematisch herausstellen. Leider ist ein gutes Datenschutzniveau in der Regel unsichtbar (vgl. Lepperhoff/Jaspers 2013). Datenschutzskandale können die wirtschaftliche Existenz eines Unternehmens bedrohen, sei es durch einen Imageverlust oder durch Auflagen der zuständigen Aufsichtsbehörde. Zudem sind Datenschutzskandale kostspielig, wenn empfindliche Bußgelder verhängt werden oder teure Imagekampagnen durchzuführen sind. Zukünftig sollen die Bußgelder nach der EU-Datenschutzgrundverordnung (Entwurf) in der Höhe erheblich gesteigert werden. Indem man grundlegende Datenschutzprinzipien wie z. B. Erforderlichkeit, Zweckbestimmung, Datenvermeidung und Datensparsamkeit in Verbindung mit einer Verhältnismäßigkeitsprüfung konsequent umsetzt, lassen sich bei IT-Projekten Kosten einsparen und Aufwand reduzieren, wie mehrere Konzernbetriebsräte berichten. Änderungen von IT-Systemen können durch vorherigen echten Systemdatenschutz erheblich vereinfacht durchgeführt werden. Fehlender Datenschutz und mangelnde Datensicherheit können Unternehmen teuer zu stehen kommen.

Hinzu kommen im DB-Konzern grundsätzliche Anforderungen an IT-Systeme und Verfahren, die Transparenz über die Datenverarbeitung im Unternehmen und Konzern schaffen sollen. Alle verwendeten DV-Systeme müssen klar strukturiert und transparent sowie abschließend und vollständig dokumentiert sein (§ 8 Abs. 1 KBV BDS). Das ist eine wesentliche Voraussetzung dafür, dass die *Gebote der Datensicherheit und des Datenschutzes nach § 9 und Anlage zu § 9 BDSG* eingehalten werden können. Daran mangelt es immer wieder in der Praxis. Zum Trennungsgebot zur Zweckbindung in Anlage zu § 9 BDSG Satz 1 Nr. 8 regelt die KBV BDS explizit und wiederum vorbildlich in § 7:

> „§ 7 Trennungsgebot
> (1) Personenbezogene Beschäftigtendaten sind vollständig getrennt nach dem jeweiligen Zweck, zu dem sie erhoben wurden, zu verarbeiten und zu nutzen. (2) Die verantwortliche Stelle muss durch geeignete technische und organisatorische Maßnahmen die Einhaltung des Trennungsgebotes sicherstellen."

Mangelnder Datenschutz kann zu einem Strafverfahren führen, wenn die zuständige Aufsichtsbehörde eine Anzeige bei den Strafermittlungsbehörden erstattet. Vorsätzliche und unverhältnismäßige Datenschutzverstöße können als Straftaten gewertet werden (Bundesgerichtshof, Urteil v. 4.6.2012 – 1 StR 32/13). Verstöße gegen Datenschutzbestimmungen können arbeitsrechtliche Maßnahmen des Arbeitgebers nach § 138 Bürgerliches Gesetzbuch (BGB) nichtig machen (BAG, Urteil v. 15.11.2012 – 6 AZR 339/11).

Guter und qualitätsorientierter Datenschutz sollte von den Beteiligten Personen im Unternehmen immer als Wettbewerbsfaktor und unerlässlicher Baustein einer guten Unternehmenskultur gesehen werden. Bei der Deutschen Bahn ist vorbildlicher Beschäftigtendatenschutz ein wichtiger Faktor im Kampf um qualifizierte Fachkräfte und um junge Talente.

Datenschutz braucht ausreichende Ressourcen

Der Beschäftigtendatenschutz darf von der jeweiligen *verantwortlichen Stelle* nicht rein wirtschaftlichen Überlegungen bzw. Budgetzwängen untergeordnet werden. § 3 Abs. 7 BDSG definiert:

> „Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt."

Dezentraler und zentraler Datenschutz benötigen ausreichende Ressourcen, sei es Personal, zeitliche Entlastung, Räume, Aus- und Fortbildung, Schulungen und fixe Besprechungstermine. Eine dezentrale Datenschutzorganisation kann zudem richtig viel Geld kosten, allerdings ebenso wie ein unterlassener Datenschutz. Auf der Nutzenseite des Ressourceneinsatzes für guten betrieblichen Datenschutz steht dafür unter anderem Akzeptanz und Vertrauen der Belegschaft, Rechtssicherheit, Transparenz und grundlegendes Vertrauen zwischen allen Beteiligten im Konzern, wie das Beispiel des DB-Konzerns deutlich zeigt.

Betriebsvereinbarungen zum Beschäftigtendatenschutz als Rechtsvorschrift

Vieles spricht dafür, den Beschäftigtendatenschutz in einer gesonderten (Konzern-)Betriebsvereinbarung explizit zu regeln. Vor allem gibt eine solche Betriebsvereinbarung *Rechtssicherheit* und trägt durch nützliche, konkrete und überprüfbare Regelungen zur Prozess-, Struktur- und Ergebnisqualität

in diesem Handlungsfeld bei. Sie erleichtert die alltägliche Arbeit vor Ort und trägt, richtig praktiziert, zur vermehrten Kommunikation über die Gewährleistung der informationellen Selbstbestimmung bei. Auch im betrieblichen Datenschutz ist offenkundig Kommunikation von besonderer Bedeutung.

Allerdings sind dabei einige Erkenntnisse aus der Diskussion der KBV BDS grundsätzlich zu beachten. Betriebsvereinbarungen sollten auch für Daten in Papierform wie z. B. in Archivierungssystemen (auch Personalaktenarchiv) gemäß § 32 Abs. 2 BDSG gelten. Betriebsvereinbarungen, seien sie zu IT-Verfahren mit Datenschutzbestandteilen, zu Torkontrollen oder vollständig als Rahmenbetriebsvereinbarung zum Beschäftigtendatenschutz formuliert, müssen klare Gebote, Verbote und richtige Begriffsbestimmungen enthalten (§ 1 Abs. 4 und Anlage 1 zu KBV BDS, § 3 BDSG). Ansonsten kann keine Handlungssicherheit für einen maximalen Beschäftigtendatenschutz erreicht werden. Unter anderem ist ein klares und eindeutiges Verbot von Leistungs- und Verhaltenskontrollen zu vereinbaren.

Betriebsvereinbarungen als *Rechtsvorschrift für den Datenschutz gemäß § 4 Abs. 1 BDSG* müssen sich auf gesetzliche Grundlagen, z. B. im Bundesdatenschutzgesetz, konkret beziehen. Da viele Regelungen im BDSG unbestimmt bzw. zu vage sind, müssen die erforderlichen Datenschutzvorgaben und Mitbestimmungsregeln im Sinne einer Anpassung an das jeweilige Unternehmen konkretisiert werden. Diese Bestimmungen müssen *ausreichend konkret, kontrollierbar und nachvollziehbar* sein. Leerformeln und Selbstverständlichkeiten hingegen sind zu vermeiden, z. B. dass bei allen Aktivitäten des Arbeitgebers die gesetzlichen Regelungen des Datenschutzes und der Persönlichkeitsrechte der Mitarbeiter beachtet werden. Solche Formulierungen sind wenig hilfreich.

Datenschutzbegriffe sind im Datenschutzrecht legal definiert und sollten keinesfalls umformuliert werden, wie leider oft in Betriebsvereinbarungsentwürfen zu lesen ist. Allerhöchstens sind sie zu konkretisieren, damit sie ein gemeinsames Verständnis der Betriebsparteien ermöglichen (vgl. Anlage 1 zur KBV BDS, siehe Anhang). Das Gleiche gilt für Begriffe aus dem Betriebsverfassungsrecht. Unbestimmte Rechtsbegriffe wie z. B. „erforderlich", „rechtzeitig" oder „umfassend" sind wenn möglich mit Definitionen aus Rechtsquellen, Beispielen oder Erläuterungen zu konkretisieren.

Der Beschäftigtendatenschutz in Betriebsvereinbarungen sollte stets alle Phasen der Datenverwendung umfassen, somit stets auch als sachlichen Gegenstand die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten der Beschäftigten (Beschäftigtendaten) beinhalten. Im personellen

Geltungsbereich sollten sich die Betriebsvereinbarungen auf Beschäftigte gemäß § 3 Abs. 11 BDSG beziehen. Auch Bewerber und ehemalige Beschäftigte, deren Beschäftigungsverhältnis beendet ist, sollten in den personellen Geltungsbereich pragmatisch einbezogen werden, wenn die Betriebsvereinbarung richtig die Phasen der Begründung, der Durchführung und der Beendigung des Beschäftigungsverhältnisses im Sinne von § 32 Abs. 1 BDSG umfassend regeln soll. § 10 KBV BDS stellt hierfür das hilfreiche Gebot auf:

> „Die Begriffe ‚Beschäftigte' und ‚Personenbezogene Beschäftigtendaten' sind im Rahmen der Auslegung und Umsetzung dieser Vereinbarung im Zweifel weit auszulegen."

So sollte für die Phase der Begründung nicht vergessen werden, Bewerbungsunterlagen bei abgelehnten Bewerbern und Bewerberinnen zurückzugeben oder zu vernichten, wenn keine Einwilligung zur langfristigen Speicherung der Unterlagen und der Daten für eine spätere Einstellung vorliegt. Für leitende Angestellte sollte der Arbeitgeber sich verpflichten, die vereinbarten Regelungen ebenso umzusetzen, z. B. durch eine Vereinbarung mit dem Sprecherausschuss (§ 2 KBV BDS) oder durch Einwilligungen.

Immer ist ein korrekt formuliertes Beweisverwertungsverbot aufzunehmen, das die Einführung von heimlich und unzulässig gewonnenen Tatsachen in gerichtliche Prozesse verbietet und personalrechtliche Maßnahmen unzulässig macht. So kann z. B. formuliert werden:

> „Informationen und Daten, die unter Verletzung gesetzlicher Vorschriften, anderer Bestimmungen oder der vorliegenden Betriebsvereinbarung vom Arbeitgeber rechtswidrig gewonnen wurden, dürfen nicht zu Lasten der Beschäftigten zu arbeitsrechtlichen Maßnahmen genutzt werden. Entgegen Vorstehendem vorgenommene negative personelle Maßnahmen sind unwirksam und werden zurückgenommen. Der Betriebsrat und betroffene Beschäftigte können die Löschung der Informationen und Daten verlangen. Dem Verlangen ist vom Arbeitgeber ausnahmslos zu entsprechen."

In der Praxis bereitet ein richtiges *Löschkonzept,* das die Vernichtung von Akten oder die konsequente Löschung von Daten auf der Festplatte beinhaltet, immer wieder große Probleme. Deshalb ist es unbedingt erforderlich, kon-

krete Löschfristen für gespeicherte Datenbestände, Aufbewahrungsfristen für Auswertungen/Reports und ein umsetzbares und kontrollierbares Löschkonzept zu vereinbaren. Ebenso sollten Verschlüsselungsverfahren nicht vernachlässigt werden (§ 9 und Anlage zu § 9a Satz 3 BDSG).

Eine Betriebsvereinbarung zu IT-Verfahren sollte immer auch bei allen Fragen zu Prozessen und Strukturen des Beschäftigtendatenschutzes die Mitbestimmung der Interessenvertretungen maximal wahren, ausbauen und stets Verfahren der Information, Beteiligung und Mitbestimmung sorgfältig beschreiben und vor allem konkret umsetzen. Dabei sollte im Interesse eines vorbildlichen Datenschutzes möglichst über die gesetzlichen Ansprüche der Betriebsräte zugunsten der Beschäftigten hinausgegangen werden – so vorbildlich geschehen in der KBV BDS der Deutschen Bahn. Dies wurde offensiv vom neuen Vorstand gewollt und wird auch heute noch praktiziert.

Eine Betriebsvereinbarung sollte aus Qualitätsgründen Datenschutzaudits regeln, die den Stand der Einhaltung der Betriebsvereinbarung und des Beschäftigtendatenschutzes überprüfen helfen und Chancen zur kontinuierlichen Verbesserung des Datenschutzniveaus aufzeigen. Datenschutzaudits helfen zudem bei der Vergabe von Auftragsdatenverarbeitung nach § 11 BDSG, da während des Auftragsdatenverhältnisses regelmäßige Kontrollen beim Auftragnehmer vorgesehen sind (§ 11 Abs. 2 BDSG; Kiesche/Wilke 2015).

In die Schlussabstimmungen zur Betriebsvereinbarungen ist eine Regel zur Beweislast des Arbeitgebers aufzunehmen, wenn Betriebsräte Verstöße gegen die jeweilige Betriebsvereinbarung rügen. In diesem Fall obliegt es dem Arbeitgeber, dies zu widerlegen. Die abschließende Feststellung, ob ein Verstoß vorliegt, sollte eine unabhängige Stelle (§ 30 KBV BDS) treffen, die festzulegen ist. In § 29 Abs. 1 der KBV BDS ist diese *Beweislastumkehr* festgehalten. Somit stellt der Arbeitgeber mit einer solchen Regelung das notwendige Vertrauen wieder her.

Wird ein Verstoß gegen das Datengeheimnis (§ 12 KBV BDS, § 5 BDSG) oder gegen die Betriebsvereinbarung festgestellt, so können die zuständigen Vorgesetzten zur Rechenschaft gezogen werden. Zuwiderhandlungen gegen diese Vereinbarung werden nämlich bei schuldhaftem Verhalten, wozu auch Unterlassen zählen kann, mit individuellen arbeits- bzw. vertragsrechtlichen Konsequenzen gegenüber den verantwortlichen Vorgesetzten geahndet, soweit deren schuldhaftes Tun bzw. Unterlassen zum Verstoß beigetragen hat (§ 29 Abs. 2 KBV BDS). Die (arbeitsrechtlichen) Konsequenzen werden von der unabhängigen Stelle, die paritätisch mit je drei Mitgliedern des Arbeitgebers und drei vom KBR benannten Mitgliedern besetzt ist, festgelegt (§§ 29 Abs. 3 und 30 Abs. 1 KBV BDS).

Beschäftigtendatenschutz muss mit einem Kulturwandel einhergehen

Das Beispiel des DB-Konzerns zeigt eindringlich: Beschäftigtendatenschutz ist nicht nur eine Frage der Rechtssetzung und Rechtsüberwachung, sondern auch eine Frage der vertrauensvollen Unternehmenskultur und des Bewusstseiwns für ein besonders wichtiges Grundrecht.

Gerade dann, wenn es zu Datenschutzverstößen größeren Ausmaßes gekommen ist, muss anschließend ein systematischer Kulturwandel im Sinne von Change Management betrieben werden, der möglichst alle Beschäftigten erreicht. Allen Beschäftigten ist daher systematisch und vorrangig die Angst vor Datenschutz und Datenverstößen zu nehmen. Das erfordert umfassende Transparenz, unter anderem hinsichtlich der Ziele und Zwecke der Datenverarbeitung, der grundlegenden Datenschutzprinzipien und der Auftragsdatenverarbeitung. Zur Verwirklichung von Transparenz gehört eine umfassende Dokumentation, die das BDSG z. B. in § 32 Abs. 1 Satz 2 bei *internen Ermittlungen* vorsieht.

Das vorrangige Ziel der KBV BDS ist neben der Nachhaltigkeit die Herstellung von Transparenz, damit unter anderem die Beschäftigten ihre Kontrollaufgaben und Rechte im Datenschutz effektiv wahrnehmen können. Das setzt verschiedene Maßnahmen voraus: vor allem eine umfassende Unterweisung (§ 4g Abs. 1 Satz 4 Nr. 2 BDSG), Informationen, Workshops und Schulungs- bzw. Sensibilisierungsmaßnahmen für IT-Administratoren, Führungskräfte und Beschäftigte sowie die Beteiligung der Beschäftigten und Führungskräfte. Administratoren sind die Personen im Unternehmen, die die informationstechnische Infrastruktur des Unternehmens auf der Basis von umfassenden Zugriffsrechten auf das System verwalten (z. B. planen, installieren, konfigurieren und pflegen) oder Zugriffe auf Daten verwalten oder durchführen (KBV BDS Anlage 1 Nr. 11).

Beim DB-Konzern ist besonders die Datenübersicht gemäß § 24 Abs. 2 KBV BDS hervorzuheben. Sie bereitet den Weg dafür, eine fundierte Auskunft nach § 34 BDSG zu verlangen. Ebenso sollten Anfragen von Beschäftigten an den Datenschutzbeauftragten oder an die Betriebsräte genutzt, verallgemeinert und viel stärker als bisher für das interne Marketing von Beschäftigtendatenschutz in Unternehmen eingesetzt werden.

Auf dem Weg zu einem vorbildlichen Datenschutz in Unternehmen und Konzernen ist es von entscheidender Bedeutung, dass die beteiligten Datenschützer, Personalverantwortlichen, Vertreter der Abteilung Arbeitsrecht und Betriebsräte ein gemeinsames Verständnis dessen herausbilden, was guter Beschäftigtendatenschutz tatsächlich bedeutet. Das setzt eine eindeutige

Klärung oder Festlegung der Datenschutzbegriffe und Ziele voraus. Im DB-Konzern wurde beispielsweise der Unterschied zwischen *Auftragsdatenverarbeitung* und *Funktionsübertragung* exakt geklärt. In Seminaren für Interessenvertretungen bereitet diese Unterscheidung in der Regel die größten Schwierigkeiten. Dieses Verständnis hilft, bei neuen Themen des Beschäftigtendatenschutzes in Verhandlungen kooperativ eine gemeinsame Lösung zu finden.

Datenschutzrecht muss in Tagungen, Seminaren oder Workshops vereinfacht und anhand von konkreten Beispielen und Fällen verdeutlicht bzw. geübt werden; er muss als Grundrecht der Beschäftigten vermittelt werden. Datenschutz muss mögliche Probleme erkennen und lösen, damit den Beteiligten sein Nutzen bewusst und die Organisation gezielt aus Erfahrung klug wird (Wilke/Kiesche 2015). Datenschutzerfolge sollten dargestellt und kommuniziert werden, wenn z. B. Führungskräfte beim Datenumgang mehr Rechtssicherheit haben und Beschäftigte im Umgang mit Kundendaten jederzeit Unterstützung und Beratung anfordern können und erheblich sicherer werden.

Die Erkenntnis, dass ein vorbildlicher Datenschutz dabei hilft, Beschäftigte im Umgang mit Kundendaten zu stärken und Stress durch Ängste vor Datenschutz zu nehmen, ist für Betriebsräte bei der Bildungsplanung von besonderer Bedeutung. Sie können bei der Entwicklung und Durchführung von Datenschutzbildungsmaßnahmen, die vom betrieblichen Datenschutzbeauftragten organisiert werden, ihre Informations-, Beratungs- und Mitbestimmungsrechte bei der Bildungsplanung gemäß §§ 96–98 BetrVG nutzen.

Diese Erkenntnis ist zukünftig stärker als bisher auch auf Datenschutzschulungen für Betriebsräte zu übertragen, die viel stärker problemorientiert und lebendig zu gestalten wären, was leider nicht oft der Fall ist. Dann könnten auch wieder mehr junge Betriebsräte als Multiplikatoren für das sperrige Thema gewonnen werden. Betriebsräte für den Beschäftigtendatenschutz zu gewinnen, ist ein wichtiger Teil des notwendigen Kulturwandels zu einem vorbildlichen Beschäftigtendatenschutz. Im DB-Konzern werden mit vereinten Kräften erhebliche Anstrengungen unternommen, Betriebsräte im Beschäftigtendatenschutz zu schulen und sie zur Fachkraft für Datenschutz und Datensicherheit auszubilden. Der Arbeitgeber unterstützt diese Qualifizierungen. Die Ausbildung hat die Vertrauensperson beim Vorstand C (VbV) initiiert und intensiv begleitet. Durchgeführt und intensiv begleitet wurden die Veranstaltungen von der Bildungsgesellschaft TRANSMIT in Kooperation mit dem Sachverständigen des KBR und der Fachhochschule Frankfurt. In einem angefügten besonderen Modul zu den bahnspezifischen Regelun-

gen betreffend Datenschutz und Datensicherheit wirkten ebenfalls der Konzerndatenschutz und die IT-Sicherheitsorganisation mit.

Datenschutz lebt von Vertrauen, wie das Beispiel der Deutschen Bahn zeigt – gerade auch zwischen Mitgliedern der Abteilung Arbeitsrecht, Führungskräften, Datenschützern, Beschäftigten und Betriebsräten. Bislang wird in Unternehmen das Problem des Kulturwandels hin zu einem vorbildlichen Datenschutz noch viel zu wenig beachtet.

Die Überprüfung anhand von Audits, ob Datenschutzvorschriften wirklich beachtet und gelebt werden, sollte nicht so sehr als Kontrolle, sondern vielmehr als „Hilfe zur Selbsthilfe" durchgeführt werden, um gemeinsam Datenschutzlücken und Lösungen zu finden. Datenschutzstrukturen und -prozesse in Unternehmen sind viel stärker als bisher für Selbstdatenschutz nutzbar zu machen, unter anderem auch durch Voreinstellungen in Technik und Technikdesign. So kann z. B. bei Mails und Dateien mit Beschäftigtendaten im DB-Konzern voreingestellt werden, dass diese sich zu einem bestimmten Zeitpunkt selbst löschen. Darüber entscheidet dann der Beschäftigte als Nutzer.

Grundsatz der Verhältnismäßigkeit

Datenschützer und Betriebsräte sollten verstärkt dazu übergehen, bei der Einführung und Anwendung von technischen Kontrollsystemen und personenbezogenen Dateien einschließlich Datenbanken den Grundsatz der Verhältnismäßigkeit anzuwenden und zu überprüfen (vgl. Kock/Francke 2009, S. 648 f.; Brink/Wybitul 2014). Hierauf weist ausdrücklich die KBV BDS in § 18 Abs. 1 Satz 1 hin.

Eine datenschutzrechtliche Abwägung zwischen den Interessen der Arbeitgeber und der Beschäftigten als Grundrechtsträger im Sinne einer Verhältnismäßigkeitsprüfung (vgl. Düwell 2012; BAG v. 9.7.2013, 1 ABR 2/13 (A)) hat bei jeder Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten voranzugehen. Die datenschutzrechtliche Verhältnismäßigkeitsprüfung ist durch die Rechtsprechung in drei Schritte untergliedert worden, insbesondere durch das BAG in der Rechtsprechung zur Videoüberwachung (BAG, Beschl. v. 29.6.2004 – 1 ABR 21/03; Beschl. v. 14.12.2004 – 1 ABR 34/03; Beschl. v. 26.8.2008 – 1 ABR 16/07; siehe auch BAG, Urteil vom 20.06.2013 – 2 AZR 546/12, BB 7/2014, S. 890, 892).

Es muss überprüft werden, ob die geplante Überwachungsmaßnahme *geeignet* ist, um ein berechtigtes Interesse der verantwortlichen Stelle zu verwirklichen, beziehungsweise, ob sie einen legitimen Zweck verfolgt. Anschließend ist zu prüfen, ob die vorgesehene Maßnahme *erforderlich* ist oder

ob es mildere Mittel, z. B. andere, weniger intensive Eingriffe in die Persönlichkeitsrechte des Betroffenen gibt. In einem dritten Schritt ist abschließend die *Angemessenheit* der Maßnahme zu überprüfen: die Verhältnismäßigkeit in einem engeren Sinn, das heißt, ob die schutzbedürftigen Interessen der betroffenen Beschäftigten am Ausschluss der Datenverwendung überwiegen (Wybitul/Pötters 2014, S. 437, 439).

Schlagkräftige dezentrale Datenschutzorganisation

Das Beispiel des DB-Konzerns verdeutlicht, dass gerade bei verbundenen Unternehmen Datenschutzstrukturen und -prozesse vor allem dezentral und nach Bedarf aufgebaut werden müssen. Dezentrale Fachkräfte und Vertrauenspersonen für den Datenschutz sind zu bestellen und zu unterstützen, müssen vor Ort auf die Einhaltung von Datenschutzvorschriften *hinwirken* und auf mögliche Datenschutzprobleme rechtzeitig aufmerksam machen. Sie haben keine Sanktionsmöglichkeiten (vgl. § 4g Abs. 1 Satz 1 BDSG).

Datenschutz muss effizient und wirksam den jeweiligen Konzerngesellschaften vor Ort bzw. den Geschäftsfeldern angepasst werden, weil es in den einzelnen Konzerngesellschaften unterschiedliche Fragestellungen, Arbeitsplätze und Datenschutzprobleme geben kann. Geschäftsfelder sind im konkreten Fall DB Bahn Fernverkehr, DB Bahn Regio, DB Bahn Vertrieb, DB Schenker Rail, DB Netze Fahrweg, DB Netze Personenbahnhöfe und DB Dienstleistungen. Bei der Deutschen Bahn gibt es auch Spartendatenausschüsse, die Verfahrensmeldungen auf Zulässigkeit überprüfen. Die Sparten des DB-Konzerns sind Personenverkehr, Transport und Logistik und Dienstleistungen.

Externe Datenschutzbeauftragte haben in der Regel das Problem, dass sie sich zu wenig in der jeweiligen Organisation auskennen. Da können Fachkräfte für den Datenschutz und Vertrauenspersonen für den Datenschutz die Lücken schließen und sich mit externen Datenschutzbeauftragten gut ergänzen. Sie sind stets auszubilden, in notwendigem Umfang freizustellen, mit ausreichenden Ressourcen zu unterstützen, intern bekanntzumachen und mit allen anderen Akteuren des Beschäftigtendatenschutzes angemessen zu vernetzen. In etlichen größeren Unternehmen gibt es, besonders wenn externe Datenschutzbeauftragte bestellt sind, dezentral zusätzliche Koordinatoren für den Datenschutz. Diese sind aber in der Regel nicht vor Kündigung geschützt und haben keinen Fortbildungsanspruch. Betroffene Mitarbeiter, die sich an den Koordinator wenden, sind dann nicht davor geschützt, in der verantwortlichen Stelle offenkundig zu werden.

Für eine effektive Datenschutzorganisation hat die Deutsche Bahn AG detaillierte Struktur- und Prozessvorgaben erstellt, die für Überlegungen in eigenen Unternehmen hilfreich sein können. Besonders wichtig erscheint dabei der Umstand, dass Compliance, Recht, Konzernsicherheit und Datenschutz zentral bei einem Vorstand zusammengeführt werden. Die Abteilung Datenschutz ist somit auf der Vorstandsebene gleichberechtigt angeordnet.

Richtlinien für Datenschutzstörfälle

Es bietet sich auf jeden Fall an, die Vorgaben des § 42a BDSG zu schwerwiegenden Datenabflüssen oder Datenpannen in einer innerbetrieblichen Richtlinie umzusetzen. Diese Vorgaben im BDSG werden in der zu erwartenden EU-Datenschutzgrundverordnung voraussichtlich noch verschärft. Aus Datenschutzstörfällen und -verstößen im Beschäftigtendatenschutz sollte die jeweilige Organisation lernen und sie möglichst zum Anlass nehmen, die Qualität des vorhandenen Datenschutzes in jedem Einzelfall kritisch zu überprüfen und zu verbessern. Geschieht ein Datenstörfall und wird dieser offenkundig, kann dies dazu genutzt werden, wieder im Unternehmen den Kulturwandel in Richtung eines aufmerksamen und vorbildlichen Datenschutzes zu thematisieren. Größere Datenschutzprobleme und -verstöße können für die Durchführung eines Audits genutzt und in Schulungsmaßnahmen aufgegriffen werden. In der Praxis gilt diese Vorschrift zu Datenschutzstörfällen seit 2009. Sie wurde aber noch selten innerbetrieblich umgesetzt und kommuniziert und ist zu wenig bei Interessenvertretungen bekannt.

Betriebsvereinbarungen zum Datenschutz mit der Aufsichtsbehörde von Beginn an abstimmen

Die Entwicklung von Betriebsvereinbarungen als andere vorrangige Rechtsvorschriften für den Datenschutz im Sinne von § 4 Abs. 1 BDSG sollte stets als Projekt konzipiert und möglichst in vertrauensvoller Zusammenarbeit gestaltet und durchgeführt werden. Dabei ist nicht zu vergessen, die jeweilige Aufsichtsbehörde für den Datenschutz hinzuziehen, die derartige Betriebsvereinbarungen gemäß § 38 i. V. m. §§ 4b, 4c BDSG prüfen kann. Die Beratung gemäß § 38 Abs. 1 Satz 2 BDSG durch die Datenschutzaufsichtsbehörde, die viel stärker als Beratungs- denn als Kontrollinstanz gesehen werden sollte, ist möglichst frühzeitig und kontinuierlich einzuholen.

Nachhaltiger Datenschutz erfordert Datenschutzaudits

Das Beispiel der Datenschutzaudits bei der Deutschen Bahn verdeutlicht, wie ein nachhaltiger und dauerhafter Datenschutz durch Audits zu erreichen ist.

Da ein Ausführungsgesetz zu § 9a BDSG fehlt, sind Datenschutzaudits nach wie vor zwar freiwillig, aber ein wichtiges Element der Selbstkontrolle. Sie dienen dazu, die Wirksamkeit von Datenschutzstrukturen und -prozessen zu überprüfen und den Grundsatz der kontinuierlichen Verbesserung auch im Datenschutz langfristig anzuwenden. Noch erfolgen solche Audits in der Praxis leider viel zu selten. Sie sind aus Sicht von Betriebsräten und Beschäftigten unerlässlich, weil sie unter anderem damit die Rollen und Berechtigungen im Soll- und Ist-Zustand überprüfen und somit wesentliche Datenschutzschwachstellen im Unternehmen aufdecken können. Mit Audits kann überprüft werden, ob und inwieweit Regelungen in einer Betriebsvereinbarung zu IT-Systemen eingehalten werden.

Betriebsräte sollten immer darauf drängen, derartige regelmäßige Audits, durchgeführt von Fachauditoren, in der Datenschutzorganisation ihres Unternehmens strukturell zu verankern und insbesondere in Betriebsvereinbarungen abzusichern. Checklisten für Audits gibt es in ausreichender Anzahl, unter anderem von den Datenschutzaufsichtsbehörden, die sie bei einer Prüfung zugrunde legen (Bussche/Voigt 2014, S. 1 ff.). Institutionalisierte Datenschutzaudits, auch zum Cloud Computing, gibt es beim Unabhängigen Landeszentrum für Datenschutz Schleswig Holstein.

Im DB-Konzern gibt es mit der CDA eine eigene Auditabteilung, die derartige Audits durchführt. Die Auditoren arbeiten mit einem Ampelsystem, wenn sie Empfehlungen am Ende des Audits aussprechen. Sie differenzieren nach kurzfristigen, mittel- und langfristigen Maßnahmen. Für Letztere sind stets Investitionen erforderlich und deshalb kurzfristig ohne Vorlaufzeit nicht zu realisieren. Die Farbe Rot zeigt an, was sofort abzustellen ist. Gelb ist eine Warnung, mittel- oder langfristig zu einem bestimmten Termin Abhilfe zu schaffen und Grün ist freie Fahrt im Datenschutz. Auch in anderen Unternehmen würde ein solches Vorgehen helfen, Datenschutzmaßnahmen nicht frühzeitig an Budgetzwängen, am Alltagsgeschäft oder anderen unvorhergesehenen Umständen scheitern zu lassen. Das setzt jedoch immer eine Überprüfung der vorgeschlagenen Maßnahmen zu dem jeweils gesetzten Termin voraus, ggf. auch ein Nachaudit.

Das Beispiel des DB-Konzerns zeigt: Die Audits sollten immer mit einem Bericht enden, der Verbesserungsvorschläge mit der Setzung von Fristen enthält und zu treffende Maßnahmen nach Dringlichkeit gewichtet. Diese Berichte sollten vom Arbeitgeber unbedingt den Betriebsräten für ihre Aufgabenerfüllung nach § 80 Abs. 1 Nr. 1 BetrVG und § 80 Abs. 2 BetrVG zur Verfügung gestellt werden. Betriebsräte sollten sich das Recht zugestehen lassen, derartige Auditberichte anzufordern.

Andere Unternehmen und Konzerne sollten das Prinzip der Selbstkontrolle durch Einrichtung eines dezentralen Datenschutzes verstärken und sich mit einer praxisgerechten Kombination von dezentralen und zentralen Datenschutz aufstellen. Hierzu gehören auch Datenschutzaudits durch eine zentrale Auditabteilung, Datenschutz- oder IT-Sicherheitsfunktionsträger oder durch die IT-Revision, die auch kleineren und mittleren Unternehmen dringend zur Nachahmung empfohlen werden kann. Kleinere Unternehmen können Beratungen durch externe Datenschutzbeauftragte, Wirtschaftsprüfer oder Aufsichtsbehörden für den Datenschutz in Anspruch nehmen.

In der Praxis ist es eher die Regel, dass der betriebliche Datenschutzbeauftragte erst dann einen Jahresbericht über seine Aktivitäten erstellt, wenn eine Kontrolle der Aufsichtsbehörde ansteht. Selbst wenn ein Datenschutzbericht der Geschäftsleitung vorliegt, wird dieser oft den Betriebsräten vorenthalten, auch entgegen § 80 Abs. 2 BetrVG. Das Beispiel der Deutschen Bahn zeigt, dass es anders geht: Um Transparenz und Vertrauen auf Seiten der Interessenvertretungen herzustellen, ist es unbedingt erforderlich, sämtliche Datenschutzdokumente wie z. B. Verfahrensverzeichnis, Vorabkontrolle und Vertrag zur Auftragsdatenverarbeitung nach § 11 BDSG den zuständigen Betriebsräten zugänglich zu machen.

In diesem Zusammenhang ist bei der Deutschen Bahn ein weiteres Instrument eingeführt, um Beschäftigtendatenschutz als kontinuierlichen Verbesserungsprozess in Bewegung bzw. dynamisch zu halten: Mit dezentralen Datenschutzfachkräften werden Zielvereinbarungen hinsichtlich des Datenschutzes getroffen und regelmäßig die Zielerreichung überprüft. Die fachliche Führung obliegt dem zentralen Konzerndatenschutz. Auch mit der Konzerndatenschutzbeauftragten oder der Abteilungsleiterin für den Beschäftigtendatenschutz wird eine solche Zielvereinbarung abgeschlossen. Die Ziele können sich z. B. auf die Anzahl der durchzuführenden Schulungen oder auf die zu bearbeitenden Themen im Datenschutz beziehen. Zumindest in Betriebs- und Dienstvereinbarungen, in Beratungen oder Seminaren mit Interessenvertretungen ist das Instrument der Zielvereinbarungen für den Datenschutz bislang relativ unbekannt.

Datenschutzmanagement ganzheitlich als Prozess gestalten

Die Deutsche Bahn AG will mit der KBV BDS und den anzupassenden alten und neuen Konzernvereinbarungen zu IT-Systemen, Dateien und Datenbanken mit Beschäftigtendaten vor allem Transparenz herstellen und Nachhaltigkeit sichern. Das erfordert eine Standardisierung der Datenschutzprozesse – hier setzt der DB-Konzern auf Musterverträge, Musterverfahrensverzeich-

nisse, Checklisten, Datenübersichten und Ähnliches mehr. Hier können andere Unternehmen durchaus solche Muster übernehmen und an ihre Bedingungen anpassen. Gute und brauchbare Muster gibt es genügend. Es käme darauf an, sie tatsächlich zu nutzen und immer wieder der Wirklichkeit des Datenschutzes anzupassen – das Rad muss nicht immer wieder neu erfunden werden.

In der Prozessgestaltung sollte die Phase der Evaluation des Datenschutzniveaus nicht vernachlässigt werden. Ebenso wie die Wirksamkeitskontrolle im Arbeitsschutzrecht, z. B. bei der Durchführung der Gefährdungsbeurteilung gemäß § 5 ArbSchG, ist das Datenschutzaudit ein geeignetes Instrument für die Evaluation von Strukturen, Prozessen und Ergebnissen. Audits zum Beschäftigtendatenschutz sollten viel mehr von den Betriebsparteien genutzt werden, um Datenschutzlücken, -defizite und -verstöße zu identifizieren und abzustellen (Kiesche/Wilke 2013; Probst 2015, S. 38 ff.) und vor allem darüber ins Gespräch zu kommen.

7 RECHTLICHE GRUNDLAGEN

Der Betriebsrat hat nach §80 Abs. 1 Nr. 1 BetrVG die Aufgabe, die Einhaltung des Bundesdatenschutzgesetzes zu überwachen, wie das Bundesarbeitsgericht wiederholt festgestellt hat. Er ist neben dem betrieblichen Datenschutzbeauftragten, dessen Stellung und Aufgaben in §§4f und 4g BDSG geregelt sind, der Hüter des Beschäftigtendatenschutzes. Aus der Rechtsüberwachungsfunktion folgt ein Anspruch des Betriebsrats, rechtzeitig und vollständig über die Einführung und Änderung von IT-Systemen, Dateien und Datenbanken mit Beschäftigtendaten unterrichtet zu werden. Die rechtzeitige Unterrichtung bedeutet, dass Information und Beratung bereits mit Beginn der Planungsphase und zu einem Zeitpunkt erfolgen müssen, dass vorgeschlagene Gestaltungsalternativen des Betriebsrats noch ohne unzumutbaren Aufwand realisierbar sind. Für seine Überwachungsfunktion im Datenschutz benötigt der Betriebsrat z. B. folgende Unterlagen:

- Schnittstellenverzeichnis (mit ein- und ausgehenden Datensätzen)
- Positivkataloge der verarbeiteten Daten und Auswertungen
- Zweckbestimmung der möglichen Erfassung, Verarbeitung und Nutzung der Daten
- betroffene Personengruppen
- zugriffsberechtigte Personen
- Empfänger der Daten
- konkrete Regelfristen für die Löschung der Daten und Beschreibung der nach §9 BDSG getroffenen Maßnahmen.

Im Datenschutz muss die verantwortliche Stelle ein Verfahrensverzeichnis nach §§4e und g BDSG erstellen, das vom betrieblichen Datenschutzbeauftragten geführt wird. Nach §80 Abs. 2 BetrVG hat der Betriebsrat auf diese Dokumentation einen Anspruch, ebenso auf Unterlagen zu einer Zulässigkeitsprüfung oder einer Vorabkontrolle nach §4d Abs. 5 und 6 BDSG. Bei der Deutschen Bahn AG spielt ebenfalls der Vertrag zur Auftragsdatenverarbeitung eine wichtige Rolle. Hier liegt ebenfalls ein Informationsanspruch vor, da die Unterlage für die Aufgabe der Rechtsüberwachungsfunktion im Datenschutzrecht erforderlich ist. Zu den Unterlagen gemäß §80 Abs. 2 BetrVG gehören auch Auditberichte, Tätigkeitsberichte der Datenschutzbeauftragten, die Dokumentation des Verdachts auf Begehung einer Straftat im Beschäftigungsverhältnis nach §32 Abs. 1 Satz 2 BDSG und die Zugriffsberechtigungen.

Zur Rechtsüberwachungsfunktion tritt eine Rechtssetzungsfunktion als Mitbestimmungs- und Initiativrecht hinzu, wenn technische Einrichtungen eingeführt oder geändert werden, die für eine Leistungs- und Verhaltenskontrolle objektiv geeignet sind (§ 87 Abs. 1 Nr. 6 BetrVG). Ein datenverarbeitendes System ist zur Überwachung bestimmt, wenn es individualisierte oder individualisierbare Verhaltens- oder Leistungsdaten selbst erhebt oder aufzeichnet. Hierfür liegt langjährige Rechtsprechung des BAG vor (z. B. Beschluss v. 25.9.2012 - 1 ABR 45/11, BB 2013, S. 699–701). Auch § 32 Abs. 3 BDSG verweist ausdrücklich darauf, dass die Rechte der Interessenvertretungen von den Vorgaben des BDSG zum Beschäftigtendatenschutz unberührt bleiben. Diese Vorschrift hat eine wichtige Klarstellungsfunktion, die in der Praxis oft benötigt wird, um die Mitgestaltung des Beschäftigtendatenschutzes durch die Interessenvertretung durchsetzen zu können.

Die Mitbestimmung bei der Einführung und Änderung von technischen Kontrolleinrichtungen nach § 87 Abs. 1 Nr. 6 BetrVG bezieht sich auf automatisierte Verfahren der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten, so z. B. auf ein Personalverwaltungssystem, ein Zeiterfassungssystem oder eine digitale Personalakte. Schaltet der Arbeitgeber Externe für die Datenverarbeitung ein, schließt dies das Mitbestimmungsrecht des Betriebsrats nicht aus. Der Arbeitgeber muss durch entsprechende Vertragsgestaltung sicherstellen, dass der Betriebsrat seine Mitbestimmungsrechte uneingeschränkt wahrnehmen kann (Kock/Francke 2009, S. 651).

Seit 2009 gelten die Vorschriften des BDSG zum Beschäftigtendatenschutz auch für die nichtautomatisierte Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten, z. B. in Personalakten. Der Betriebsrat kann überwachen, ob die Vorschriften zum Datenschutz auch bei nichtautomatisierter Verarbeitung eingehalten werden. Bei allen Verfahren ist auch zu überprüfen, ob das Ordnungsverhalten der Beschäftigten betroffen ist, so z. B. bei der Einführung und Anwendung der IT-gestützten Zeiterfassung.

Eine zweite Möglichkeit des Betriebsrats, die abstrakten Bestimmungen des BDSG zu konkretisieren und an die Verhältnisse im Betrieb, im Unternehmen oder im Konzern anzupassen, ergibt sich aus § 4 Abs. 1 BDSG in Verbindung mit der Rechtsprechung des BAG. § 4 Abs. 1 BDSG stellt den Grund-Satz auf, dass eine Verarbeitung personenbezogener Daten von Betroffenen grundsätzlich verboten ist, es sei denn, eine Einwilligung der bzw. des Betroffenen oder eine andere Rechtsvorschrift erlaubt die Datenverwendung. Zu den anderen Rechtsvorschriften gehören auch Tarifverträge und Betriebs- bzw. Dienstvereinbarungen. Eine Betriebsvereinbarung, die IT-Verfahren und die dazugehörige Datenverarbeitung regelt, darf jedoch nicht zu Un-

gunsten der Beschäftigten vom BDSG-Standard abweichen (Kiesche/Wilke 2012, S. 10; Kiesche/Wilke 2014b) und muss sich im Rahmen des Persönlichkeitsschutzes (§ 75 Abs. 2 BetrVG und Art. 1, 2 GG) bewegen. In der Praxis finden sich oft Rahmenbetriebsvereinbarungen. Grundsätzlich ist eine Rahmenbetriebsvereinbarung über den Einsatz von IT-Systemen oder den Beschäftigtendatenschutz nur auf freiwilliger Grundlage möglich (Däubler 2013, Rdnr. 304 f.).

Im Zusammenhang mit der Regelung von automatisierten Datenverarbeitungsverfahren stellt sich die Frage nach der Zuständigkeit der Betriebsratsgremien, das heißt: Inwieweit hat der örtliche Betriebsrat, der Gesamtbetriebsrat oder der Konzernbetriebsrat die Regelungsbefugnis? Für die Zuständigkeit der Betriebsratsgremien auf der Betriebs-, Unternehmens- oder Konzernebene gemäß § 50 und § 58 BetrVG ist entscheidend, dass die zwingende Notwendigkeit besteht, die Einführung der Technik unternehmensüberschreitend oder konzernweit zu regeln. Diese zwingende Erforderlichkeit ergibt sich dadurch, dass das IT-System nicht auf den einzelnen Betrieb oder auf das Unternehmen beschränkt ist und deshalb die Interessen der Arbeitnehmer nicht mehr auf der betrieblichen Ebene bzw. der des Unternehmens gewahrt werden können.

Der Konzernbetriebsrat ist nur zuständig, wenn weder Gesamtbetriebsrat noch Betriebsrat zuständig sind. Es ist zu unterscheiden, ob die Zuständigkeit aufgrund einer Beauftragung zustande kommt oder originär. Die originäre Zuständigkeit des Konzernbetriebsrats ergibt sich, wenn die Einführung von IT-Verfahren mehrere Unternehmen betrifft und es zum anderen objektiv „ein zwingendes Erfordernis“ für eine unternehmensübergreifende Regelung gibt. Maßgeblich sind stets die konkreten Umstände im Konzern und in den einzelnen Unternehmen. Das heißt: Die Zuständigkeit des KBR ist in jedem Einzelfall zu prüfen. Die zwingende Erfordernis für eine unternehmensweite Regelung und damit für die Zuständigkeit des KBR ergibt sich unter anderem aus technischen Gründen, z. B. bei der Einführung von SAP ERP zentral bei einer Konzerntochter oder bei einem Ethik- bzw. Verhaltenskodex (BAG v. 25.9.2012 – 1 ABR 45/11, in: RDV 2013, S. 157; ausführlich Besgen/Apelt 2013, S. 74–78; Kock/Francke 2009, S. 649–650; Trittin/Fischer 2009, S. 343).

LITERATUR- UND INTERNETVERZEICHNIS

Besgen, Nicolai/Apelt, Daniel (2013): Die Zuständigkeit des Konzernbetriebsrats für Konzern(rahmen)betriebsvereinbarungen, in: Sammlung arbeitsrechtlicher Entscheidungen, Heft 4/2013, S. 74–78.

Brink/Stefan/Wybitul, Tim: Der „neue Datenschutz" des BAG – Vorgaben zum Umgang mit Beschäftigtendaten und Handlungsempfehlungen zur Umsetzung, in: Zeitschrift für Datenschutz 2014, S. 225.

Busche, Axel Frhr. von dem/Voigt, Paul (2014): Konzerndatenschutz. Rechtshandbuch. München

Däubler, Wolfgang (2013): Internet und Arbeitsrecht. 4. Aufl., Frankfurt am Main.

Däubler, Wolfgang (2015): Gläserne Belegschaften? Das Handbuch zum Arbeitnehmerdatenschutz, 6. Aufl., Frankfurt am Main.

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo (2014): Bundesdatenschutzgesetz, 4. Aufl., Frankfurt am Main.

Dix, Alexander (2009): Bericht des Berliner Beauftragten für den Datenschutz und Informationsfreiheit 2009, S. 118–119. Download unter: http://www.thm.de/zaftda/tb-bfdi/cat_view/25-tb-bundeslaender/8-berlin

Dix, Alexander (2013): Aufsichtsbehörden und die Kontrolle der Konzernunternehmen, unveröffentlichter Vortrag, Berlin.

Düwell, Franz Josef (2012): Verhältnismäßigkeitsgrundsatz und Kontrolle, unveröffentlichtes Manuskript, Weimar.

Fritz, Michael (2012): Beschäftigtendatenschutz im Konzern Deutsche Bahn aus arbeitsrechtlicher Sicht, in: Zeitschrift für Arbeitsrecht, S. 197–208.

Gola, Peter (2013): Datenschutz Jahrbuch 2014, Heidelberg u. a.

Gola, Peter/Wronka, Georg (2013): Handbuch Arbeitnehmerdatenschutz, 6. Aufl., Heidelberg u. a.

Gola, Peter/Jaspers, Andreas (2011): Das Bundesdatenschutzgesetz im Überblick, 6. Aufl., Heidelberg u. a.

Hallermann, Ulrich (2013): Der „Teilzeit-Datenschutzbeauftragte" und das Verfahrensverzeichnis: Praxistipps für eine schlanke Umsetzung der BDSG-Vorgaben, in: Recht der Datenverarbeitung Heft 4/2013, S. 173–178.

Kiesche, Eberhard/Wilke, Matthias (2015): IT-Outsourcing mit Hindernissen. Leitfaden zur Auftragsdatenverarbeitung in: Computer und Arbeit, Heft 5/2015, S. 21–24.

Kiesche, Eberhard/Wilke, Matthias (2014a): Anti-Fraud-Management. Kriminalität bekämpfen mit Mitbestimmung und Datenschutz, in: Computer und Arbeit, Heft 1/2014, S. 4–10.

Kiesche, Eberhard/Wilke, Matthias (2014b): Vereinbarungen zum Schutz von Beschäftigtendaten, in: Computer und Arbeit, Heft 6/2014, S. 26-30.

Kiesche, Eberhard/Wilke, Matthias (2013): Audit des internen Datenschutzmanagements. Beschäftigtendatenschutz auf dem Prüfstand, in: Computer und Arbeit, Heft 5/2013, S. 26–32.

Kiesche, Eberhard/Wilke, Matthias (2012): Neue Überwachungsformen in Call-Centern, in: Computer und Arbeit, Heft 4/2012, S. 5–12.

Kiesche, Eberhard/Wilke, Matthias (2011): Das Verfahrensverzeichnis. Freie Sicht auf die Datenverarbeitung, in: Computer und Arbeit, Heft 10/2011, S. 27–33.

Kock, Martin/Francke, Julia (2009): Mitarbeiterkontrolle durch systematischen Datenabgleich zur Korruptionsbekämpfung, in: Neue Zeitschrift für das Arbeitsrecht, Heft 12/2009, S. 646–651.

Lepperhoff, Niels/Jaspers, Andreas (2013): Neuer Datenschutzstandard DS-BvD-GDD-01, in: MultiMedia und Recht, Heft 10/2013, S. 617 f.

Mähner, Nicolas (2010): Neuregelung des § 32 BDSG zur Nutzung von personenbezogener

Mitarbeiterdaten. Am Beispiel der Deutschen Bahn AG, in: MultiMedia und Recht, Heft 13/2010, S. 379–382.

Müller-Glöge, Rudi/Preis, Ulrich/Schmidt, Ingrid (2012): Erfurter Kommentar zum Arbeitsrecht, 12. Aufl., München.

Newiger, Chris (2012): Datenflüsse im Konzern am Beispiel Deutsche Bahn AG. Unveröffentlichter Vortrag bei der GDD am 22.11.2012 in Köln.

Probst, Thomas (2015): Datenschutzaudits, in: Stoppkotte, Eva-Maria/Wilke, Matthias (Hrsg.), Big Data im Betrieb, S. 38–46.

Simitis, Spiros (Hg.) (2014): Bundesdatenschutzgesetz, 8. Aufl., Baden-Baden.

Steinkühler, Bernd (2009): Kein Datenproblem bei der Deutschen Bahn AG? Mitnichten, in: Betriebs-Berater, Heft 24/2009, 1294 f.

Trittin, Wolfgang/Fischer, Esther (2009): Datenschutz und Mitbestimmung. Konzernweite Personaldatenverarbeitung und die Zuständigkeit der Arbeitnehmervertretung, in: Neue Zeitschrift für das Arbeitsrecht, Heft 7/2009, S. 343.

Vogt, Volker (2014): Datenübertragung innerhalb und außerhalb des Konzerns, in: Betriebs-Berater, Heft 5/2014, S. 245–249.

Wilke, Matthias, Kiesche, Eberhard (2015): Aus Erfahrung klug werden, in: Stoppkotte, Eva-Maria/Wilke, Matthias (Hrsg.), Big Data im Betrieb, S. 42–46

Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.) (2013): Datenschutzrecht in Bund und Ländern, München.

Wybitul, Tim (2009): Das neue Bundesdatenschutzgesetz: Verschärfte Regeln für Compliance und interne Ermittlungen, in: Betriebs-Berater, Heft 30/2009, S. 1582–1584.
Wybitul, Tim (2011): Handbuch Datenschutz im Unternehmen, Frankfurt am Main.

Wybitul, Tim/Pötters, Stephan (2014): BAG definiert Beschäftigtendatenschutz neu, in: Betriebs-Berater, Heft 8/2014, S. 437.

Wybitul, Tim (2014): Neue Spielregeln bei Betriebsvereinbarungen und Datenschutz, in: Neue Zeitschrift für Arbeitsrecht Heft 5/2014, S. 226–231.

ULD/Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein (Hg.) (2010): Private sowie dienstliche Internet- und E-Mail-Nutzung, pdf, Download unter: https://www.datenschutzzentrum.de/internet/private-und-dienstliche-internetnutzung.pdf.

DB-Konzern-Dokumente und -Links

DB-Konzern (2011): Konzernbetriebsvereinbarung Beschäftigtendatenschutz im DB Konzern (KBV BDS), Berlin/Frankfurt, Download unter: http://www.evg-online.org/Arbeitswelt/Mitbestimmung/Betriebsverfassung

DB-Konzern (2011): Rahmen-Konzernbetriebsvereinbarung über Einführung und Betrieb von Verfahren zur Verarbeitung personenbezogener Beschäftigtendaten im DB Konzern (RKBV-Beschäftigten-DV), Berlin/Frankfurt, unveröffentlicht.

DB-Konzern (2012): Konzernbetriebsvereinbarung zum Einsatz, zur Nutzung und zur Zulässigkeit von Auswertungen bei BKU (Internet und E-Mail) im DB Konzern (KBV IT), Berlin/Frankfurt, unveröffentlicht.

DB-Konzern (2013): Konzernbetriebsvereinbarung Konzerninterne Datenflüsse im DB Konzern (KBV KID), Berlin/Frankfurt, Download unter: http://www.evg-online.org/Arbeitswelt/Mitbestimmung/Betriebsverfassung.

DB-Konzern (2013): Konzernbetriebsvereinbarung Hinweismanagement (KBV Hinweismanagement), Berlin/Frankfurt (unveröffentlicht).

DB-Konzern (2014a): Der Vorstand der Deutschen Bahn AG, Download unter: http://www.deutschebahn.com/de/konzern/konzernprofil/vorstand.

DB-Konzern (2014b): Mitarbeiter in Zahlen, Download unter: http://www.deutschebahn.com/de/konzern/konzernprofil/zahlen_fakten/mitarbeiter.html.

ANHANG

A) Aufgaben der Fachkräfte für Datenschutz (FDS)

- Koordinierung von Datenschutzangelegenheiten
- Beratung der Geschäftsleitung in Datenschutzangelegenheiten, ggf. in Abstimmung mit dem Konzerndatenschutz
- Zusammenarbeit mit der Konzerndatenschutzbeauftragten (KDSB/DSB) und Mitwirkung bei der Erfüllung ihrer Aufgaben
- Mitwirken im Jour Fixe Datenschutz (JFD)
- Leitung der „Datenausschüsse“ in den zugeordneten Konzernunternehmen unter Mitwirkung der Vertrauenspersonen für den Datenschutz (VPDS) in den „verantwortlichen Stellen“; ggf. Delegation an die VPDS.
- Information an die KDSB/DSB über Vorhaben der automatisierten Verarbeitung personenbezogener Daten
- Veranlassen der Beteiligung des Konzerndatenschutzes/DSB bei erforderlichen Vorabkontrollen
- Veranlassen der Beteiligung des Konzerndatenausschusses unter Leitung der KDSB bei beabsichtigter Inbetriebnahme konzernübergreifender Verfahren mit der Verarbeitung von Mitarbeiterdaten
- Mitwirkung in Fachgremien für den Datenschutz
- Prüfung von Verfahrensmeldungen
- Veranlassen der Genehmigung für datenschutzrelevante Verfahren durch die Unternehmensleitung bzw. bei Verarbeitung von Mitarbeiterdaten durch den Personalleiter
- Abstimmen von Verfahrensmeldungen und Änderungsmeldungen mit der/dem KDSB zu automatisierten Verarbeitungen mit personenbezogenen Daten, die einer Vorabkontrolle bedürfen oder unternehmensübergreifenden Charakter haben
- Sicherstellen der Erstellung und Pflege von dezentralen Verfahrensverzeichnissen bei den verantwortlichen Stellen, Sicherstellen der Übermittlung von Verfahrensverzeichnissen an den Konzerndatenschutz
- Mitwirken bei der Durchführung von Einzelkontrollen durch den Konzerndatenschutz
- Mitwirkung bei der Schutzbedarfsfeststellungen für DV-Verfahren
- Überwachen der Beteiligung der Interessensvertretung bei der Einführung und wesentlichen Veränderung von automatisierten Verarbeitungen, die der Verarbeitung von Beschäftigtendaten dienen

- Veranlassen und Durchführen von Audits und Kontrollen
- Sicherstellen der Unterrichtung der KDSB/DSB bei Hinweisen auf Verdachtsfälle oder tatsächliche Datenschutzverstöße
- Veranlassen und Mitwirken bei Schulung und Fortbildung der mit der Verarbeitung personenbezogener Daten betrauten Personen sowie bei der Präventionsarbeit
- Abstimmen der Bearbeitung und Beantwortung von Anfragen der Aufsichtsbehörden mit der KDSB
- Melden von Verdachtsfällen oder tatsächlichen Datenschutzverstößen an die KDSB

B) Anlage 1 der KBV BDS

Begriffsbestimmungen
Soweit in dieser Anlage nicht definiert, gelten die Begriffsbestimmungen des BDSG in der am 1.9.2009 in Kraft getretenen Fassung.

(1) *Personenbezogene Daten* sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Dazu zählen auch
  - Angaben, die Rückschlüsse auf bestimmte natürliche Personen oder ihre privaten/dienstlichen Verhältnisse zulassen wie z. B. Alter, Anschrift, dienstliche oder private E-Mail-Adresse, Telefonnummer von Einzelpersonen, Angaben über deren familiären Hintergrund, Solvenz, Lohnpfändungen, Nebenbeschäftigungen, Kontobewegungen, Grund- oder Kfz-Besitz usw. sowie
  - sog. Verkehrsdaten wie z. B. Einzelverbindungsnachweise, Logfiles, Daten auf Proxyservern, User-ID usw.

(2) *Besondere Arten* personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

(3) *Erheben* ist das Beschaffen von Daten über den Betroffenen.

(4) *Verarbeiten* ist das Speichern, Verändern, Übermitteln, Sperren und Löschen von Daten. Im Einzelnen ist
  - *Speichern* das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung.

- *Verändern* das inhaltliche Umgestalten gespeicherter personenbezogener Daten.
- *Übermitteln* das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
  - die Daten an den Dritten weitergegeben werden oder
  - der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft.

(5) *Nutzen* ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(6) *Verwendung* ist jede Erhebung, Verarbeitung und Nutzung von Daten.

(7) *Verantwortliche Stelle* ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

(8) *Dritter* ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten für die verantwortliche Stelle im Auftrag erheben, verarbeiten oder nutzen.

(9) *Auftragsdatenverarbeitung* umfasst die Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Bei der Auftragsdatenverarbeitung wird nicht die Aufgabe selbst, zu deren Zweck die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten erfolgt, ausgelagert, sondern lediglich der zur Aufgabenerledigung erforderliche Umgang mit den Daten. Der in Anspruch genommenen Serviceeinrichtung wird der Umgang mit den Daten nach Weisung und unter materieller Verantwortung des Auftraggebers übertragen. Die datenschutzrechtliche Verantwortung für die Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten verbleibt beim Auftraggeber. Dieser verantwortet auch die technischen und organisatorischen Maßnahmen. Erkennungsmerkmale für Auftragsdatenverarbeitung sind:

- fehlende Entscheidungsbefugnis des Auftragnehmers,
- Weisungsgebundenheit des Auftragnehmers bezüglich dessen, was mit den Daten geschieht,
- Umgang nur mit personenbezogenen Daten, die der Auftraggeber zur Verfügung stellt; es sei denn, der Auftrag ist auch auf die Erhebung von Daten gerichtet,

- Ausschluss der Verarbeitung oder Nutzung der Daten zu eigenen Zwecken des Auftragnehmers,
  - keine (vertragliche) Beziehung des Auftragnehmers zum Betroffenen,
  - Auftragnehmer tritt (gegenüber dem Betroffenen) nicht in eigenem Namen auf.

(10) *Funktionsübertragung*: Bei der Funktionsübertragung wird auch die der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zugrunde liegende Aufgabe ganz oder teilweise abgegeben. Die in Anspruch genommene Serviceeinrichtung erbringt – über die technische Durchführung des Umgangs mit personenbezogenen Daten hinaus – materielle Leistungen mit Hilfe der überlassenen Daten. Sie handelt hierbei eigenverantwortlich. Erkennungsmerkmale für Funktionsübertragung:

- Weisungsfreiheit des Dienstleisters bezüglich dessen, was mit den Daten geschieht
- Überlassung von Nutzungsrechten an den Daten
- eigenverantwortliche Sicherstellung von Zulässigkeit und Richtigkeit der Daten durch den Dienstleister, einschließlich des Sicherstellens der Rechte von Betroffenen (Benachrichtigungspflicht, Auskunftsanspruch)
- Handeln des Dienstleisters (gegenüber dem Betroffenen) im eigenen Namen
- Entscheidungsbefugnis des Dienstleisters in der Sache.

(11) *Administratoren* sind Personen, welche die informationstechnische Infrastruktur des Unternehmens auf der Basis von umfassenden Zugriffsrechten auf das System verwalten (z. B. planen, installieren, konfigurieren und pflegen) oder Zugriffe auf Daten verwalten oder durchführen.

(12) *Vorratsdatenverarbeitung* im Sinne dieser Vereinbarung liegt vor, wenn personenbezogene Daten ohne abschließende Festlegung von Ziel und Zweck erhoben, verarbeitet oder genutzt werden.

(13) *Nebendatenverarbeitung* ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten außerhalb von führenden und kollektivrechtlich geregelten Systemen.

(14) *Automatisierte Verarbeitung* ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. (Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.)

(15) *Sperren* ist das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken.
(16) *Löschen* ist das Unkenntlichmachen gespeicherter personenbezogener Daten, um deren weitere Verwendung auszuschließen.
(17) *Anonymisieren* ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft jeweils einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.
(18) *Pseudonymisieren* ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.
(19) *Verfahren* ist eine Verarbeitung von Daten oder ein Bündel von Datenverarbeitungen, die über eine von der verantwortlichen Stelle definierte Zweckbestimmung verbunden sind.

ÜBER DIE SAMMLUNG VON BETRIEBSVEREINBARUNGEN

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

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

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

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

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

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