

Personaldatenverarbeitende Systeme gibt es in Betrieben und Verwaltungen schon seit Jahren. Allen diesen Systemen ist gemeinsam, daß mit ihrer Hilfe eine Fülle personenbezogener Daten der Beschäftigten gespeichert, verarbeitet und ausgewertet werden können.

Personenbezogene Daten sind – so definiert es das Bundesdatenschutzgesetz – »Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlicher Person« (§ 3 Abs.1 BDSG). Und solche »Einzelangaben« stecken in Personalabrechnungs- und Informations-Systemen, in Zeiterfassungs- und Zugangskontrollsystemen, sie fallen an bei der bargeldlosen Kantinenabrechnung, in Produktions-Planungs- und Steuerungs-Systemen und der Betriebsdatenerfassung, in Telefonsystemen und bei der Bürokommunikation – letztlich kann jedes EDV-System auch Personaldaten speichern und verarbeiten. Der Trend zur elektronischen Personaldatenverarbeitung, der mit den Personalabrechnungs- und Informationssystemen (z.B. PAISY) eingeleitet wurde, verstärkt sich noch, vor allem weil die Systeme immer kleiner, immer billiger, immer schneller werden. Sichtbares Zeichen dieser Entwicklung ist der verstärkte Einsatz von Personal Computern in allen Unternehmensbereichen.

Gefahr für Persönlichkeitsrechte!

Damit können Gefahren auch für die Persönlichkeitsrechte der Beschäftigten einhergehen: Die ständige und allgegenwärtige Erhebung, Verarbeitung und Auswertung von Informationen führt zu einer von den Arbeitnehmern gar nicht mehr wahrnehmbaren Kontrolle. Zusammenhang, Hintergrund und »Entstehungsgeschichte« der dabei gespeicherten Daten bleiben vielfach unbekannt oder werden schnell vergessen – das führt zu unrichtigen Beurteilungen. Dessen ungeachtet werden aus gespeicherten Daten »Persönlichkeitsprofile« abgeleitet, die mit dem wirklichen Menschen möglicherweise kaum noch etwas zu tun haben, trotzdem aber häufig Grundlage für (Personal-) Entscheidungen werden. Diese Gefahr

Betriebliche Datenschutzbeauftragte ...

Partner oder Handlanger?

In sehr vielen Betrieben führen die Datenschutzbeauftragten ein ausgesprochenes Schattendasein. Es gibt sie zwar, aber kaum jemand kennt sie. Und wer sie kennt, möchte mit ihnen nicht viel zu tun haben. Das verwundert etwas, denn zumindest außerhalb der Betriebe ist Datenschutz ja durchaus ein Thema, auf das immer mehr Menschen sensibel reagieren. Auch Betriebsräte machen da keine Ausnahme, möglicherweise aber einen großen Fehler: Überschneidungen zwischen den Aufgaben des betrieblichen Datenschutzbeauftragten und denen des Betriebsrats legen es eigentlich nahe, sich um eine echte Kooperation zu bemühen.

Richtig ist, daß fehlende Mitbestimmungsrechte des Betriebsrats bei der Bestellung des Datenschutzbeauftragten dazu führen, daß in der Regel ein »Mann des Arbeitgebers« bestellt wird. Trotzdem aber kann der Betriebsrat erfolgreich sein, wenn er nur ernsthaft genug versucht, im Datenschutzbeauftragten einen kompetenten Partner zu finden, statt ihm von vornherein nur mit Mißtrauen zu begegnen und ihn »links« liegen zu lassen. Manfred Schuhr und Bruno Schierbaum nennen die Gründe ...



wird um so größer, je mehr Daten aus ganz verschiedenen Bereichen sich beliebig miteinander verknüpfen lassen. Und zudem vergessen Computer (im Gegensatz zu Menschen) einmal erfaßte Informationen nie – die ›Gnade des Vergessens‹ entfällt. Um diesen Gefahren zu begegnen, gibt es – rechtlich gesehen – zwei Wege:

›Individualrechtlich‹, als Abwehrmöglichkeit für den einzelnen, kommt die Anwendung des Bundesdatenschutzgesetzes (BDSG) in Betracht, dessen Zweck darin besteht, ›den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird‹ (§ 1 Abs. 1 BDSG). Für die Umsetzung des BDSG hat ein nach § 36 Abs. 1 BDSG zu bestellender betrieblicher Datenschutzbeauftragter zu sorgen.

›Kollektivrechtlich‹, also durch den Betriebsrat, können personaldatenverarbeitende Systeme und damit Erfassung, Verarbeitung, Auswertung und Verwendung von personenbezogenen Daten im Rahmen von Betriebsvereinbarungen geregelt werden. Der Betriebsrat greift dabei auf die einschlägigen Informations-, Beratungs- und Mitbestimmungsrechte des Betriebsverfassungsgesetzes zurück.

Zusammen gesehen gibt es bei der Umsetzung und Überwachung des Arbeitnehmer-Datenschutzes also erhebliche Berührungspunkte zwischen den Aufgaben des betrieblichen Datenschutzbeauftragten und den Aufgaben des Betriebsrats. Deshalb muß es im Interesse der Betriebsräte liegen, sich mit der Person und den Aufgaben des betrieblichen Datenschutzbeauftragten, aber natürlich auch mit ihren eigenen Aufgaben im Arbeitnehmer-Datenschutz näher zu befassen.

Aufgaben des Datenschutzbeauftragten ...

Die Aufgaben des betrieblichen Datenschutzbeauftragten sind in § 37 BDSG beschrieben. Danach hat der Datenschutzbeauftragte ...

... die Ausführung des BDSG sowie anderer Rechtsvorschriften über den

Datenschutz sicherzustellen (§ 37 Abs. 1 Satz 1 BDSG);

... die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden, zu überwachen (§ 37 Abs. 1 Nr. 1 BDSG);

nahmen zu sorgen. Da der Datenschutzbeauftragte keine Weisungsbefugnis gegenüber den Beschäftigten hat, liegt die Umsetzung der entsprechenden Maßnahmen jedoch allein beim Arbeitgeber.

Der Datenschutzbeauftragte hat insbesondere ...

ÜBERSICHT 1

Bestellung des Datenschutzbeauftragten

Ein betrieblicher Datenschutzbeauftragter muß bestellt werden, wenn ...

... bei automatisierter Verarbeitung in der Regel mehr als 5 Arbeitnehmer ständig personenbezogene Daten verarbeiten;

... bei nicht-automatisierter Verarbeitung in der Regel mindestens 20 Arbeitnehmer ständig personenbezogene Daten verarbeiten.

›Ständig‹ heißt nicht ununterbrochen – der Zeitaufwand spielt keine Rolle. Es genügt, wenn die Aufgabe ›Personaldatenverarbeitung‹ nur einmal monatlich anfällt.

Persönliche Voraussetzungen

Fachkunde:

Der Datenschutzbeauftragte muß über technische, rechtliche, organisatorische und pädagogisch-didaktische Kenntnisse verfügen:

– Grundkenntnisse über Verfahren und Techniken der automatisierten Datenverarbeitung;

– allgemeine betriebswirtschaftliche und organisatorische Kenntnisse;

– allgemeine juristische Kenntnisse, besonders zum Datenschutzrecht;

– Kenntnisse über erwachsenengerechte Aus- und Fortbildung.

Zuverlässigkeit:

Neben allgemeinen und oft schwer zu bewertenden Charaktereigenschaften wie Integrität, Verschwiegenheit, Verantwortungsbewußtsein, Gründlichkeit und Durchsetzungsvermögen, gehört zur Frage der Zuverlässigkeit auch das Problem von Interessenkollisionen, die auftauchen, wenn die Datenschutzaufgaben in Konflikt kommen mit anderen beruflichen Tätigkeiten. Das trifft beispielsweise zu auf EDV-Leiter, Mitglieder der Geschäftsleitung, Personalleiter, Marketingleiter, Leiter der Rechtsabteilung.

... die Schulung des DV-Personals vorzunehmen (§ 37 Abs. 1 Nr. 2 BDSG);

... bei der Auswahl des DV-Personals mitzuwirken (§ 37 Abs. 1 Nr. 3 BDSG);

... Übersichten über die eingesetzte Hard- und Software zu führen (§ 37 Abs. 2 BDSG).

Interessant an dieser Aufzählung ist vor allem die einleitende ›Generalklausel‹, die dem Datenschutzbeauftragten nicht nur eine überwachende, sondern eine durchaus aktive Rolle zuweist – er hat für die Beachtung aller einschlägigen Datenschutzvorschriften und für die *Einleitung der hierfür erforderlichen Maß-*

... die Vorschriften des BDSG in *konkrete Verhaltensregeln für das Unternehmen* umzusetzen;

... die *Zulässigkeit der Datenverarbeitung und -nutzung* zu überprüfen (§ 4 BDSG);

... dafür zu sorgen, daß die *Individualrechte der Beschäftigten auf Benachrichtigung, Auskunft, Berichtigung, Löschung und Sperrung von Daten* beachtet werden (§§ 33 bis 35 BDSG);

... die Umsetzung und Einhaltung *technisch-organisatorischer Datenschutzmaßnahmen*, wie sie im § 9 BDSG festgelegt sind, zu überwachen.

Vor allem das Umsetzen des BDSG in konkrete Verhaltensregeln für das Unternehmen ist für betriebliche Datenschutzbeauftragte eine schwierige und auch aufwendige Aufgabe. Es muß ein umfassendes Datenschutzkonzept entwickelt werden, mit Regeln bzw. Richtlinien, nach denen sich die Verarbeitung personenbezogener Daten im Unternehmen dann zu richten hat. Zu

diesem Zweck wird in vielen Betrieben ein sogenanntes Datenschutz-Handbuch geführt, das die betriebsinternen Richtlinien und Merkblätter zum Datenschutz enthält, ergänzt durch die für das Unternehmen bedeutsamen Datenschutz-Gesetze und -Verordnungen. Dieses Datenschutz-Handbuch dient den Organisationseinheiten, die den Datenschutz umsetzen bzw. beachten müssen, als Arbeitsgrundlage.

Es sollte selbstverständlich sein, ist es in der Regel aber nicht: Der Datenschutzbeauftragte hat zu prüfen und zu gewährleisten, daß die Erhebung, Verarbeitung

und Nutzung personenbezogener Daten in jeder Verarbeitungsphase *rechtlich zulässig* ist. Dies gilt übrigens nicht nur für die Daten von Beschäftigten, sondern beispielsweise auch für die von Kunden und Lieferanten. Entscheidend dabei ist in jedem Falle der § 4 Abs. 1 BDSG, der festlegt, daß die Verarbeitung und Nutzung personenbezogener Daten *nur dann zulässig* ist, wenn ...

- ... der Betroffene eingewilligt hat,
- ... eine spezielle Rechtsvorschrift dieses erlaubt, oder
- ... das BDSG selber es zuläßt.

Zudem gilt: Die Verarbeitung und Nutzung der personenbezogenen Daten ist nur im Rahmen der Zweckbindung eines Vertragsverhältnisses oder eines vertragsähnlichen Vertrauensverhältnisses zulässig – für jede Einzelinformation, jedes ›Datum‹ muß also vom betrieblichen Datenschutzbeauftragten geprüft werden, ob ein ›gesetzlicher Erlaubnistatbestand‹ überhaupt vorliegt!

Das bezieht sich nicht nur auf die Erfassung und Verarbeitung einzelner Daten, sondern meint durchaus auch die EDV-Systeme insgesamt. Es dürfen nur solche Systeme zum Einsatz kommen, die den Schutz der Persönlichkeitsrechte der Beschäftigten gewährleisten.

Alle Möglichkeiten der unzulässigen Datenverarbeitung und die Gefährdung bzw. der Mißbrauch personenbezogener Daten müssen also durch entsprechende Datenschutzmaßnahmen verhindert werden.

Der § 9 BDSG und vor allem die Anlage zu § 9 regeln die dafür notwendigen technischen und organisatorischen Maßnahmen detailliert in Form der sogenannten ›zehn Gebote des Datenschutzes‹ (siehe Übersicht 2). Allerdings sind diese ›Gebote‹ ausdrücklich dem Prinzip der ›Verhältnismäßigkeit‹ unterstellt: Sie sind nur dann erforderlich, ›wenn der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht‹.

Damit es kein Mißverständnis gibt: Dieses Prinzip der Verhältnismäßigkeit bietet keine Möglichkeit, die vom Gesetz ausgesprochenen Ge- und Verbote zu umgehen – sie sind in jedem Falle einzuhalten –, es geht einzig und allein um Art und Umfang der technisch-organisatorischen Maßnahmen, die die Einhaltung

ÜBERSICHT 2

Die ›zehn Gebote‹ der Personaldatenverarbeitung

Zugangskontrolle	Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, in denen personenbezogene Daten verarbeitet werden, zu verwehren.
Datenträgerkontrolle	Es ist zu verhindern, daß Datenträger (z.B. Disketten) unbefugt gelesen, kopiert, verändert oder entfernt werden können.
Speicherkontrolle	Die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten ist zu verhindern.
Benutzerkontrolle	Es ist zu verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können.
Zugriffskontrolle	Es ist zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.
Übermittlungskontrolle	Es ist zu gewährleisten, daß überprüft und festgestellt werden kann, an welchen Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können.
Eingabekontrolle	Es ist zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in Datenverarbeitungssysteme eingegeben worden sind.
Auftragskontrolle	Es ist zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
Transportkontrolle	Es ist zu verhindern, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.
Organisationskontrolle	Die innerbehördliche oder innerbetriebliche Organisation ist so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird.

Zusammengestellt nach: Anlage zu § 9 Bundesdatenschutzgesetz

aller einschlägigen Rechtsvorschriften bewirken sollen.

Der Datenschutzbeauftragte hat darüber hinaus die Einhaltung anderer Rechtsvorschriften sicherzustellen, die sich mehr oder weniger direkt mit dem Datenschutz beschäftigen. Einige Beispiele dazu:

- Freie Entfaltung der Persönlichkeit (§ 75 Abs. 2 BetrVG);
- Informations-, Beratungs- und Mitbestimmungsrechte des Betriebsrats;
- Begrenzung der Fragen, die der Arbeitgeber vor und nach der Einstellung stellen darf;
- Begrenzung der persönlichen Angaben in schriftlichen Arbeitsverträgen;
- Recht auf Akteneinsicht für die Beschäftigten (§ 83 BetrVG);
- Betriebsvereinbarungen und Einigungsstellensprüche.

Schon bei diesen allgemeinen Aufgaben des betrieblichen Datenschutzbeauftragten zeigen sich weitgehende

Überschneidungen mit den Aufgaben und Rechten des Betriebsrats. Auch er hat selbstverständlich die ›freie Entfaltung der Persönlichkeit‹ zu schützen und zu fördern (§ 75 Abs. 2 BetrVG). Auch er hat nach § 80 Abs. 1 Nr. 1 BetrVG die Durchführung der ›zugunsten der Arbeitnehmer geltenden Gesetze, Verordnungen, Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen‹ zu überwachen – und dazu gehören das BDSG und andere datenschutzrechtliche Vorschriften.

Starke Überschneidungen oder – positiv formuliert – Möglichkeiten zur Kooperation liegen im Bereich des § 87 Abs. 1 Nr. 6 BetrVG, nach dem bekanntlich die ›Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen‹, der Mitbestimmung des Betriebsrats unterliegen. Ist ein EDV-System also *objektiv geeignet*, Leistung oder Verhalten der Beschäftigten zu überwachen (Näheres dazu in CI 7-8/92, ab Seite 39), wäre eine

Einführung auch nach dem BDSG unzulässig, wenn dem Betriebsrat sein Mitbestimmungsrecht verweigert wurde. Zu Beginn eines EDV-Projektes hat also der Datenschutzbeauftragte auch zu prüfen, ob der Arbeitgeber die Mitwirkungs- und Mitbestimmungsrechte des Betriebsrats beachtet hat!

Ordnungsgemäße Programmanwendung ...

Im laufenden Betrieb muß der Datenschutzbeauftragte die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme überwachen (§ 37 Abs. 1 Nr. 1 BDSG). Da in § 37 BDSG lediglich Beispiele genannt werden, die Aufgaben des Datenschutzbeauftragten jedoch sehr weitreichend sind (er hat die Ausführung des BDSG sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen), bezieht sich die Überwachung nicht nur auf die eigentliche *Verarbeitung* (§ 3 Abs. 5 BDSG), sondern auch auf das *Erheben* (§ 3 Abs. 4 BDSG) und das *Nutzen* (§ 3 Abs. 6 BDSG) personenbezogener Daten.

Hier setzt neben dem § 87 Abs. 1 Nr. 6 BetrVG ein weiteres Mitbestimmungsrecht des Betriebsrats an. Nach § 94 BetrVG bedürfen Personalfragebögen der Zustimmung des Betriebsrats. Dieses Mitbestimmungsrecht umfaßt jede schematisierte oder standardisierte Befragung von Bewerbern oder Beschäftigten über persönliche Verhältnisse, Kenntnisse und Fähigkeiten durch den Arbeitgeber – unerheblich ist, welche Hilfsmittel (Papier und/oder Computer) dafür benutzt werden. Ganz eindeutig fallen also sehr viele »Erhebungen« personenbezogener Daten (nicht nur im Rahmen von Einstellungen, sondern auch im laufenden Arbeitsverhältnis) unter dieses Mitbestimmungsrecht.

Bei alledem muß der Datenschutzbeauftragte – wie bereits erwähnt – insbesondere sicherstellen, daß datenschutzspezifische Vorschriften, wie z.B. Zulässigkeit der Datenverarbeitung, Sicherstellen der Rechte der Betroffenen, Verpflichtung auf das Datengeheimnis und technisch-organisatorische Datenschutzmaßnahmen, durchgeführt bzw. geprüft werden.

ÜBERSICHT 3

Aktuelle Anschriften der Aufsichtsbehörden für den nicht-öffentlichen Bereich:

Land	oberste Aufsichtsbehörde	regionale Aufsichtsbehörden
Baden-Württemberg	Innenministerium Baden-Württemberg Postfach 102443 W-7000 Stuttgart 1	
Bayern	Bayrisches Staatsministerium des Inneren Odeonsplatz 3 W-8000 München 22	Regierung von Oberbayern Maximilianstraße 39 W-8000 München 22 Regierung von Niederbayern Regierungsplatz 540 W-8300 Landshut Regierung der Oberpfalz Emmeransplatz 8/9 W-8400 Regensburg Regierung von Oberfranken Ludwigstraße 20 W-8580 Bayreuth Regierung von Mittelfranken Schloß W-8800 Ansbach Regierung von Unterfranken Peterplatz 9 8700 Würzburg Regierung von Schwaben Fronhof 10 8900 Augsburg
Berlin	Senator für Inneres Fehrbelliner Platz 2 W-1000 Berlin 31	
Brandenburg	Innenministerium des Landes Brandenburg Henning-von-Treskow-Straße 9–13 O-1560 Potsdam	
Bremen	Der Landesbeauftragte für den Datenschutz Arndtstraße 1 W-2850 Bremerhaven 1	
Hamburg	Der Hamburgische Datenschutzbeauftragte Baumwall 7 W-2000 Hamburg 11	
Hessen	Hessischer Minister des Inneren Friedrich-Ebert-Allee 12 W-6200 Wiesbaden	Regierungspräsident Darmstadt Luisenplatz 2 W-6100 Darmstadt Regierungspräsident Kassel Steinweg 6 W-3500 Kassel Regierungspräsident Gießen Landgraf-Philipp-Platz 1 W-6300 Gießen
Mecklenburg-Vorpommern	Innenministerium des Landes Mecklenburg-Vorpommern Karl-Marx-Straße 1 O-2710 Schwerin	
Niedersachsen	Niedersächsisches Ministerium des Inneren Lavesallee 6 W-3000 Hannover 1	
Nordrhein-Westfalen	Innenminister des Landes Nordrhein-Westfalen Haroldstraße 5 W-4000 Düsseldorf 1	Regierungspräsident Köln Zeughausstraße 4 - 8 W-5000 Köln 1 Regierungspräsident Arnberg Seibertstraße 1 W-5760 Arnberg
Rheinland-Pfalz	Ministerium des Innern Schillerplatz 3 - 5 W-6500 Mainz	Bezirksregierung Koblenz Stresemannstraße 3 - 5 W-5400 Koblenz Bezirksregierung Trier Mustorstraße 14 W-5500 Trier Bezirksregierung Rheinhessen-Pfalz Friedrich-Ebert-Straße 14 W-6730 Neustadt/Weinstraße
Saarland	Der Landesbeauftragte für den Datenschutz Franz-Dobisch-Straße 12 W-6600 Saarbrücken	
Sachsen	Staatsministerium des Innern Archivstraße 1 O-8060 Dresden	
Sachsen-Anhalt	Innenministerium des Landes Sachsen-Anhalt Postfach 1947 O-3010 Magdeburg	
Schleswig-Holstein	Innenminister des Landes Schleswig-Holstein Düsternbrookerweg 92 Landeshaus W-2300 Kiel 1	
Thüringen	Innenministerium des Landes Thüringen Schillerstraße 27 O-5085 Erfurt	

Eine Überwachung der ordnungsgemäßen Anwendung ist nur gewährleistet, wenn bestimmte Prinzipien und Regeln eingehalten werden. Hierzu zählen beispielsweise eine sorgfältige Programm-dokumentation, Funktionstrennung, das Vier-Augen-Prinzip, das automatische Führen eines ›Logbuches‹, die Dokumentation manueller Eingriffe und deren Kontrolle.

Damit Vorschläge des Datenschutzbeauftragten bei der System-Entwicklung und -Einführung auch wirklich berücksichtigt werden können, ist es notwendig, daß der Datenschutzbeauftragte – wie ja auch der Betriebsrat! – rechtzeitig (also schon in der Planungsphase) und umfassend über die einzuführende Hard- und Software unterrichtet wird.

Schulung des DV-Personals ...

Eine vordringliche Aufgabe des Datenschutzbeauftragten besteht darin, die Beschäftigten mit den Datenschutzvorschriften vertraut zu machen (§ 37 Abs. 1 Nr. 2 BDSG). Dadurch soll bei denen, die personenbezogene Daten verarbeiten, ein Bewußtsein für die Notwendigkeit des Datenschutzes geschaffen werden. Da die Durchführung der Schulungsmaßnahmen zu den *ausdrücklichen* Aufgaben des Datenschutzbeauftragten gehört, hat dieser *selbst* – unter Berücksichtigung der betrieblichen Gegebenheiten – zu bestimmen, was die geeigneten Schulungsmaßnahmen sind. Der Arbeitgeber hat hierfür die erforderlichen Sachmittel und Räumlichkeiten zur Verfügung zu stellen.

Datenschutz-Schulungen sind unter anderem auch eine wesentliche Voraussetzung für die Verpflichtung der betroffenen Beschäftigten auf das Datengeheimnis (§ 5 BDSG). Diese offizielle Verpflichtung kann und soll deshalb nur nach einer entsprechenden Schulung erfolgen.

Auch diese Aufgabe des Datenschutzbeauftragten wird durch ein Mitbestimmungsrecht des Betriebsrats berührt. Da die Vermittlung von Datenschutz-Wissen zu den *notwendigen* Bestandteilen der Aus- und Fortbildung gehört, handelt es sich dabei um Bildungsveranstaltungen im Sinne der §§ 96 bis 98 BetrVG – das

ÜBERSICHT 4

Fragenkatalog zum betrieblichen Datenschutz

Nr. Frage	Rechtliche Grundlage
1. Ist ein Text des Bundesdatenschutzgesetzes (BDSG) im Betrieb verfügbar, um die wesentlichen Normen nachlesen zu können?	BGBl I Nr. 73 vom 29. 12. 1990, Seite 2954 ff
2. Sind die zusätzlich notwendigen speziellen Gesetze vorhanden – z.B. Abgabenordnung, Sozialgesetzbücher, Zivilprozeßordnung, Arbeits- und Steuergesetze?	§ 1 Abs. 4 und § 4 Abs. 1 BDSG
3. Wurde eine Erhebung über die Aufzeichnungen (Unterlagen, Karteien, Ablagen, Dateien), die Daten natürlicher Personen (z.B. Beschäftigte, Kunden, Lieferanten) enthalten, in allen Abteilungen des Betriebes veranlaßt, durchgeführt und ausgewertet, um festzustellen, ob und wo Dateien im Sinne des BDSG vorhanden und Schutz- und Sicherungsmaßnahmen zu treffen sind?	§§ 1, 3, 37 BDSG
4. Wurde festgelegt, wer für die Aufzeichnung und die Verarbeitung dieser Daten zuständig und verantwortlich ist, und wurden diese Mitarbeiter auf das Datengeheimnis verpflichtet?	§ 5 BDSG
5. Sind die verpflichteten oder zu verpflichtenden Mitarbeiter und deren Vorgesetzte, die Umgang mit personenbezogenen Daten haben, ausreichend über das BDSG und den Datenschutz informiert?	§§ 5, 37 BDSG
6. Ist die Zulässigkeit der Verarbeitung geschützter personenbezogener Daten anhand der Erlaubniskriterien für die einzelnen Datenverarbeitungsphasen (Speichern, Übermitteln an Dritte, Verändern, Löschen und Sperren) und die Nutzung dieser Daten geprüft und sichergestellt, oder müssen Maßnahmen eingeleitet werden, die die Zulässigkeit der Verarbeitung weiterhin gewährleisten?	§ 1 Abs. 4 BDSG in Verbindung mit §§ 28, 35 BDSG
7. Wurden die Betroffenen über den Tatbestand der Speicherung ihrer Daten benachrichtigt, oder ist geprüft und sichergestellt, daß sie auf andere Weise von der Speicherung Kenntnis erlangt haben?	§ 33 BDSG
8. Wurden den zuständigen Mitarbeitern und Vorgesetzten eindeutige Verhaltensregeln gegeben für den Fall, daß Betroffene ihre Rechte wahrnehmen?	§§ 6, 34, 35 BDSG
Sind bereits Auskunftsbegehren vorgekommen und wie wurden sie abgewickelt?	§ 34 BDSG
Wurde die Berichtigung, Sperrung oder Löschung von Daten gefordert?	§ 35 BDSG
9. Sind die Verträge mit Auftragnehmern, die Datenverarbeitung für den Betrieb durchführen (z.B. Service-Rechenzentrum) der Rechtslage durch schriftliche Vertragsstatuten angepaßt?	§ 11 BDSG
10. Für den Fall, daß es einen Datenschutzbeauftragten noch nicht gibt: Wurde geprüft, ob ein Datenschutzbeauftragter zu bestellen ist?	§ 36 BDSG

angelehnt an: GDD; Datenschutz und Datensicherung im Unternehmen, Köln 1992, Seite 71

heißt: Mitbestimmung nach § 98 BetrVG. Und das wiederum bedeutet: Diese Maßnahmen dürfen nicht einseitig vom Arbeitgeber bzw. vom Datenschutzbeauftragten durchgeführt werden – sie bedürfen der Zustimmung des Betriebsrats, der auf diesem Weg auf die Schulungsinhalte und die Auswahl der Teilnehmer Einfluß nehmen kann. Auch der Betriebsrat kann an diesen Schulungen teilnehmen, ohne daß das seine Ansprüche auf eigene Schulungen nach § 37 Abs. 6 BetrVG berühren würde.

Auswahl des DV-Personals ...

Der Datenschutzbeauftragte hat ›beratend mitzuwirken‹ auch bei der Auswahl der Personen, die mit der Verarbeitung personenbezogener Daten beschäftigt sind (§ 37 Abs. 1 Nr. 3 BDSG). Dieses Mitwirkungsrecht bezieht sich dabei sowohl auf die Einstellung von Personal wie auch auf die Umsetzung von Beschäftigten. Die Vorschrift beschränkt hier die Mitwirkung des Datenschutzbeauftragten ausdrück-

lich auf eine Beratung. Er hat keineswegs darüber zu entscheiden, wer überhaupt für die Datenverarbeitung in Betracht kommt – ein wie immer auch verstandenes ›Vetorecht‹ hat er also nicht. Vielmehr ist die Personalentscheidung letztendlich Sache des Arbeitgebers.

In dieser Frage gehen die Rechte des Betriebsrats (etwas) weiter. Denn nach § 99 Abs. 2 BetrVG hat der Betriebsrat immerhin das Recht, unter bestimmten Umständen seine Zustimmung zu einer Einstellung oder Versetzung zu verweigern. Beispielsweise dann, wenn er die begründete Befürchtung hat, daß eine für die Personaldatenverarbeitung vorgesehene Person durch ›gesetzwidriges Verhalten‹ den ›Betriebsfrieden‹ stören würde. Begründet könnte diese Befürchtung dann sein, wenn jemand an einem anderen Arbeitsplatz bereits schwerwiegendere datenschutzrechtliche Verstöße begangen hat.

Es handelt sich bei § 37 Abs. 1 Nr. 3 BDSG jedoch nicht nur um ein Recht, sondern vielmehr um eine *Pflicht* des Datenschutzbeauftragten, bei der Personalauswahl mitzuwirken. Dabei sollte sich die Mitwirkung nicht allein auf die Erstellung von Auswahlrichtlinien beschränken – die nach § 95 Abs. 1 BetrVG wiederum der Mitbestimmung durch den Betriebsrat unterliegen! –, sondern sich auch auf jede einzelne Personalmaßnahme beziehen. Dieses kann in der Weise geschehen, daß dem Datenschutzbeauftragten Bewerbungsunterlagen, Zeugnisse usw. vorgelegt werden. Zudem kann er ein Gespräch mit dem Bewerber führen.

Je bedeutsamer die zu besetzende Stelle unter Verarbeitungsgesichtspunkten ist, desto wichtiger ist die Beteiligung des Datenschutzbeauftragten.

Führen von Übersichten ...

Von großer Bedeutung auch und gerade im Hinblick auf die Informations- und Mitwirkungsrechte *des Betriebsrats* ist die in § 37 Abs. 2 BDSG enthaltene Regelung, nach der dem Datenschutzbeauftragten vom Arbeitgeber ›Übersichten‹ zur Verfügung zu stellen sind, und zwar über ...

DOKUMENTATION

Betriebsvereinbarung zum betrieblichen Datenschutzbeauftragten

Ziele

Geschäftsleitung und Betriebsrat stimmen darin überein, daß durch den Abschluß dieser Betriebsvereinbarung folgende Ziele erreicht werden sollen:

- Sicherstellung der Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz (z.B. Betriebsvereinbarungen).
- Einvernehmliche Regelungen bezüglich eines betrieblichen Datenschutz-Konzeptes.
- Enge Kooperation zwischen dem Datenschutzbeauftragten und der Interessenvertretung.

Bestellung und Abberufung

Die Bestellung und Abberufung/Kündigung des Datenschutzbeauftragten wird einvernehmlich mit dem Betriebsrat geregelt.

Der Datenschutzbeauftragte ist unmittelbar der Geschäftsleitung unterstellt. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden.

Persönliche Voraussetzungen

Der Datenschutzbeauftragte muß im Rahmen der geforderten Fachkunde über technische, rechtliche und organisatorische Kenntnisse verfügen. Das bedeutet im einzelnen:

- Grundkenntnisse der automatisierten Datenverarbeitung;
- allgemeine betriebswirtschaftliche Kenntnisse und Kenntnisse der Betriebsorganisation;
- Kenntnisse des Datenschutzes und sonstiger damit zusammenhängender Rechtsvorschriften;
- pädagogisch-didaktische Fähigkeiten.

Ein Datenschutzbeauftragter, der bei seiner Bestellung noch nicht über die notwendigen Qualifikationen verfügt, muß diese unverzüglich durch Schulungsmaßnahmen erwerben.

Bezüglich der Zuverlässigkeit des Datenschutzbeauftragten sind folgende Bedingungen zu erfüllen:

- keine vorherigen Verstöße gegen die Datenschutzvorschriften;
- Vermeidung von Interessenkollisionen aufgrund der Ausübung anderer betrieblicher Funktionen.

Aufgaben

Der betriebliche Datenschutzbeauftragte ist bei der Wahrnehmung seiner Aufgaben weisungsfrei. Er ist jedoch verpflichtet, entsprechenden Hinweisen aller Beteiligten nachzugehen und dem Betriebsrat und der Geschäftsleitung Bericht über die Erledigung der Hinweise zu geben.

Der Datenschutzbeauftragte hat mindestens einmal jährlich in der Betriebsversammlung einen Bericht über seine Tätigkeit einschließlich seiner Funktion abzugeben.

Der Datenschutzbeauftragte darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden.

Dem Datenschutzbeauftragten unterliegen folgende allgemeine Kontrollaufgaben:

- Überwachung des ordnungsgemäßen Einsatzes der DV-Programme;
- Sicherstellung der Einweisung und Verpflichtung der mit der Verarbeitung personenbezogener Daten befaßten Mitarbeiter;
- Gewährleistung der Rechte der Beschäftigten auf Benachrichtigung, Auskunft, Berichtigung, Löschung und Sperrung von beanstandeten Daten.

Zudem hat er insbesondere folgende Einzelaufgaben zu erfüllen:

- Führung der Datenübersichten;
- Mitwirkung bei der Auswahl von DV-Personal;
- Schulung des DV-Personals im Umgang mit personenbezogenen Daten;
- Einschalten der Aufsichtsbehörde bei Verstößen.

Zusammenarbeit mit der Interessenvertretung

Die vom Datenschutzbeauftragten im Zusammenhang mit der Auswahl des DV-Personals erstellten Auswahlrichtlinien unterliegen der Mitbestimmung des Betriebsrats. Inhalte, Umfang und Teilnehmer der vorgesehenen Schulungen werden einvernehmlich mit dem Betriebsrat abgesprochen.

Der Vorsitzende des Betriebsrats nimmt in Absprache mit dem Datenschutzbeauftragten eine Verpflichtung der Betriebsratsmitglieder auf das Datengeheimnis gemäß BDSG vor.

Betriebsrat und Datenschutzbeauftragter arbeiten wegen der gleichgelagerten Aufgabenstellung im Arbeitnehmer-Datenschutz vertrauensvoll zusammen, insbesondere bei dem Austausch von Informationen und bei der gegenseitigen Beratung.

Der Datenschutzbeauftragte unterliegt in bezug auf alle Informationen, die er vom Betriebsrat erhält, der Schweigepflicht gegenüber der Geschäftsleitung.

... eingesetzte Datenverarbeitungsanlagen,
... Bezeichnung und Art der Dateien,
... Art der gespeicherten Daten,
... Geschäftszwecke, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist,
... deren regelmäßige Empfänger und zugriffsberechtigte Personengruppen oder Personen, die allein zugriffsberechtigt sind.

Diese Verpflichtung ist für den Betriebsrat in zweierlei Hinsicht wichtig:

1. Der Betriebsrat kann sich auf diese Verpflichtung zur Führung von Übersichten berufen, wenn ihm gegenüber behauptet wird, Unterlagen dieser Art gebe es gar nicht – sollte das stimmen, wäre es ein eindeutiger Verstoß gegen das BDSG.
2. Diese Übersichten entsprechen in Form und Inhalt weitgehend den Hardware-, Software- und Datenkatalogen, die fester Bestandteil aller Betriebsvereinbarungen sind, in denen die Einführung personaldatenverarbeitender Systeme geregelt wird.

Das heißt jedoch nicht, daß diese Übersichten vom Betriebsrat einfach in Betriebsvereinbarungen übernommen werden sollten. Sie können aber eine wesentliche Grundlage für die Entwicklung eigener Vorstellungen und Forderungen sein und eignen sich auch, um die Einhaltung bereits abgeschlossener Betriebsvereinbarungen zu kontrollieren.

So gesehen ist es für den Betriebsrat nicht ohne Interesse, ob und wie diese Übersichten erstellt und gepflegt werden. Zwei positive Beispiele sind auf der Seite 28 abgebildet. Die Übersichten sind vom betrieblichen Datenschutzbeauftragten selbstverständlich auf ihre Richtigkeit zu prüfen und jeweils auf dem aktuellen Stand zu halten.

Übersichten über nur vorübergehend erstellte, sogenannte ›temporäre‹ Dateien müssen nach Bundesdatenschutzgesetz *nicht* geführt werden, wenn die Dateien innerhalb von drei Monaten nach ihrer Erstellung wieder gelöscht werden (§ 37 Abs. 3 BDSG) – was allerdings nicht heißt, daß der Betriebsrat nicht auch in diesen Fällen seine ›üblichen‹ Informations- und Beteiligungsrechte hätte. Trotzdem

leistet diese neu in das BDSG aufgenommene Regelung, insbesondere vor dem Hintergrund des verstärkten PC-Einsatzes in den Unternehmen, einem möglichen Mißbrauch mit personenbezogenen Daten Vorschub.

Praktische Schritte zur Kooperation ...

Aus dem bisher Dargestellten wird deutlich, daß in bezug auf den Arbeitnehmer-Datenschutz starke Überschneidungen der Aufgaben des betrieblichen Datenschutzbeauftragten mit den Aufgaben des Betriebsrats existieren. So wird in diesem Zusammenhang auch von einer ›doppelten Kontrollkompetenz‹ gesprochen. Dies legt – wie gesagt – eine Zusammenarbeit nahe. Weder das BDSG noch das Betriebsverfassungsgesetz enthalten jedoch Regelungen über das Verhältnis zwischen Datenschutzbeauftragtem und Betriebsrat.

Trotzdem wird überwiegend angenommen, daß beide Seiten in Fragen des Arbeitnehmer-Datenschutzes eng zusammenarbeiten *sollten*. Dabei kann der Betriebsrat unterschiedliche Wege beschreiben, die von den betrieblichen Gegebenheiten, aber auch von der Person des Datenschutzbeauftragten abhängen.

Erkundigungen zum betrieblichen Datenschutzbeauftragten

Der Betriebsrat erkundigt sich bei den monatlichen Besprechungen mit dem Arbeitgeber zunächst einmal, ob es im Betrieb einen betrieblichen Datenschutzbeauftragten gibt. Ist dies nicht der Fall, prüft er, ob die Voraussetzungen des § 36 Abs. 1 BDSG für eine Bestellung gegeben sind (siehe Übersicht 1). Sind die Voraussetzungen erfüllt, sollte der Betriebsrat den Arbeitgeber schriftlich auffordern, eine geeignete Person zu benennen. Folgt der Arbeitgeber dieser Aufforderung nicht, kann der Betriebsrat nach § 38 BDSG die Aufsichtsbehörde für den Datenschutz anrufen (Adressen in Übersicht 3). Das gleiche gilt, wenn eine Person zum Datenschutzbeauftragten bestellt wurde, die die Anforderungen an die vom Gesetz geforderte Fachkunde und Zuverlässigkeit nicht erfüllt (Übersicht 1).

Besonders häufig wird in der Praxis gegen das Kriterium der *Zuverlässigkeit* verstoßen, wenn Personen zu Datenschutzbeauftragten bestellt werden, die aufgrund ihrer anderen, betrieblichen Tätigkeiten in Interessenkonflikte kommen könnten – was dann zu Lasten des Datenschutzes gehen würde. Aus diesem Grund sollten Mitglieder der Geschäftsleitung, EDV-Leiter, Personalleiter, Leiter der Rechtsabteilung u.ä. *nicht* zu Datenschutzbeauftragten bestellt werden. Die Aufsichtsbehörde für den Datenschutz würde in einem solchen Fall dem Arbeitgeber auferlegen, eine rechtmäßige Bestellung vorzunehmen bzw. einen ungeeigneten Datenschutzbeauftragten abzulösen. Wird ein Datenschutzbeauftragter nicht bestellt, oder wird jemand bestellt, dem ›Fachkunde‹ und/oder ›Zuverlässigkeit‹ fehlen, handelt das entsprechende Unternehmen ordnungswidrig und kann mit einer Geldbuße bis zu 50 000,- DM belegt werden.

Kontaktaufnahme mit dem Datenschutzbeauftragten

Ist im Betrieb die Stelle eines Datenschutzbeauftragten besetzt, sollte von Seiten des Betriebsrats so bald wie möglich ein Gesprächstermin vereinbart werden. Zur Vorbereitung der Kontaktaufnahme sollte dem Datenschutzbeauftragten vorab ein Fragenkatalog übermittelt werden. Dabei kann sich der Betriebsrat an dem von der Gesellschaft für Datenschutz und Datensicherung entwickelten Fragenkatalog orientieren (Übersicht 4). Ein solcher Fragenkatalog sollte vom Arbeitgeber bzw. dem betrieblichen Datenschutzbeauftragten schriftlich beantwortet und in einer gemeinsamen Sitzung dann Punkt für Punkt durchgesprochen werden. Aufgrund dieses Verfahrens wird der Betriebsrat dann sowohl die Qualifikation des betrieblichen Datenschutzbeauftragten wie auch seine (geplanten) Aktivitäten zum Datenschutz erkennen und beurteilen können.

Absprachen über eine Zusammenarbeit

Als Beginn der Zusammenarbeit zwischen Betriebsrat und Datenschutzbeauftragtem sollten dem Betriebsrat alle Unterlagen, die zum Arbeitnehmer-Datenschutz existieren, in Kopie überlassen

- *einvernehmliche* Bestellung und Abberufung des Datenschutzbeauftragten;
- Pflicht zur umfassenden Berichterstattung gegenüber der Interessenvertretung und den Beschäftigten;
- enge Zusammenarbeit bei Betriebsvereinbarungen zu EDV-Systemen.

Das bedeutet, daß die Verhandlung über eine solche Vereinbarung wohl nicht ohne Konflikte über die Bühne gehen dürfte. Die Chancen des Betriebsrats, sich mit seinen Vorstellungen durchzusetzen, sind dann besonders gut, wenn ...

- ... Kontaktaufnahme und Kooperation mit dem betrieblichen Datenschutzbeauftragten bisher positiv verlaufen sind;
- ... die Verhandlungen im Zusammenhang mit anderen Betriebsvereinbarungen zum EDV-Einsatz geführt werden, bei denen der Betriebsrat ein *Mitbestimmungsrecht* hat.

Da es sich nicht um eine erzwingbare Betriebsvereinbarung handelt, sollte der Betriebsrat seinen Verhandlungsspielraum vorab genau festlegen. Sind wichtige (über die gesetzlichen Bestimmungen hinausgehende) Punkte nicht durchzusetzen, sollte eventuell auf den Abschluß der Betriebsvereinbarung ganz verzichtet werden.

Ob in der betrieblichen Praxis eine Zusammenarbeit mit dem betrieblichen Datenschutzbeauftragten realisiert werden kann, wird nur der praktische Versuch zeigen. Dabei können die hier dargestellten Punkte als Anregungen für die Bemühungen des Betriebsrats dienen. Ein ernsthafter Versuch jedenfalls lohnt sich, denn im Erfolgsfall können die Aktivitäten des Betriebsrats zur Umsetzung und Kontrolle des Arbeitnehmer-Datenschutzes erheblich erleichtert werden. Umgekehrt würde aber auch der Arbeit des Datenschutzbeauftragten durch eine enge Zusammenarbeit mit dem Betriebsrat größerer Nachdruck verliehen.

Manfred Schuhr
TBS Niedersachsen
Bruno Schierbaum
BTQ Oldenburg