Datenschutz im Personalratsbüro

1. Einleitung

Die Verarbeitung personenbezogener Daten der Beschäftigten durch den Arbeitgeber wird seit Jahren in den Behörden und Unternehmen diskutiert. So ist es gängige Praxis, dass die Datenverarbeitung im Rahmen von Dienst-/Betriebsvereinbarungen geregelt wird. Die Diskussion um die Datenverarbeitung und den Datenschutz bei der Interessenvertretung selbst führt sowohl in der betrieblichen Praxis als auch in der Fachliteratur eher ein „Schattendasein".

Diskussionen in Fachkreisen hat es vor allem um die Frage der Zulässigkeit der Kontrolle des Betriebsrats durch den betrieblichen Datenschutzbeauftragten (bDSB) gegeben. In der Praxis spielt Datenschutz in Bezug auf den Personalrat häufig nur dann eine Rolle, wenn der Arbeitgeber dem Personalrat ihm zustehende Informationen mit dem Hinweis auf den Datenschutzes verweigern will. Vor diesem Hintergrund soll nachfolgend das Thema „Datenschutz im Personalratsbüro" dargestellt werden[1)].

2. Verarbeitung von Beschäftigten-Daten

Mit der verstärkten Einführung und Anwendung von Informations- und Kommunikationstechniken (IuK) in den Behörden erfolgt eine Zunahme an automatisierter Verarbeitung personenbezogener Daten der Beschäftigten. Denn gerade mit der zunehmenden Vernetzung ist der einzelne in seinem Arbeits- und Kommunikationsverhalten weitgehend kontrollierbar geworden, schon allein dadurch, dass die Systemadministratoren alles, was über das behördeninterne Netz läuft, mitlesen können. In diesem Sinne hat jede Email „Postkarten-Charakter". Mit der technischen Entwicklung und der technischen Ausstattung der Behörden muss auch der Datenschutz – im Sinne von **Schutz der Persönlichkeitsrechte** – an Gewicht gewinnen.

Um den Datenschutz bei der Verarbeitung von Beschäftigtendaten zu wahren, existieren im Personalvertretungsrecht Beteiligungsrechte des Personalsrat in Form von Informations-, Überwachungs- und Mitbestimmungsrechten. Zur zentralen Norm hat sich hier der § 75 Abs. 3 Nr. 17 BPersVG (bzw. die entsprechenden Vorschriften der Landespersonalvertretungsgesetze) herauskristallisiert. Dieses Mitbestimmungsrecht dient in erster Linie dem Schutz der Persönlichkeitsrechte des einzelnen Beschäftigten gegen technische Kontrolleinrichtungen, da diese Kontrolleinrichtungen stark in die Persönlichkeitsrechte eingreifen. So unterliegen technische Einrichtungen, die es ermöglichen, Leistung oder Verhalten der Beschäftigten zu überwachen, der Mitbestimmung der Interessenvertretung. Bei der Erhebung von Daten kann der Schutz der Persönlichkeitsrechte durch das Mitbestimmungsrecht nach § 75 Abs. 3 Nr. 8 BPersVG gesichert werden. Zudem hat der Personalrat nach § 68 Abs. 1 Nr. 2 BPersVG die Einhaltung des Bundesdatenschutzgesetzes (BDSG) zu überwachen.

Der Schutz der Persönlichkeitsrechte wird in der Regel über den Abschluss von **Dienstvereinbarungen** gewährleistet, wobei die Vorgaben des BDSG zu beachten sind[2)]. Im Rahmen entsprechender Regelungen sollen u. a. in Bezug auf den Schutz der Persönlichkeitsrechte folgende Ziele erreicht werden:

- Schaffung von Transparenz über die Verarbeitung personenbezogener Daten der Beschäftigen,
- Verarbeitung und Auswertung von personenbezogenen Daten im Rahmen einer engen Zweckbindung und Zweckbestimmung bezogen auf das Arbeitsvertragsverhältnis,
- Festlegung der zugriffsberechtigten Personen,
- Vereinbarung von Löschungsfristen,
- Ausgestaltung der Rechte der Beschäftigten auf Benachrichtigung, Auskunft, Berichtigung, Löschung und Sperrung,
- Vereinbarung der Kontrollrechte des Personalrats.

Diese kurze Darstellung zeigt, dass die automatisierte Verarbeitung personenbezogener Daten der Beschäftigten durch den Arbeitgeber in den Behörden mit Hilfe der Mitbestimmungsrechte im

1) Der Artikel basiert auf einem Vortrag des Autors auf dem AiB-Kongress „Elektronische Kommunikation und Datenschutz" am 19.9.02 in Potsdam.

2) Die Arbeitgeber im öffentlichen Bereich sträuben sich sehr oft, mit dem Personalrat Dienstvereinbarungen abzuschließen. Dieses ist unverständlich, denn entsprechende Dienstvereinbarungen setzen als andere Rechtsvorschriften den Datenschutz in ihrem Regelungsbereich um und schaffen für die Dienststelle, die Vorgesetzten und auch für die Beschäftigten Rechtssicherheit.

Rahmen von Dienstvereinbarungen geregelt werden kann.

Wie in den Dienststellen in allen Bereichen/Abteilungen die Datenverarbeitung zunimmt, ist auch die Arbeit von Personalräten ohne den Einsatz von IuK-Techniken gerade in größeren Dienststellen kaum noch vorstellbar. So nutzen Personalräte nicht nur einzelstehende PCs und moderne Telefone, sondern in größeren Gremien auch ein eigenes Netzwerk. Zudem können Personalräte auf das **behördeninterne Intranet** und auch auf das **Internet** mit den Funktionen Datenübertragung (File-Transfer) und E-Mail zugreifen. Dass die Interessenvertretung diese modernen Medien vom Arbeitgeber zur Verfügung gestellt bekommen, ist mit der Novellierung des BetrVG besonders hervorgehoben worden. In § 40 Abs. 2 BetrVG heißt es: „Für die Sitzungen, die Sprechstunden und die laufende Geschäftsführung hat der Arbeitgeber in erforderlichem Umfang Räume, sachliche Mittel, Informations- und Kommunikationstechnik sowie Büropersonal zur Verfügung zu stellen." Auch wenn es im BPersVG diese Regelung nicht gibt, gehören moderne Informations- und Kommunikationstechniken zu dem „erforderlichen Geschäftsbedarf" des Personalrats im Sinne des § 44 Abs. 2 BPersVG.

Mit der zunehmenden Nutzung von IuK-Techniken und der damit verbundenen Verarbeitung personenbezogener Daten gewinnt **Datenschutz im Personalratsbüro** an Bedeutung. Man kann jedoch den Eindruck gewinnen, dass die Verarbeitung personenbezogener Daten der Beschäftigten, die durch den Arbeitgeber erfolgt, seit Jahren diskutiert und durch Dienstvereinbarungen geregelt wird, wohingegen die Verarbeitung personenbezogener Daten der Beschäftigten durch die Interessenvertretung eher „am Rande" diskutiert wird. Es ist aber unstrittig, dass auch im Rahmen der Personalratsarbeit – also auch im Personalratsbüro – das BDSG zwingend einzuhalten ist[3].

3. Weiterleitung personenbezogener Daten an den Personalrat

Da die personenbezogenen Daten der Beschäftigten, die vom Personalrat verarbeitet bzw. genutzt werden, in erste Linie vom Arbeitgeber kommen, soll nachfolgend die rechtliche Grundlage für die Weitergabe der Daten geklärt werden. Denn häufig wollen Arbeitgeber der Interessenvertretung Informationen verwehren und weisen darauf hin, dass die Weitergabe personenbezogener Daten an den Personalrat aus Gründen des Datenschutzes ganz oder teilweise unzulässig sei oder aber vorher die Einwilligung des Beschäftigten eingeholt werden müsse.

Der Personalrat wird im Rahmen seiner Aufgaben, die ihm nach dem BPersVG eingeräumt bzw. aufgegeben werden, auch personenbezogene Daten der Beschäftigten verarbeiten und nutzen müssen. Dabei ist von praktischer Bedeutung, ob die Interessenvertretung selbst Adressat des BDSG ist. Das BDSG gilt für die Phasen der Erhebung, Verarbeitung und Nutzung personenbezogener Daten und ist gemäß § 1 Abs. 2 BDSG von folgenden Stellen – im BDSG „verantwortliche Stellen" genannt – anzuwenden:

- öffentliche Stellen des Bundes und
- nicht-öffentliche Stellen[4].

Die Anwendung des BDSG hängt also von der **Rechtsform der datenverarbeitenden Stelle** ab.

3.1 Der Arbeitgeber/das Unternehmen als Adressat des BDSG

Öffentliche Stellen des Bundes sind Behörden, die Organe der Rechtspflege und andere öffentlich-rechtliche organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen unabhängig von ihrer Rechtsform (§ 2 Abs. 1 BDSG).

Nicht-öffentliche Stellen sind – in Abgrenzung zu öffentlichen Stellen – natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen öffentlichen Rechts (§ 2 Abs. 4 BDSG).

Maßgebend dafür, dass eine datenverarbeitende Stelle dem privaten (nicht-öffentlichen Bereich) zuzuordnen ist, ist zunächst allein die privatrechtliche Organisationsform. „Natürliche" Personen – gleichgültig, ob sie als Privatpersonen auftreten oder bei der Ausübung einer selbstständigen Arbeit (Einzelfirma, freie Berufe) auftreten – sowie alle privatrechtlichen Unternehmungen und Vereinigungen – in der Rechtsform GmbH, OHG, KG, Verein, Stiftung, Partei etc. – gehören zu den nicht-öffentlichen Stellen[5]. Die rechtliche Selbstständigkeit ist ein entscheidendes Kriterium dafür, wer das BDSG anzuwenden hat. Das bedeutet, dass das einzelne Unternehmen (bzw. die einzelne Behörde) Adressat des BDSG ist.

Die Interessenvertretung ist selbst weder als so genannte „öffentliche Stelle" noch als „nicht-öffentliche Stelle" anzusehen, da sie keine rechtlich selbstständige Stelle ist. Somit ist der Personalrat auch **nicht direkter Adressat des BDSG**. Die Interessenvertretung ist wie jeder Beschäftigte bzw. wie jede Abteilung der Dienststelle bzw. des Unternehmens Teil der verantwortlichen Stelle und gegenüber der eigenen Dienststelle bzw. dem eigenen Unternehmen kein Dritter im Sinne des BDSG. Dieses ist die einhellige Meinung der Datenschützer. Dieser Meinung hat sich auch das BAG angeschlossen. Das BAG vertritt in einem aktuellen Beschluss die Auffassung, „dass der GBR nicht etwa ‚Dritter' im Sinne des § 3 Abs. 9 BDSG außerhalb der ‚speichernde Stelle'[6] im Sinne des § 3 Abs. 8 BDSG, also des Unternehmens steht. Vielmehr ist er selbst Teil der speichernden Stelle. Dies entspricht heute hinsichtlich der Betriebsräte wohl allgemeiner Meinung…"[7].

Da die Interessenvertretung nicht Dritter im Sinne des BDSG ist, sondern Teil der verantwortlichen Stelle[8], bedeutet dieses für die Weitergabe personenbezogener Daten durch den Arbeitgeber an die Interessenvertretung folgendes: Der Datenfluss innerhalb eines Unternehmen oder Behörde stellt keine Übermittlung im Sinne des § 3 Abs. 4 Nr. 3 BDSG dar. Läge eine Übermittlung vor, müsste die Weiterleitung von personenbezogenen Daten vorab auf Zulässigkeit nach § 4 BDSG geprüft werden. Die Weiterleitung personenbezogener Daten vom Arbeitge-

3) Vgl. BAG, Beschluss v. 11.11.1997, Datenschutz und Datensicherheit, 1998, S. 227.

4) Für öffentliche Stellen der Länder gilt das jeweilige Landesdatenschutzgesetz, wobei es hier noch eine Reihe von Ausnahmen gibt. So gilt in der Regel für sogenannte Eigenbetriebe der Städte und Gemeinden das BDSG.

5) Vgl. für viele: Gola/Schomerus, Bundesdatenschutzgesetz, 7. Auflage, 2002, § 2 Rn. 19.

6) Im alten BDSG war die Bezeichnung für die datenverarbeitende Stelle „speichernde Stelle". Mit der Novellierung des BDSG wird der Begriff „speichernde Stelle" durch den Begriff „verantwortliche Stelle" ersetzt, was datenschutzrechtlich jedoch keine weiteren Konsequenzen hat.

7) BAG, Beschluss v. 11.11.1997, Datenschutz und Datensicherheit, 1998, S. 228 mit weiteren Nachweisen.

8) Vgl. auch: Lorenzen/Schmitt/Etzel/Gerhold/Schlatmann/Rehak, Bundespersonalvertretungsgesetz, § 68 Rn. 61.

ber zum Personalrat unterliegt aber nicht der zusätzlichen Zulässigkeitsprüfung nach dem BDSG. Maßgeblich für die Weiterleitung der Daten an den Personalrat ist allein das BPersVG[9]. Deshalb kann der Arbeitgeber dem Personalrat nicht Informationen unter Hinweis auf den Datenschutz verweigern[10].

3.2 Zulässigkeit der Verarbeitung personenbezogener Daten der Beschäftigten

Die Zulässigkeit der Datenverarbeitung ergibt sich für die verantwortliche Stelle aus § 4 i.V.m. § 28 BDSG[11]. Dabei geht das BDSG davon aus, dass die Verarbeitung und Nutzung personenbezogener Daten verboten ist, außer sie ist erlaubt. Die Einbindung der Erhebung von Daten in dieses Regelungsprinzip („Verbot mit Erlaubnisvorbehalt") ist dann gegeben, wenn die erhobenen Daten anschließend automatisiert verarbeitet werden sollen. Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur erlaubt bzw. zulässig, soweit

- das BDSG (insbesondere § 28 BDSG) oder
- eine andere Rechtsvorschrift dieses erlaubt oder anordnet oder
- der Betroffene eingewilligt hat.

Die Dienststelle kann auf der Basis gesetzlicher Vorschriften („andere Rechtsvorschrift") personenbezogene Daten der Beschäftigten verarbeiten. Eine **„andere Rechtsvorschrift"** in diesem Sinne kann auch eine **Dienstvereinbarung** sein. Die Dienststelle kann sich aber auch als rechtliche Grundlage auf das BDSG selbst oder genauer ausgedrückt auf den § 28 BDSG beziehen. Dieses wird in der Praxis die zentrale rechtliche Basis für die Datenerhebung, -verarbeitung und -nutzung sein, wobei dieses nur in einer sehr engen Zweckbindung und Zweckbestimmung bezogen auf das Arbeitsverhältnis erlaubt ist. Auf der Basis dieser rechtlichen Vorgabe dürfen im Rahmen der Zweckbestimmung des Arbeitsvertragsverhältnisses **personenbezogene Daten** der Beschäftigten auch durch den **Personalrat** – als ein Teil der verantwortlichen Stelle – verarbeitet werden. Als weitere alternative Möglichkeit der rechtmäßigen Verarbeitung personenbezogener Daten kann die Einwilligung des Beschäftigten herangezogen werden, was aber in der Praxis nach Auffassung des Autors eher selten geschieht. Eine Einwilligung muss dabei den Anforderungen des § 4a BDSG genügen, was u. a. Freiwilligkeit und Schriftlichkeit umfasst.

Die Prüfung der Rechtmäßigkeit (d.h. Zulässigkeit) der Datenverarbeitung wird vom Unternehmen bzw. der Dienststelle bzw. vom betrieblichen Datenschutzbeauftragten/behördlichen Datenschutzbeauftragten vorgenommen werden müssen.

3.3 Weiterleitung personenbezogener Daten an den Personalrat

Werden personenbezogene Daten an den Personalrat weitergeleitet, die der Arbeitgeber bereits gespeichert hat, kann der Personalrat davon ausgehen, dass diese Daten auch rechtmäßig im Sinne des BDSG erhoben und gespeichert worden sind. Der Personalrat kann und darf dann im Rahmen seiner Aufgabenerfüllung nach dem BPersVG diese personenbezogenen Daten verarbeiten, ohne dass eine Zulässigkeits-Prüfung nach § 4 BDSG von Seiten des Personalrats noch einmal erfolgen muss. Das hat u.a. zur Folge, dass der Beschäftigte – entgegen der Auffassung einiger Arbeitgeber – nicht seine Einwilligung erteilen muss, wenn der Arbeitgeber seine personenbezogenen Daten an die Interessenvertretung weiterleitet.

Die Weiterleitung von personenbezogenen Daten der Beschäftigten an den Personalrat bestimmt sich allein durch die **Vorgaben des BPersVG**. So ist die Voraussetzung für die sachgerechte Wahrnehmung der Aufgaben nach dem BPersVG eine vollständige und rechtzeitige Unterrichtung des Personalrats durch den Arbeitgeber. Dazu enthält das BPersVG in § 68 Abs. 2 BPersVG eine allgemeine Informationspflicht des Arbeitgebers. Die Unterrichtung muss ohne Mahnung durch den Personalrat erfolgen, wobei die vom Arbeitgeber geschuldete Unterrichtung die Interessenvertretung in die Lage versetzen soll, in eigener Verantwortung selbst zu prüfen, ob sich für sie weitere Aufgaben ergeben und ob sie tätig werden muss. Der Arbeitgeber hat diejenigen Auskünfte zu erteilen, die erforderlich sind, damit die Interessenvertretung ihren Aufgaben nachkommen kann[12]. Zu den Aufgaben des Personalrats gehören u. a. das Überwachungsrecht (§ 68 Abs. 1 Nr. 2 BPersVG) und die Mitbestimmungsrechte (z.B. nach den §§ 75 Abs. 3 Nr. 17 und 75 Abs. 3 Nr. 8 BPersVG).

Dem Personalrat sind zusätzlich **auf Verlangen** jederzeit die zur Durchführung seiner Aufgaben erforderlichen Unterlagen zur Verfügung zu stellen. Zu diesen Aufgaben können die in § 68 Abs. 1 BPersVG aufgelisteten Aufgaben und wie bereits erwähnt, die Aufgaben, die sich aus dem Überwachungsrecht, den verschiedenen Mitbestimmungsrechten ergeben, gehören.

3.4 Beispiele für Informationen mit personenbezogenen Daten

Als **Beispiele** für Informationen, die der Interessenvertretung überlassen werden müssen und die auch personenbezogene Daten der Beschäftigten enthalten können, sind zu nennen:

- Auswertungen einer vom Arbeitgeber durchgeführten Mitarbeiterbefragung, wenn die gewonnenen Erkenntnisse auch für die Betriebsratsarbeit von Bedeutung sein können,
- alle relevanten Arbeitszeitdaten der Arbeitnehmer, insbesondere, wenn der Arbeitgeber Vertrauensarbeitszeit einführen will,
- angemeldete Nebentätigkeiten der einzelnen Arbeitnehmer, inklusive Namen, Umfang und Art,
- Geschäftsverteilung und Kompetenzen nach innen und außen (Zuständigkeiten, Vollmachten, Vertretungsbefugnisse auf Arbeitgeberseite),
- Gesamtübersicht über alle für den Betrieb eingesetzten freien Mitarbeiter unter Angabe der Personalien, des Aufgabengebietes, des Arbeitsplatzes, der festgelegten Arbeitszeiten und der Art der Entlohnung,
- Namen derjenigen Personen, die besonderen Schutzgesetzen unterliegen (z.B. Schwangere, Jugendliche, Schwerbehinderte, ältere Beschäftigte),
- Schwangerschaft von Beschäftigten, selbst wenn sie den Arbeitgeber auffordern, diese Information nicht weiterzugeben[13].

In Bezug auf die Einführung und Anwendung von IuK-Techniken haben sowohl das BAG als auch das BVerwG die In-

9) Vgl. Fitting/Kaiser/Heither/Engels/Schmidt, Betriebsverfassungsgesetz, 21. Aufl. 2002, § 1 Rn. 210; Simitis/Dammann/Geiger/Mallmann/Walz, Kommentar zum Bundesdatenschutzgesetz, Loseblatt, § 3 Rn. 233.

10) Vgl. Fitting/Kaiser/Heither/Engels/Schmidt (Fn. 9), § 1 Rn. 210.

11) Gemäß § 12 Abs. 4 BDSG gelten für bestehende und zukünftige dienst- oder arbeitsrechtliche Rechtsverhältnisse anstelle der entsprechenden Vorgaben im zweiten Abschnitt des BDSG der § 28 Abs. 1 und 3 Nr. 1 BDSG sowie die §§ 33 bis 35 BDSG.

12) Vgl. BAG, Beschluss v. 17.3.87, AiB 1987, S. 289.

13) Vgl. mit weiteren Nachweisen: Däubler/Kittner/Klebe (Hg.), Betriebsverfassungsgesetz, 8. Aufl. 2002, § 80 Rn. 75; Fitting/Kaiser/Heither/Engels/Schmidt (Fn. 9), § 80 Rn. 61; vgl. auch die Beispiele bei: Lorenzen/Schmitt/Etzel/Gerhold/Schlatmann/Rehak (Fn. 8), § 68 Rn. 45.

formationen, die auch personenbezogene Daten enthalten können, folgendermaßen umrissen. Der Arbeitgeber hat die Interessenvertretung im Rahmen des Überwachungsrechtes und auch des Mitbestimmungsrechtes zu unterrichten über

- eingesetzte Hard- und Software,
- alle bestehenden Dateien, in denen personenbezogene Daten der Beschäftigten gespeichert sind,
- Übermittlung der Daten an Dritte,
- Verknüpfung und Auswertung der personenbezogenen Daten[14].

Auf Verlangen der Interessenvertretung hat der Arbeitgeber die oben aufgeführten Informationen aber auch beispielsweise folgende Informationen vorzulegen:

- Zeiterfassungskarten, wenn die Interessenvertretung den Umfang der Ableistung von Überstunden prüfen will,
- monatliche Aufstellungen über erfasste Abwesenheits- und bezahlte Überstundenzeiten,
- Unterlagen, woraus die Interessenvertretung entnehmen kann, welche Arbeitnehmer wann wie viele Überstunden geleistet haben,
- Listen über die tarifliche Eingruppierung der Arbeitnehmer, sofern die Interessenvertretung diese überprüfen will,
- Nachweise über die Durchführung gesetzlicher Vorschriften, z.B. über die Gewährung von Stillzeiten nach dem Mutterschutzgesetz, Urlaubslisten nach BUrlG, Zahl der beschäftigten Schwerbehinderten, Mehrarbeitsaufstellung nach Tarifvertrag[15].

4. Kontrolle des Datenschutzes

Im Rahmen der Umsetzung des Datenschutzes kommt einer wirksamen Kontrolle eine zentrale Bedeutung zu. Die Kontrollinstanzen (Abb. 1) sind auch für die Verarbeitung und Nutzung personenbezogener Daten durch den Personal-/Betriebsrat von Bedeutung.

4.1 Kontrollinstanzen

Das Kontrollsystem für den öffentlichen und nicht-öffentlichen Bereich umfasst die Kontrolle durch

- den betrieblichen/behördlichen Datenschutzbeauftragten
- den Betriebs-/Personalrat (nur in Bezug des Beschäftigten-Datenschutzes),
- die Aufsichtsbehörde und
- den Betroffenen (Beschäftigten).

4.2 Betrieblicher/behördlicher Datenschutzbeauftragter

Nach § 4 f Abs. 1 BDSG müssen öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen einen betrieblichen Datenschutzbeauftragten (bDSB) schriftlich bestellen. Eine Bestellung muss in nicht-öffentlichen Betrieben (Privatbetriebe) nicht erfolgen, wenn höchsten vier Beschäftigte mit der Verarbeitung personenbezogener Daten beschäftigt sind. Diese Einschränkung für kleine Betriebe gibt es für den öffentlichen Bereich nicht. Der bDSB hat auf die Einhaltung des BDSG und anderer Gesetze über den Datenschutz hinzuwirken. So hat der bDSB u. a.

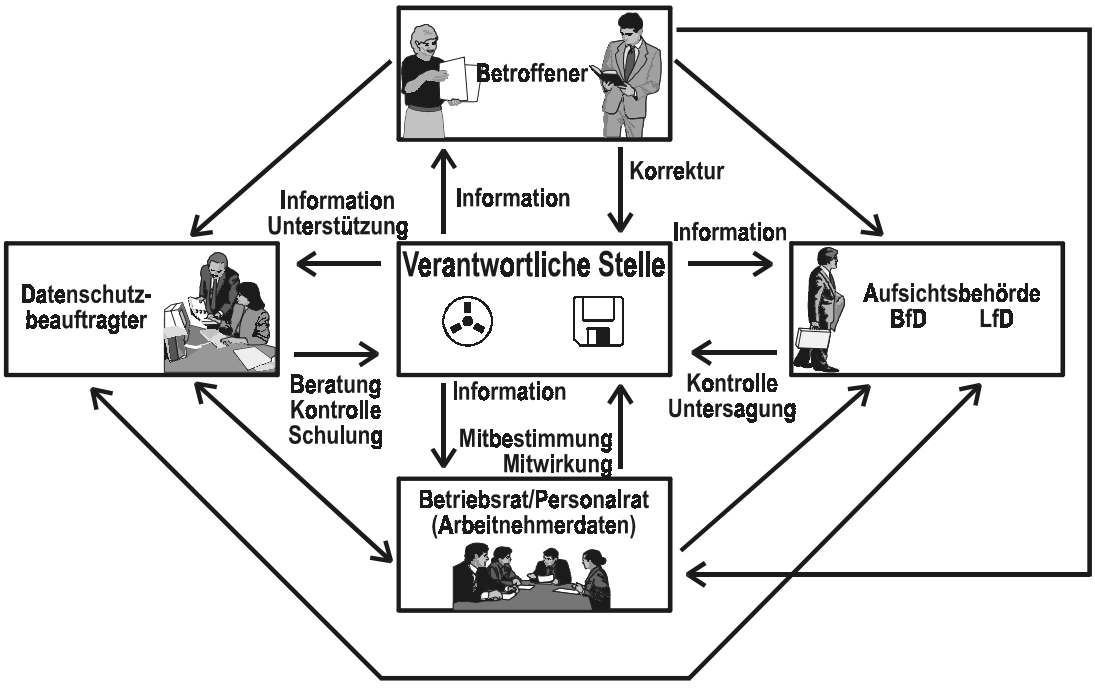
- das BDSG in konkrete Verfahrensregeln umzusetzen,
- die Prüfung der Zulässigkeit der Datenverarbeitung gemäß § 4 BDSG vorzunehmen,
- dafür Sorge zu tragen, dass die Individualrechte der Beschäftigten auf Benachrichtigung, Auskunft, Berichtigung und Sperrung (§ 33 ff. BDSG) eingehalten werden
- auf die Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen nach § 9 BDSG hinzuwirken[16].

14) Vgl. BAG, Beschluss v. 17.3.87, Arbeitsrecht im Betrieb, 12/87, S. 288; BVerwG, Beschluss v. 8.11.1989, Recht der Datenverarbeitung, 3/90, S. 144.

15) Vgl. Däubler/Kittner/Klebe (Hg.), (Fn. 13), § 80 Rn. 90 mit weiteren Beispielen und Nachweisen.

16) Vgl. Schierbaum, Datenschutz im Betrieb – Handlungshilfe für Betriebsräte und betriebliche Datenschutzbeauftragte, 2001, S. 85; Schierbaum, Betrieblicher Datenschutzbeauftragter und Betriebsrat – Die zwei Akteure des Arbeitnehmer-Datenschutzes, AiB 2001, S. 517 ff.

Abb. 1: Kontrollinstanzen des Datenschutzes



Im Rahmen seiner Aufgabenerfüllung hat der bDSB Übersichten gemäß § 4e BDSG zu führen. Zudem wird der bDSB auch vor Ort an einzelnen PCs und Servern Kontrollen durchführen können.

Nach dem BDSG selbst wäre damit grundsätzlich auch die Möglichkeit gegeben, beim Personalrat entsprechende Kontrollen durchzuführen. So könnte der bDSB neben der Übersicht über die gespeicherten personenbezogenen Daten hinaus auch sehen, ob die Interessenvertretung bestimmte Vereinbarungen oder Verhandlungsstrategien entwickelt hat. Zudem könnte der bDSB gar Protokolle von Personalratssitzungen einsehen. Allein anhand dieser Beispiele wird jedoch deutlich, dass die Interessenvertretung entsprechenden Kontrollen nicht unkritisch gegenüberstehen kann[17].

Diese Frage der **Kontrolle des Betriebsrats** durch den bDSB war bis zum Beschluss des Bundesarbeitsgerichts vom 11.11.1997 sehr umstritten, wobei das Ergebnis dieser Auseinandersetzung erhebliche Konsequenzen für den Datenschutz im Betriebsratsbüro hat. In der Literatur bestanden – und bestehen auch heute noch – zwei gegensätzliche Auffassungen. Auf der einen Seite wird ein entsprechendes Kontrollrecht damit begründet, dass der Betriebsrat als Teil der verantwortlichen Stelle in gleicher Weise wie jede Abteilung im Unternehmen einer Kontrolle des bDSB unterliege. Denn eine Kontrolle gehöre zu den vom BDSG geforderten Schutzvorkehrungen. Auch die von Betriebsräten geäußerte Befürchtung, dass der Arbeitgeber sich mit Hilfe des bDSB Informationen über die Betriebsratsarbeit verschaffe, sei schon deshalb unbegründet, da der bDSB wegen seiner Unabhängigkeit und Schweigepflicht gegenüber dem Arbeitgeber diesem auch keine Angaben machen dürfe, die die Arbeit des Betriebsrats beeinträchtige[18].

Auf der anderen Seite wird von einem großen Teil der Literatur eine Kontrolle abgelehnt, da der Betriebsrat seine Aufgaben eigenständig und unabhängig wahrnehmen können muss. Schon frühzeitig haben die Befürworter des Kontrollrechts die Argumente für die Ablehnung selbst geliefert, indem sie auf die Gefahr hinwiesen, dass dieses Kontrollrecht zum „Einfallstor für die Versorgung des Arbeitgebers mit ihm sonst nicht zugänglichen Informationen wird."[19] Da dieses vom Betriebsverfassungsgesetz im Verhältnis zwischen Betriebsrat und Arbeitgeber gerade nicht gewollt sei, sei eine derartige Einflussnahme auf die Tätigkeit des Betriebsrats nicht als zulässig anzusehen[20].

4.3 Rechtsprechung BAG

Diese Diskussion müsste mit dem Beschluss des BAG[21] vorerst beendet sein. Das BAG hat sich in seiner Entscheidung den Kontrollgegnern angeschlossen hat. Es hält das **Kontrollrecht** mit der vom BetrVG vorgeschriebenen **Unabhängigkeit** des Betriebsrat für **unvereinbar**. Denn ein so massiver Eingriff in das Strukturprinzip des BetrVG kann dem BDSG nicht entnommen werden. Das Ergebnis leitet das Gericht vor allem aus der Stellung des bDSB ab. Denn der bDSB nimmt im Betrieb keine neutrale Stellung ein und ist eher dem Arbeitgeber zuzurechnen, da dieser ihn auswählt und zum Datenschutzbeauftragten bestellt. Der Betriebsrat hat dabei auch kein Beteiligungsrecht, das es ihm – wie etwa bei der Bestellung und Abberufung angestellter Betriebsärzte oder Fachkräfte für Arbeitssicherheit nach § 9 Abs. 3 ASiG – ermöglichen würde, dafür zu sorgen, dass das Amt von einer Person seines Vertrauens wahrgenommen wird. Das Zustimmungsverweigerungsrecht des Betriebsrat nach § 99 BetrVG kommt nur dann in Betracht, wenn die Bestellung gleichzeitig mit als Versetzung oder Einstellung zu sehen ist. Wird ein leitender Angestellter zum bDSB bestellt, kommt dieses Zustimmungsverweigerungsrecht erst gar nicht zum Tragen.

Weiterhin stellt das BAG fest, dass der bDSB die Aufgaben des Arbeitgebers erfüllt, da er nach der Konzeption des BDSG ein Instrument der Selbstkontrolle des Unternehmens ist, das neben der Fremdkontrolle durch Aufsichtsbehörde steht. Somit ist der BDSB als „verlängerter Arm" des Arbeitsgebers anzusehen[22]. Die im BDSG verankerte Verschwiegenheitspflicht[23] ist nach Auffassung des Gerichts ebenfalls nicht geeignet, „dem bDSB im Spannungsverhältnis zwischen Arbeitgeber und Betriebsrat eine neutrale Position zu verschaffen."[24] Denn die Daten, die den Meinungsbildungsprozess des Betriebsrats betreffen, bleiben weitgehend außerhalb der Verschwiegenheitspflicht.

Nach Auffassung des BAG würde eine Unterwerfung des Betriebsrats unter die Kontrollbefugnis des bDSB damit einem Vertreter des Arbeitgebers Zugang zu grundsätzlich allen Dateien des Betriebsrats eröffnen ohne Rücksicht darauf, ob sie personenbezogene Daten enthalten oder nicht. Insoweit wäre der Betriebsrat damit unmittelbar der Kontrolle durch den betrieblichen Gegenspieler unterworfen.

Dieses wäre mit der Unabhängigkeit des Betriebsrats nicht vereinbar; denn: „Die Unabhängigkeit des Betriebsrats ist als tragendes Prinzip von so hoher Bedeutung für die Betriebsverfassung, dass dem Gesetzgeber des BDSG nicht unterstellt werden kann, er habe stillschweigend so tief und konfliktträchtig in dieses Prinzip eingreifen wollen."[25]

So kommt das BAG zu dem Ergebnis, dass die vom BetrVG geforderte Unabhängigkeit der Betriebsräte vom Arbeitgeber eine Kontrolle des bDSB in Bezug auf die Datenverarbeitung des Betriebsrats ausschließt[26].

Die Aussagen des BAG zur betriebsverfassungsrechtlichen Unabhängigkeit des Betriebsrats und dem daraus folgenden Ausschluss der Kontrolle durch den bDSB sind auch auf das Verhältnis **Personalrat** und **behördlichen Datenschutzbeauftragten** anzuwenden[27].

4.4 Keine Kontrolle des Personalrats durch Vertreter des Arbeitgebers

Der BAG-Beschluss stellt für die Person des bDSB fest, dass eine Kontrolle des Betriebsrats durch einen Vertreter des Arbeitgebers ausgeschlossen ist. Über sehr weitreichende Kontrollmöglichkeiten

17) Vgl. auch: Wedde, Datenverarbeitung im Betriebsratsbüro – Wer kontrolliert den Datenschutz, AiB 1999, S. 697.

18) Vgl. v. Hoyningen-Heune, Datenverarbeitung durch Betriebsrat und Datenschutzbeauftragten, Beilage zur Neuen Zeitschrift für Arbeits- und Sozialrecht, 1985, S. 23 f.; vgl. auch Schierbaum/Kiesche, Arbeitnehmerdatenschutz – Aufgaben für den betrieblichen Datenschutzbeauftragten und den Betriebsrat, Computer und Recht, 3/93, S. 157 f. mit weitern Nachweisen.

19) Simitis/Dammann/Mallmann/Reh, Kommentar zum Bundesdatenschutzgesetz, 1981, § 28 Rn. 144.

20) Vgl. hierzu Schierbaum/Kiesche (Fn. 18), S. 157 f. mit weiteren Nachweisen.

21) Vgl. BAG, Beschluss v. 11.11.97, Datenschutz und Datensicherheit, 1998, S. 227 ff.

22) Vgl. BAG, Beschluss v. 11.11.97, Datenschutz und Datensicherheit, 1998, S. 230.

23) Im novellierten BDSG ist die Verschwiegenheitspflicht in § 4 f Abs. 4 BDSG geregelt.

24) BAG, Beschluss v. 11.11.97, Datenschutz und Datensicherheit, 1998, S. 230.

25) BAG, Beschluss v. 11.11.97, Datenschutz und Datensicherheit, 1998, S. 231.

26) Vgl. für den Personalrat: Wolber, Keine Kontrolle der Personalvertretung durch den behördeninternen Datenschutzbeauftragten, PersR 1998, S. 420 ff.; wohl anderer Auffassung: Kuhring/Werner, Kontrolle des Betriebsrats durch den betrieblichen Datenschutzbeauftragten, Datenschutz und Datensicherheit, 2000, S. 159 ff.

27) Vgl. Lorenzen/Schmitt/Etzel/Gerhold/Schlatmann/Rehak (Fn. 8), § 68 Rn. 67a.

verfügen in Behörden und Betrieben aber auch die **Systemadministratoren**. So können sie alle Informationen, die über das betriebliche/behördliche Netzwerk laufen, lesen. Dieses bezieht sich sowohl auf das Arbeitsverhalten, als auch auf das Kommunikationsverhalten der Beschäftigten. Mit entsprechender Software können sich die Systemadministratoren u. U. auch ohne Wissen der einzelnen Beschäftigten auf jeden PC aufschalten und alle Dateien und Daten zur Kenntnis nehmen. Zudem können sie die Verbindungsdaten von E-Mails (Adresse, Zeit etc.) und auch die Inhalte von E-Mail mitlesen und kontrollieren. Ist die Interessenvertretung in das betriebliche Netz eingebunden, ist eine entsprechende Kontrolle durch die Systemadministratoren ebenfalls möglich.

Gerade vor dem Hintergrund des BAG-Beschlusses muss der Interessenvertretung die Möglichkeit gegeben werden, sich dieser möglichen Kontrolle durch die Systemadministratoren und damit einer möglichen Kontrolle durch den Arbeitgeber zu entziehen. Vor diesem Hintergrund muss der Interessenvertretung ein einzelstehender PC oder ein eigenes kleines Netzwerk zur Verfügung gestellt werden, um so unkontrolliert zur Erfüllung ihrer Aufgaben z.B. Internet- und E-Mail zu nutzen.

4.5 Kontrolle durch den Bundesbeauftragten für den Datenschutz

Für die Fremdkontrolle des Datenschutzes im öffentlichen Bereich des Bundes ist der Bundesbeauftragte für den Datenschutz (BfD) zuständig (§§ 22 ff. BDSG). Der BfD kontrolliert bei den öffentlichen Stellen des Bundes die Einhaltung des BDSG und anderer Rechtsvorschriften zum Datenschutz. Die öffentlichen Stellen des Bundes sind bei entsprechenden Prüfungen verpflichtet, den BfD bei der Erfüllung seiner Aufgaben zu unterstützen. So ist dem BfD und seinen Beauftragten insbesondere

- Auskunft zu ihren Fragen zu geben sowie
- Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren und
- jederzeit Zutritt in alle Diensträume zu gewähren.

Der BfD teilt die Ergebnisse seiner Kontrolle der öffentlichen Stelle mit. So kann er auch Vorschläge zur Verbesserung des Datenschutzes und vor allem zur Beseitigung festgestellter Mängel machen.

Der Kontrolle durch den BfD unterliegt auch der Personalrat.

Abb. 2: „8 Gebote" zum Datenschutz – Anlage zu § 9 BDSG

„8 Gebote" zum Datenschutz Anlage zu § 9 BDSG	
1. Zutrittskontrolle	Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.
2. Zugangskontrolle	Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.
3. Zugriffskontrolle	Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
4. Weitergabekontrolle	Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.
5. Eingabekontrolle	Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.
6. Auftragskontrolle	Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
7. Verfügbarkeitskontrolle	Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
8. Getrennte Verarbeitung	Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

5. Konsequenzen für den Datenschutz bei der Interessenvertretung

Auch wenn durch den BAG-Beschluss deutlich geworden ist, dass eine Kontrolle des Betriebsrats durch den bDSB auszuschließen ist, muss natürlich auch im Betriebsratsbüro und ebenso im Personalratsbüro der Datenschutz umgesetzt und die Einhaltung des BDSG auch kontrolliert werden. Das heißt, die Interessenvertretung bewegt sich keineswegs „in einem datenschutzfreien Raum"[28]. Nach § 68 Abs. 1 Nr. 2 BPersVG hat der Personalrat darüber zu wachen, dass die zugunsten der Beschäftigten geltenden Gesetze durchgeführt werden. Vor diesem Hintergrund muss er auch für die Umsetzung des Datenschutzes im eigenen Arbeitsbereich sorgen.

28) Vgl. BAG, Beschluss v. 11.11.97, Datenschutz und Datensicherheit, 1998, S. 232.

Dabei ist es sinnvoll, dass der Personalrat einen **„eigenen Datenschutzbeauftragten“** benennt[29], der die Umsetzung des Datenschutzrechts „in die Hand“ nimmt. Diese Person ist jedoch kein behördlicher Datenschutzbeauftragter im Sinne des BDSG, sondern die Benennung einer Person stellt eine Form der Selbstkontrolle des Personalrats dar. Dieses Personalratsmitglied sollte sich intensiv mit den Vorgaben des Datenschutzrechts befassen und die Aufgaben nach dem BDSG wahrnehmen, die der bDSB im Personalratsbüro nicht wahrnehmen kann bzw. darf. Es soll nicht unerwähnt bleiben, dass der Personalrat selbstverständlich eine Kontrolle durch den bDSB dulden oder erlauben kann, gerade wenn ein gutes Vertrauensverhältnis zwischen dem Personalrat und dem bDSB besteht.

5.1 Zulässigkeit der Datenverarbeitung im Personalratsbüro

Der Personalrat hat ähnlich wie der bDSB die Einhaltung des BDSG zu überwachen (§ 68 Abs. 1 Nr. 2 BPersVG). Wie bereits erwähnt, muss sich die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch den Personalrat eng an den Vorgaben des BPersVG halten. In diesem Zusammenhang ist die vom BDSG vorgeschriebene Zweckbindung und Zweckbestimmung in Bezug auf das Vertragsverhältnis zwischen Beschäftigten und Arbeitgeber zu beachten. Die Daten dürfen nur dann verarbeitet werden, wenn dieses für die Aufgabenerfüllung des Personalrats zwingend erforderlich ist. Wenn die Daten nicht mehr benötigt werden, d.h. die Zweckbestimmung weggefallen ist, sind sie zu löschen[30]. Zudem scheidet auch folgerichtig eine Vorratsspeicherung aus. So hat der Personalrat die bestehenden gesetzlichen Regelungen eng auszulegen, auch wenn es im Einzelfall seine Arbeit erschwert[31].

5.2 Führen von Übersichten

Da der bDSB keinen Zugang zum Personalratsbüro hat, ist er auch nicht ohne weiteres in der Lage, die geforderten **Übersichten nach § 4e BDSG** zu führen. So wird der Personalrat dieses übernehmen müssen.

Die Übersicht muss vor allem folgende Angaben enthalten

- Zweckbestimmung der Datenerhebung, -verarbeitung und -nutzung
- Regelfristen zur Löschung
- eine allgemeine Beschreibung, ob die Maßnahmen nach § 9 BDSG zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

Abb. 3: Rechte der Betroffenen

BDSG	Inhalt der Bestimmung
§ 4 Abs. 3	Unterrichtung bei Direkterhebung
§ 33	Benachrichtigung über Speicherung und Art der Daten
§ 34	Auskunft über gespeicherte personenbezogene Daten, Herkunft und Empfänger, Zweck der Speicherung und regelmäßige Übermittlung
§ 35 Abs. 1	Berichtigung, wenn Daten unrichtig
§ 35 Abs. 2	Löschung bei unzulässiger Speicherung, bei sensiblen Daten und bei fehlender Erforderlichkeit
§ 35 Abs. 3 und 4	Sperrung statt Löschung bei gesetzlich vorgeschriebenen Aufbewahrungsfristen, bei Beeinträchtigung schutzwürdiger Interessen des Betroffenen und wenn der Aufwand für eine Löschung unverhältnismäßig hoch ist
	Sperrung, wenn Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt
§ 35 Abs. 5	Recht auf Widerspruch
§ 8	Unabdingbarkeit der Rechte; kein Ausschluss oder keine Beschränkung durch Rechtsgeschäft
§ 7	Schadensersatz
§ 5	Datengeheimnis

5.3 Technische und organisatorische Maßnahmen

Als Teil der verantwortlichen Stelle muss der Personalrat in seinem Aufgaben- und Arbeitsbereich die in der Anlage zu § 9 BDSG verankerten Zielvorgaben verbindlich einhalten. Mit der Novellierung des BDSG sind diese Vorgaben von vormals zehn auf acht (Abb. 2) reduziert worden. Da der Personalrat personenbezogene Daten von Beschäftigten verarbeitet und diese Daten in der Regel als sehr sensibel einzustufen sind, muss der Betriebsrat die Zielvorgaben des § 9 BDSG zwingend einhalten[32].

Die **Zutrittskontrolle** verlangt, Unbefugten den „körperlichen“ Zutritt zu den Datenverarbeitungsanlagen der Interessenvertretung zu verwehren. Es soll verhindert werden, dass Personen, die dazu nicht befugt sind, unkontrolliert in die Nähe von Datenverarbeitungsanlagen des Personalrats kommen. Hierdurch soll von vornherein die Möglichkeit unbefugter Kenntnis- und Einsichtsnahme ausgeschlossen werden. Der Kreis der Zugangsberechtigten beschränkt sich erst einmal auf die Personalratsmitglieder. So müssen bei Abwesenheit die Türen des Personalratsbüros verschlossen werden.

Die **Zugangskontrolle** soll die unbefugte Nutzung von Datenverarbeitungssystemen verhindern. Im Gegensatz bzw. in Ergänzung zur Zutrittskontrolle ist mit Zugangskontrolle das Eindringen in das EDV-System gemeint.

Die **Zugriffskontrolle** soll gewährleisten, dass die zur Benutzung berechtigten (in diesem Fall Personalratsmitglieder) nur auf die Daten zugreifen können, die sie zur Erfüllung ihrer Aufgabe benötigen. Dieses kann bei großen Gremien in Betracht kommen, wo die Mitglieder in verschiedenen Ausschüssen tätig sind.

29) Vgl. Wedde, Datenverarbeitung im Betriebsratsbüro – Wer kontrolliert den Datenschutz? AiB 1999, S. 700; Däubler/Kittner/Klebe (Hg.), (Fn. 13), § 94 Rn. 43; Böker, Des Betriebsrats eigner Datenschützer, Computer Fachwissen, 1/99, S. 31; kritisch: Gola/Schomerus (Fn. 5), § 4g Rn. 11.

30) Vgl. auch: Kamp/Roth/Klebe, EDV im Betriebsratsbüro – Eine Handlungshilfe für betriebliche Interessenvertreter, 1989, S. 33 f.

31) Wedde, Datenschutz im Betriebs- und Personalratsbüro, Computer-Fachwissen 2001, S. 30.

32) Vgl. zu den technischen und organisatorischen Maßnahmen: Schierbaum, 10 Gebote des Datenschutzes, ComputerInformation, 1995, S. 29 ff.

Durch die **Weitergabekontrolle** soll verhindert werden, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können. Unbefugt ist jedes Verhalten, dass sich nicht mit der Aufgabenerfüllung des Personalrats in Einklang bringen lässt. So sind Datenträger in einem Schrank gut verschlossen aufzubewahren.

Die **Eingabekontrolle** soll gewährleisten, dass die Datenverarbeitung und die Zugriffe auf personenbezogene Daten dokumentiert werden. Diese Zielvorgabe wird u.a. eine Protokollierung zur Folge haben müssen.

Der Punkt **Auftragskontrolle** wird nicht zum Tragen kommen, da der Personalrat wohl keine Verarbeitung personenbezogener Daten nach Außen vergeben wird.

Die neu in BDSG auf genommene **Verfügbarkeitskontrolle** zielt auf den Schutz vor zufälliger Zerstörung ab und meint z. B. Wasserschäden, Brand, Blitzschlag, Stromausfall. Maßnahmen sind z.B. Auslagerung von Sicherungskopien.

Inwieweit das **Trennungsgebot** im Personalratsbüro zum Tragen kommt, muss im Einzelfall geprüft werden.

5.4 Rechte der Beschäftigten

Die Beschäftigen haben eine Fülle an Rechten (Abb. 3) nach dem BDSG, die auch für die Datenverarbeitung durch den Personalrat gelten[33].

Selbstverständlich müssen die Rechte der Beschäftigten vor allem nach den §§ 33 ff. BDSG eingehalten werden. Diese Rechte sind unabdingbar und gelten somit auch für die Verarbeitung von Daten durch den Personalrat. Grundsätzlich wird eine Information und Benachrichtigung bei der Erhebung und Speicherung von Beschäftigten-Daten durch den Arbeitgeber erfolgen müssen. Erfolgt die Datenerhebung durch den Personalrat, z. B. im Rahmen von Mitarbeiterbefragungen, muss der Personalrat die Beschäftigten gemäß § 4 Abs. 3 BDSG informieren.

Um jedoch die weiteren Rechte Auskunft, Berichtigung, Löschung und Sperrung gewährleisten zu können, muss der Personalrat in der Lage sein, dem einzelnen Beschäftigten Auskunft über seine personenbezogenen Daten zu geben. Dieses wird jedoch nur dann möglich sein, wenn der Personalrat die Übersichten nach § 4e BDSG in aktueller Form führt.

6. Zusammenfassung

1. Die Interessenvertretung darf im Rahmen ihrer Aufgabenerfüllung personenbezogene Daten der Beschäftigen verarbeiten. Die **rechtliche Basis** für die Datenverarbeitung ist das **BPersVG** bzw. die Landespersonalvertretungsgesetze. Das BDSG beschränkt insoweit die Datenverarbeitung durch den Personalrat nicht.

2. Der **Personalrat** ist **nicht Dritter** im Sinne des BDSG, sondern Teil der verantwortlichen Stelle. Die Weiterleitung von Beschäftigten-Daten an den Personalrat stellt keine Übermittlung im Sinne des BDSG dar, sondern ist eine Weiterleitung von Daten. So muss diese Weiterleitung auch nicht auf Zulässigkeit nach § 4 BDSG überprüft werden.

3. Eine **Kontrolle des Betriebsrats** durch den bDSB ist durch den Beschluss des BAG ausgeschlossen. Dieses gilt in gleicher Weise für das Verhältnis Personalrat zum bDSB. Die Interessenvertretung hat jedoch das BDSG zwingend einzuhalten.

4. Der Personalrat sollte einen eigenen **„Datenschutzbeauftragten“** bestellen. Dieser muss die Zulässigkeit der Datenverarbeitung prüfen, die technischen und organisatorischen Maßnahmen nach § 9 BDSDG umsetzen und die Rechte der beschäftigten auf Auskunft, Berechtigung, Löschung und Sperrung umsetzen.

Bruno Schierbaum
BTQ Niedersachsen
Donnerschweer Str. 84
26123 Oldenburg
Tel.: 04 41/8 20 68
E-Mail: schierbaum@btq.de

33) Vgl. ausführlich zu den Rechten der Betroffenen: Schierbaum, Die Rechte der Beschäftigten nach dem novellierten Bundesdatenschutzgesetz, PersR 2002, S. 238 ff.