Datenschutz im Betrieb

Thema: Betriebsrat und Arbeitgeber haben die Aufgabe nach § 75 Abs. 2 BetrVG die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Diese gesetzliche Vorgabe stellt nicht nur auf die Abwehr möglicher Gefahren ab, sondern verpflichtet die Betriebsparteien, sich aktiv für den Datenschutz der Beschäftigten einzusetzen. Vor diesem Hintergrund muss der Betriebsrat die wichtigsten Vorgaben zum Datenschutz, nämlich das Bundesdatenschutzgesetz (BDSG) und das Betriebsverfassungsgesetz (BetrVG), kennen.

Inhaltsübersicht

Autor: Bruno Schierbaum (geb. 1955), Diplom-Sozialwirt, Coach und Mediator. Er arbeitet seit 1990 bei der BTQ Niedersachsen und berät und schult für Betriebs- und Personalräte. Seine Arbeitsschwerpunkte sind Technik-, Organisations- und Datenschutzberatung.

Persönlicher Kontakt: BTQ Niedersachsen, Donnerschweer Str. 84, 26123 Oldenburg; Tel: 04 41/8 20 68; E-Mail: schierbaum@btq.de

1 Begriff

Datenschutz

In Bezug auf den **Datenschutz** hört man häufig folgende Sätze: „Das kann ich Ihnen leider nicht sagen, fällt unter Datenschutz", „Wer nichts zu verbergen hat, braucht keinen Datenschutz", „Datenschutz ist Täterschutz" oder „Datenschutz legt den ganzen Betrieb lahm". Diese Sätze zeigen, dass auch über dreißig Jahre nach Verabschiedung des ersten BDSG in Deutschland der Datenschutz immer noch erhebliches Unbehagen auslöst und soweit ersichtlich in vielen Betrieben **eher einen geringen Stellenwert** besitzt.

Gemäß BDSG ist Ziel und Zweck des Datenschutzes, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Geschütztes Rechtsgut ist der Schutz der Persönlichkeitsrechte und vor allem in seiner Ausprägung des Rechts auf informationelle Selbstbestimmung. Dieses bedeutet, dass der Einzelne selbst entscheiden kann, welche personenbezogenen Daten er von sich weitergeben will. Dieses informationelle Selbstbestimmungsrecht kann nur durch Gesetz oder Einwilligung des Einzelnen eingeschränkt werden.

Schutz der Persönlichkeitsrechte

Lässt man sich bei der Frage nach dem Wesen und der Funktion des Datenschutzes von dem **Begriff „Datenschutz"** leiten, kann man leicht in die Irre geführt werden. Denn ausgehend von dem Begriff selbst könnte man zu dem Schluss kommen, es gehe um den Schutz von Daten als solche. Erst über den Zweck des Datenschutzes und den damit vom Gesetzgeber verfolgten Ziel kommt man zu einer vollständigen und zutreffenden Erschließung des Begriffs. **Zweck des Datenschutzes** ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Geschütztes Rechtsgut sind demnach nicht die Daten selbst, sondern geschütztes Rechtsgut ist der **Schutz der Persönlichkeitsrechte.**

1.1 Datenschutz als Recht auf informationelle Selbstbestimmung

Informationelles Selbstbestimmungsrecht

Grundlegend für die Bestimmung des Begriffs und des Ziels des Datenschutzes ist das **Urteil des Bundesverfassungsgerichts** aus dem Jahre 1983 zur Volkszählung, auch kurz „Volkszählungsurteil" genannt (vgl. BVerfG v. 15.12.1983, Neue Juristische Wochenschrift 8/84, S. 422 ff.). Das Gericht hat aus Artikel 1 und Artikel 2 GG ein **Recht jedes Einzelnen auf informationelle Selbstbestimmung** abge-

leitet. Das BVerfG hat das Anliegen des Datenschutzes in den ersten beiden Leitsätzen des Volkszählungsurteils folgendermaßen formuliert:

„1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten vom allgemeinen **Persönlichkeitsrecht** des **Art. 2 I i.V. mit Art. 1 Abs. 1 GG** umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des einzelnen, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

2. Einschränkungen dieses Rechts auf informationelle Selbstbestimmung sind im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsmäßigen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Bei seinen Regelungen hat der Gesetzgeber den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung der Persönlichkeitsrechte entgegenwirken."

Das BVerfG leitet aus **Artikel 1 und Artikel 2 GG** die Befugnis des Einzelnen ab, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden". Dieses Recht nennt das BVerfG „Recht auf informationelle Selbstbestimmung". Soll dieses Recht auf informationelle Selbstbestimmung eingeschränkt werden, ist der Gesetzgeber gefragt.

1.2 Folgen für den Gesetzgeber

Der Einzelne muss **Einschränkungen** des Rechts auf informationelle Selbstbestimmung im „überwiegenden Allgemeininteresse" hinnehmen. Dieses gilt jedoch nur unter bestimmten Umständen, von denen die nachfolgenden besonders hervorzuheben sind:

Gesetzliche Grundlage

- Die Einschränkung des Rechts auf informationelle Selbstbestimmung bedarf einer gesetzlichen Grundlage (**Vorbehalt eines Gesetzes**).
- Daraus müssen sich entsprechend dem **Grundsatz der Normenklarheit** die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben.
- Diese Rechtsnorm muss dem **Grundsatz der Verhältnismäßigkeit** (Geeignetheit, Erforderlichkeit) genügen.

- Es müssen **organisatorische und verfahrenstechnische Regelungen** zum Schutz der Betroffenen aufgestellt werden (z.B. Auskunfts- und Löschungsfristen, Existenz unabhängiger Datenschutzbeauftragter).
- Die Rechtsnorm muss eine **präzise Bestimmung des Verwendungszwecks** enthalten, woraus folgt, dass weder eine Vorratsspeicherung noch eine Verwendung bzw. Verarbeitung entgegen den gesetzlichen Zwecken erfolgen darf (Grundsatz der Zweckbindung).

Recht auf informationelle Selbstbestimmung

Inhalt Befugnis des Einzelnen, grundsätzlich selbst über Preisgabe und Verwendung persönlicher Angaben zu entscheiden (informationelles Selbstbestimmungsrecht)
Einschränkung „Recht auf informationelle Selbstbestimmung“ ❑ nur im überwiegenden Allgemeininteresse ❑ nur durch normenklares, verfassungsgemäßes Gesetz ❑ nur mit begleitenden organisatorischen und verfahrensrechtlichen Regelungen
Das bedeutet insbesondere: ❑ Zweckbindung und Zweckbestimmung ❑ Minimum an Daten (keine Vorausspeicherung) ❑ Transparenz ❑ Kontrolle durch unabhängige Datenschutzbeauftragte

Ein Gesetz, das die Erhebung, Verarbeitung und Nutzung personenbezogener Daten regelt, ist das **BDSG**. Daneben gibt es ca. 100 Bundesgesetze, in denen ebenfalls Regelungen zum Datenschutz enthalten sind.

Fazit

Zweck des Datenschutzes ist es, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Insbesondere durch das vom BVerfG im Volkszählungsurteil herausgestellte Recht auf informationelle Selbstbestimmung kann die Erhebung, Verarbeitung und Nutzung personenbezogener Daten auf der Basis einer gesetzlichen Vorgabe oder durch Einwilligung des Betroffenen erfolgen.

2 Sicht des Arbeitgebers

Das Bestreben des Arbeitgebers ist es, **mit Hilfe von Informations- und Kommunikationstechniken möglichst viele personenbezogene Daten zu erheben, zu verarbeiten und auszuwerten.** So werden in Personalbereich zur Lohn- und Gehaltsberechung, zur Personalplanung, Personalentwicklung und zur Personaleinsatzplanung sowohl Personalstammdaten, Qualifikationsdaten oder auch Abwesenheitsdaten mit Gründen gespeichert. Zudem haben Arbeitgeber ein Interesse daran, u.a. die Telefon-, Internet und E-Mail-Nutzung der Beschäftigen unter **Kostengesichtpunkten** zu überwachen. Absicherungen des Betriebsgeländes, der Gebäude oder auch der Parkplätze werden ebenfalls durch technische Geräte wie Zugangskontrollsysteme oder Videoüberwachung vorgenommen.

§ 75 Abs. 2 BetrVG

Bei jeglicher Erhebung, Verarbeitung oder Nutzung personenbezogener Daten **muss der Arbeitgeber den Datenschutz aller Beschäftigten zwingend zu beachten.** Dieser Auftrag leitet sich aus dem BetrVG her: Der Arbeitgeber hat nach die freie Entfaltung der Persönlichkeit der Beschäftigten zu schützen und zu fördern.

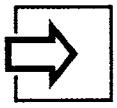
Dieses bringt für den Arbeitgeber eine **Fülle an Aufgaben** mit sich. So müssen die Vorgaben des BDSG in die Praxis umgesetzt werden. Er wird dabei unterstützt durch **den betriebliche Datenschutzbeauftragten**, wobei die Verantwortung für den Datenschutz beim Arbeitgeber verbleibt.

Folgende Aufgaben, die der Arbeitgeber umsetzen muss, erfordern auch personelle Kapazitäten

- Prüfung der Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten
- Vorabkontrolle
- Datenvermeidung und Datensparsamkeit
- technische und organisatorische Datenschutzmaßnahmen.

Daneben muss der Arbeitgeber **den Betriebsrat einbinden,** da sich aus dem BetrVG Informations-, Beratungs-, Überwachungs- und Mitbestimmungsrechte in Bezug auf den Datenschutz ableiten lassen. In diesem Zusammenhang sollte der Arbeitgeber im Einzelfall Betriebsvereinbarungen entwickeln und dadurch die Rechtmäßigkeit der Verarbeitung von Mitabeiterdaten gewährleisten.

Fazit



Die sorgfältige Umsetzung des Datenschutzes mindert das Risiko in Bezug auf Schadensersatzklagen einzelner Personen. Zudem kann der Arbeitgeber die Umsetzung des Datenschutzes auch in seiner Außendarstellung werbewirksam einsetzen.

3 Auswirkungen auf die Arbeitnehmer

Vor allem mit dem **zunehmenden Technikeinsatz**, der alle Bereiche des Arbeitslebens erfasst, ist ein **hohes Kontrollpotenzial** verbunden, und gleichzeitig ist gerade bei technischer Kontrolle der Schutz der Persönlichkeitsrechte der Beschäftigten berührt. So können mithilfe von Personalabrechungs- und -informationssystemen, mit Betriebsdatenerfassungssystemen in Produktionsbetrieben, Kundenbetreuungsprogrammen bei Banken und Versicherungen, Videoüberwachungs-, Zeiterfassungs- und Zugangskontrollsystemen und modernen Telefonanlagen **das Verhalten und/oder die Leistung der Beschäftigten überwacht** werden. Zudem können in der Regel Systemadministratoren alle Daten und Informationen zur Kenntnis nehmen, die über das betriebliche Netzwerk laufen. Mit bestimmter Software können sie über einen Fernzugriff (Remote Access) auf die PCs und Daten einzelner Beschäftigter zugreifen, Inventarisierungen von Hard- und Software vornehmen oder auch Software installieren.

Kontrolle

So sind die Folgen und die besondere Qualität der Kontrolle für die Beschäftigten beim Einsatz von IuK-Techniken vom Bundesarbeitsgericht bereits 1983 – also noch zu Zeiten der Großrechner – dargestellt worden.

Nach Auffassung des Bundesarbeitsgerichts hat der Einsatz der elektronischen Datenverarbeitung eine neue Qualität der Kontrolle und im Gegensatz zur Kontrolle durch den Menschen vor allem zur Folge, dass

- die Informationen nicht nur stichprobenweise, sondern **kontinuierlich erhoben** werden können,
- die Kontrolle für den betroffenen Arbeitnehmer häufig gar **nicht wahrnehmbar** ist, sodass Gegenreaktionen oder ein bei Kontrolle durch Menschen immer möglicher Entzug dieser Kontrolle ausscheiden,

Kontextverlust

- die Daten zu unrichtigen Beurteilungen führen, weil nicht alle Umstände des Einzelfalls erfasst werden, was zu einem **Kontextverlust der Daten** führt,
- ein **vollständiges Persönlichkeitsbild** erstellt wird, wobei der Kontextverlust der Daten die Fehleranfälligkeit erhöht,
- der einzelne Arbeitnehmer die **Kontrolle nicht verhindern kann**,

Belastungsmaterial

- die einmal **erfassten Daten auf Dauer gespeichert** werden und so auch dann noch als Belastungsmaterial verwendet werden können, wenn sie ein menschlicher Kontrolleur längst vergessen hätte,
- der Entscheidungsspielraum für die Personalabteilung immer kleiner wird, da die EDV bereits **schwer zu entkräftende Vorentscheidungen** getroffen hat (vgl. BAG, Beschluss v. 6.12.1983, Entscheidungssammlung zum Arbeitsrecht § 87 BetrVG, Bildschirmarbeitsplätze Nr. 1, S. 37 f.).

3.1 Anwendungsbereich des BDSG

Der Datenschutz der Beschäftigten und damit auch die Beschränkung der Verarbeitung personenbezogener Daten auf das betrieblich zwingend erforderliche Maß kann auf zwei verschiedenen Wegen gestaltet und abgesichert werden:

BDSG

- durch die Regelungen im **BDSG** zum Umgang mit personenbezogenen Daten, die der Arbeitgeber im individualrechtlichen Verhältnis zu beachten hat,

BetrVG

- durch kollektivrechtliche Zulässigkeitsregeln zum Arbeitnehmer-Datenschutz im Rahmen von **Betriebsvereinbarungen**, wobei diese Vereinbarungen auf den **Mitbestimmungsrechten des BetrVG** beruhen.

Personenbezogene Daten

Das BDSG regelt den **Umgang mit personenbezogenen Daten** und bildet somit die zentrale gesetzliche Basis für die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten.

Nicht öffentliche Stellen

Das BDSG nennt als **Adressaten** die öffentlichen Stellen des Bundes und die so genannten **nicht öffentlichen Stellen**. Bei Einrichtungen, in denen Betriebsräte gewählt werden, handelt es sich in der Regel um nicht öffentliche Stellen, die im BDSG auch als verantwortliche Stellen bezeichnet werden.

Nicht öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts. Zu diesen Stellen gehören natürliche Personen als Privatpersonen oder in Ausübung einer selbstständigen Tätigkeit (Einzelbetrieb, freie Berufe). Mitumfasst sind alle privatrechtlich organisierten Unternehmen in allen Rechtsformen, wie z.B. AG, GmbH, GmbH & Co KG, KGaA, OHG, KG, Genossenschaften, Stiftungen und die privatrechtlich organisierten Personenvereinigungen, wie z.B. Vereine, Verbände und politische Parteien.

Anwendung

Für diese nicht öffentlichen Stellen **kommt das BDSG zur Anwendung**, soweit sie

- **personenbezogene Daten** unter Einsatz von Datenverarbeitungsanlagen **verarbeiten**, **nutzen** oder für eine **automatisierte Verarbeitung erheben**,
- personenbezogene Daten in oder aus **nicht-automatisierten Dateien** verarbeiten, nutzen oder dafür erheben.

D

Personenbezogene Daten

Voraussetzung für die Anwendung des BDSG ist die Verwendung personenbezogener Daten. Personenbezogene Daten sind nach der Definition des § 3 Abs. 1 BDSG „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person." Diese natürliche Person wird im BDSG „Betroffener" genannt und kann seine Rechte nach dem BDSG in den jeweils unterschiedlichen Rollen, wie z.B. als Beschäftigter, Bewerber um einen Arbeitsplatz, als Bürger, Kunde, Patient oder Klient, wahrnehmen. Personenbezogene Daten sind alle Daten, die einer Person zugeordnet werden können und in irgendeiner Form Aussagen zu einer Person machen. Dazu gehören z.B. die Personalstammdaten, aber Daten über erbrachte Arbeitsleistungen, Daten über Telefon-, Internet- und E-Mail-Verhalten oder Beurteilungen durch Vorgesetzte. Diese personenbezogenen Daten müssen automatisiert verarbeitet werden oder aber manuell in so genannten nicht-automatisierten Dateien, wozu z.B. Karteikastensysteme und auch Akten gehören, soweit diese gleichartig aufgebaut und nach bestimmten Merkmalen zugänglich sind und ausgewertet werden können.

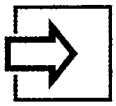
z.B.

- **persönliche Grunddaten:** z.B. Name, Anschrift, Geburtsdatum, Familienstand
- **Familiendaten:** z.B. Angaben über Familienangehörige:
- **Daten über Wohnverhältnisse:** z.B. Inhaber von Werkswohnungen
- **Daten über Einkommen und Vermögen:** z.B. Einkommenshöhe, Schulden, Verpflichtungen
- **Daten über Ausbildung:** z.B. Schulbildung, Prüfung
- **besondere Kenntnisse und Fähigkeiten:** z.B. Führerschein, Fremdsprachen
- **berufliche Daten:** z.B. Berufsausbildung, Berufsbezeichnung
- **Gesundheitsdaten:** z.B. Krankheiten, Grad der Erwerbsunfähigkeit, Kuren, besondere Empfindlichkeiten
- **soziale Daten:** z.B. Ehrenämter, Funktionen in Verbänden
- **Daten über Rechtsverstöße:** z.B. Straftaten, Ordnungswidrigkeiten, Disziplinarmaßnahmen, Führerscheinentzug

- **Werturteile:** z.B. „guter Kunde", „treuer Arbeitnehmer", „schwieriger Umgang"
- **Arbeitsdaten:** z.B. Arbeitszeiten, Fehlzeiten, Leistungsdaten, Daten über E-Mail-, Internet- und Telefonverhalten

Ausgenommen vom Anwendungsbereich des BDSG ist die Erhebung, Verarbeitung und Nutzung von Daten, die ausschließlich für **persönliche oder familiäre Tätigkeiten** erfolgt (§ 1 Abs. 2 Nr. 3 BDSG).

Fazit



Das BDSG ist in jedem Fall anzuwenden und im Betrieb umzusetzen

- bei der Verarbeitung und Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitung (automatisierte Verarbeitung),
- bei der Erhebung personenbezogener Daten für eine automatisierte Verarbeitung,
- wenn personenbezogene Daten in oder aus nicht-automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden (manuelle Datenverarbeitung).

3.2 Zentrale Regelungen im BDSG

Phasen der Datenverarbeitung

Die wichtigsten Vorgaben des BDSG sind in der nachfolgenden Tabelle zusammengestellt.

Wichtige Vorgaben im BDSG

Rechtliche Vorgabe	Inhalt
§ 4 i.V.m. § 28 BDSG	Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten
§ 3a BDSG	Datenvermeidung und Datensparsamkeit
§ 4b und c BDSG	Übermittlung personenbezogener Daten ins Ausland
§ 6a BDSG	Automatisierte Einzelentscheidungen
§ 6b BDSG	Beobachtung öffentlich zugänglicher Räume
§ 6c BDSG	Mobile Speichermedien
§ 9 BDSG	Technische und organisatorische Maßnahmen zum Datenschutz

Rechtliche Vorgabe	Inhalt
§§ 33 ff. BDSG	Rechte der Betroffenen
§ 4f und g BDSG	Betrieblicher Datenschutzbeauftragter
§ 38 BDSG	Aufgaben und Befugnisse der Aufsichtsbehörde

D

3.3 Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten

Verbot mit Erlaubnisvorbehalt

Das BDSG schützt gemäß § 1 Abs. 1 BDSG davor, dass der Betroffene (Beschäftigte) durch den **Umgang mit seinen personenbezogenen Daten** in seinem Persönlichkeitsrecht beeinträchtigt wird. Umgang mit personenbezogenen Daten umfasst die Phasen der Erhebung, Verarbeitung und Nutzung von Daten. Inwieweit personenbezogene Daten erhoben, verarbeitet oder genutzt werden dürfen, ist in § 4 i.V.m. § 28 BDSG geregelt. Dabei geht das BDSG von einem sogenannten „**Verbot mit Erlaubnisvorbehalt**" aus. Das heißt, die Verarbeitung personenbezogener Daten ist nur in dem in § 4 BDSG festgelegten Rahmen erlaubt. Daneben müssen im Einzelfall die Vorgaben von „Datenvermeidung und Datensparsamkeit", „automatisierte Einzelentscheidungen", Übermittlung personenbezogener Daten in Ausland", „Beobachtung öffentlich zugänglicher Räume" und „mobile Speichermedien" bei der Zulässigkeitsprüfung hinzugezogen werden.

Nach § 4 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten **verboten. Erlaubt bzw. zulässig ist dieses nur, soweit**

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

Keine Schlechterregelungen in Betriebsvereinbarungen

Soll die Verarbeitung personenbezogener Daten rechtmäßig erfolgen, muss **eine der oben genannten Alternativen gegeben sein.** Für die nicht immer ganz einfache Prüfung der Zulässigkeit der Verarbeitung personenbezogener Daten ist der betriebliche Datenschutzbeauftragte zuständig. Von besonderer Bedeutung für die Betriebsratsarbeit ist, dass sich Arbeitgeber und Betriebsrat bei der Umsetzung der Mitbestimmungsrechte nach dem BetrVG und beim Abschluss von Betriebsvereinbarungen im Rahmen der Vorgaben des § 4 i.V.m. § 28 BDSG bewegen müssen. Sie dürfen keine Schlechterregelungen als das BDSG treffen.

3.3.1 Zulässigkeit nach § 28 BDSG

Die Vorschrift des § 28 BDSG ist eine Erlaubnisnorm i.S.d. § 4 Abs. 1 BDSG. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig.

Zweckbestimmung eines Vertragsverhältnisses

1. wenn es der **Zweckbestimmung eines Vertragsverhältnisses** oder **vertragsähnlichen Vertrauensverhältnisses** mit dem Betroffenen dient,
2. soweit es zur Wahrung **berechtigter Interessen der verantwortlichen Stelle** erforderlich ist und kein Grund zu der Annahme besteht, dass das **schutzwürdige Interesse des Betroffenen** an dem Ausschluss der Verarbeitung oder Nutzung überwiegt oder
3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Die drei aufgeführten Zulässigkeitsalternativen begründen grundsätzlich unabhängig voneinander die Zulässigkeit des Umgangs mit personenbezogenen Daten. Gleichzeitig stehen sie jedoch nicht alternativ zueinander. Liegt etwa eine vertragliche Beziehung vor, bestimmt diese allein den Rahmen und die Zulässigkeit der Verarbeitung personenbezogener Daten. Bei vertraglichen Beziehungen kann zwar auch auf die Nr. 2 zurückgegriffen werden, wobei aber der Rahmen der Verarbeitung, der sich aus Nr. 1 ergibt, nicht erweitert werden kann.

3.3.1.1 Vertragsverhältnis oder vertragsähnliches Vertrauensverhältnis (Nr. 1)

Voraussetzung für die rechtmäßige Erhebung, Speicherung, Veränderung, Übermittlung oder Nutzung personenbezogener Daten ist, dass sie im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder eines vertragsähnlichen Vertrauensverhältnisses erfolgen muss. Es dürfen nur die Daten verarbeitet werden, die der Erfüllung der Pflichten oder der Wahrnehmung der Rechte aus dem Vertragsverhältnis dienen. Zugespitzt formuliert heißt das, dass nur die Daten erhoben, verarbeitet oder genutzt werden, **die zwingend erforderlich sind**, um das Vertragsverhältnis zu begründen und abzuwickeln. Für die Zweckbestimmung ist zudem maßgeblich, dass übereinstimmende Willenserklärungen der Vertragsparteien bestehen. Es kann also nicht auf einseitige Vorstellungen der verantwortlichen Stelle (Arbeitgeber) abgestellt werden.

Arten von Verträgen

Vertragsverhältnisse sind alle Arten von Verträgen, wie z.B. Arbeits- und Dienstverträge, Kauf-, Leih-, Werk-, Werklieferungs- und Dienstleistungs- und Mietverträge sowie Schenkungen, Bürgschaften und Auftragsverhältnisse. Stehen Betroffene mit einer verantwortlichen Stelle in verschiedenen Vertragsbeziehungen (z.B. sowohl als Beschäftigte als auch als Kunde wie im Banken-Versicherungsbereich möglich), ist die Verarbeitung von Daten nur zweckgebunden im Rahmen des jeweiligen Vertragsverhältnisses zulässig.

Vertragsähnliche Vertauensverhältnisse

Vertragsähnliche Vertrauensverhältnisse können während der konkreten Anbahnung eines Vertrags (Arbeitsvertrags) im Rahmen von entsprechenden Vorverhandlungen entstehen. Dabei kommt es auf den erfolgreichen Abschluss eines Vertrags nicht an. Vertragsähnliche Vertrauensverhältnisse sind auch nachvertragliche Verhältnisse, die etwa nach der Beendigung eines Arbeitsvertrags entstehen können.

Bei Vertragsverhältnissen oder vertragsähnlichen Vertrauensverhältnissen ist die Erhebung von Basisdaten des Betroffenen (Beschäftigter bzw. Bewerber), wie Name, Anschrift, wesentlicher Vertragsinhalt und als zulässig anzusehen. Der Umfang der Verarbeitung weiterer Daten ist nicht eindeutig zu bestimmen und lässt sich **nur im konkreten Einzelfall entscheiden**.

3.3.1.2 Wahrung berechtigter Interessen (Nr. 2)

Das Erheben, Speichern, Verändern, Übermitteln oder Nutzen von personenbezogenen Daten ist zulässig, wenn dies zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annnahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung überwiegt. Diese Vorschrift kann dann zur Anwendung kommen, **wenn kein Vertragsverhältnis oder vertragsähnliches Vertrauensverhältnis besteht**. Diese Regelung stellt eine Ausnahme zum Regelfall des § 28 Abs. 1 Nr. 1 BDSG dar und ist deshalb sehr eng auszulegen. Das Speichern der Daten muss zur Wahrung der Interessen der verantwortlichen Stelle erforderlich sein, d.h. wenn ohne Kenntnis dieser Daten die berechtigten Interessen nicht gewahrt werden können und die verantwortliche Stelle einen nicht zumutbaren Nachteil erleidet. Es muss für die rechtmäßige Erhebung, Verarbeitung und Nutzung noch hinzukommen, dass kein Grund zur Annahme besteht, dass dem berechtigte Interessen des Betroffenen entgegenstehen.

3.3.1.3 Allgemein zugängliche Quellen (Nr. 3)

Allgemein zugängliche Quellen

Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten ist auch dann zulässig, wenn die Daten aus allgemein zugänglichen Quellen stammen. Beschränkt wird dieses nur dadurch, dass das schutzwürdige Interesse des Betroffenen überwiegt. Zu den **allgemein zugänglichen Quellen** gehören z.B. Zeitungen, Zeitschriften, Rundfunk, Fernsehen, Telefonbücher, Bücher, elektronische Medien wie das Internet. Im Rahmen des Arbeitsvertragsverhältnisses kann die Datenspeicherung nicht durch diese Nr. 3 erweitert werden.

3.3.2 Andere Rechtsvorschrift

Betriebsvereinbarung

Wenn eine andere Rechtsvorschrift die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten erlaubt oder sogar anordnet, kommt es auf die Einwilligung des Betroffenen oder auf die anderen Vorgaben des § 28 BDSG nicht an. Es muss sich dabei um **Rechtsnormen** wie Gesetze, Rechtsvorordnungen, Tarifverträge, **Betriebsvereinbarungen** oder Sprüche der Einigungsstelle handeln. In Bezug auf den Beschäftigten-Datenschutz kommt Betriebsvereinbarungen eine besondere Bedeutung zu. Entsprechende Betriebsvereinbarungen verdrängen in ihrem Regelungsbereich das BDSG, dürfen jedoch nicht hinter den Vorgaben des BDSG zurückbleiben.

3.3.3. Einwilligung

Wird mit Einwilligung gearbeitet, muss sich die Einwilligung **auf die einzelnen Phasen der Datenverarbeitung beziehen**. Gegen die Einwilligung wird zu Recht eingewandt, dass sie in vielen Fällen als Zulässigkeitsvoraussetzung ungeeignet ist. Dem Bürger, dem Bewerber um einen Arbeitsplatz oder auch dem Beschäftigten bleibt häufig gar keine andere Wahl, als den Behörden, den Arbeitgebern oder Unternehmen die geforderten Daten zur Verfügung zu stellen. Zutreffend ist in jedem Fall, dass eine Einwilligung dann als Rechtsgrundlage für Datenverarbeitung fragwürdig wird, wenn der Betroffene die Einwilligung **nicht freiwillig** abgegeben hat und beispielsweise die Einwilligung unter Ausnutzung einer wirtschaftlichen Machposition „abgepresst" worden ist.

Anforderungen an eine Einwilligungserklärung nach § 4a BDSG

- Die Einwilligung muss auf der freien Entscheidung des Betroffenen beruhen.
- Der Betroffene ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung und Nutzung hinzuweisen.

- Der Betroffene ist auf die Folgen der Verweigerung der Einwilligung hinzuweisen.
- Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.
- Soll die Einwilligung mit anderen Erklärungen zusammen abgeben werden, ist sie besonders hervorzuheben.

D

Werden besondere Arten personenbezogener Daten erhoben, verarbeitet oder genutzt, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

Das BDSG knüpft an die Einwilligung bestimmte Voraussetzungen. So ist eine Einwilligungserklärung nur wirksam, wenn sie auf der **freien Entscheidung des Betroffenen** (Beschäftigten) beruht. Das heißt, die Einwilligung muss freiwillig erfolgen. Ist sie nur aufgrund arbeitgeberseitigen Drucks – etwa durch Drohung mit Kündigung oder anderen nachteiligen Maßnahmen – erteilt worden, so verfällt sie gemäß § 138 BGB der Nichtigkeit.

Hinreichend bestimmt, ausreichend und transparent

Zusätzlich muss der Betroffene auf den Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalls erforderlich oder auf Verlangen, auf die Folgen der Weigerung einer Einwilligung hingewiesen werden. Das bedeutet also, dass die Einwilligungserklärung hinreichend bestimmt sein muss. Dieses ist nur dann der Fall, wenn die Einwilligungserklärung **ausführlich und transparent** gehalten ist, sodass der Betroffene die Reichweite der Einwilligung genau ein- und abschätzen kann. In einer vorgelegten Einwilligungserklärung muss erkennbar sein, um welche **personenbezogenen Daten** es sich konkret handelt, wer die Daten verarbeitet und auswertet und ob Daten an Dritte übermittelt werden.

Schriftform

Die Einwilligung bedarf der **Schriftform**, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Die Einwilligung muss also schriftlich fixiert und vom Betroffenen **eigenhändig unterschrieben werden**. Soll die Einwilligung mit anderen Erklärungen schriftlich abgegeben werden, ist sie besonders hervorzuheben. Eine Einwilligungserklärung, die diesen Vorgaben nicht gerecht wird, ist nichtig.

Mitbestimmung des Betriebsrats

Eine Einwilligungserklärung stellt ein Fragebogen i.S.d. § 94 Abs. 1 BetrVG und dar unterliegt der **Mitbestimmung des Betriebsrats**.

3.3.4 Übermitteln von Daten für Zwecke der Werbung

„Freie" Daten für Markt- und Meinungsforschung

In § 28 Abs. 3 BDSG ist die Übermittlung so genannter „freier" Daten für Zwecke der **Werbung und der Markt- und Meinungsforschung** festgelegt. Diese Regelung kann man auch als „Verbeugung des Datenschutzes vor der Werbewirtschaft" bezeichnen. Daten können übermittelt werden, wenn es sich um listenmäßige oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt. Es kann sich dabei **ausschließlich** um folgende Daten handeln:

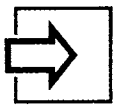
- eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe
- Berufs-, Branchen- oder Geschäftsbeteiligung
- Namen
- Titel
- Akademische Grade
- Anschrift
- Geburtsjahr

Die Übermittlung darf nur erfolgen, wenn kein Grund zu der Annahme besteht, das der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat. Ein schutzwürdiges Interesse ist nach § 28 Abs. 3 Nr. 4 BDSG immer dann gegeben, wenn im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertauensverhältnisses gespeicherte Daten übermittelt werden sollen, die sich

- auf strafbare Handlungen,
- auf Ordnungswidrigkeiten sowie
- bei Übermittlung durch den Arbeitgeber auf arbeitsrechtliche Rechtsverhältnisse beziehen.

Dieses bedeutet, dass Daten von Beschäftigten nicht für Zwecke der Werbung oder der Markt- und Meinungsforschung übermittelt werden dürfen.

Fazit



Die zentrale Vorgabe für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten bildet der § 4 i.V.m. § 28 BDSG.

Das BDSG geht von einem so genannten **„Verbot mit Erlaubnisvorbehalt"** aus.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten **ist nur zulässig**, soweit

- das BDSG (§ 28) oder
- eine andere Rechtsvorschrift dieses erlaubt oder anordnet oder
- der Betroffene (z.B. der Bewerber oder der Beschäftigte) eingewilligt hat.

Arbeitgeber und Betriebsrat haben im Rahmen der Umsetzung der Mitbestimmungsrechte nach dem BetrVG diese Vorgaben des BDSG zwingend einzuhalten.

3.3.5 Direkterhebung

Mit Kenntnis oder Mitwirkung

In § 4 Abs. 2 BDSG wird zusätzlich festgelegt, dass die Erhebung personenbezogener Daten beim Betroffenen selbst zu erfolgen hat; es wird also das **Prinzip der Direkterhebung** verankert. Dieser Grundsatz ist ein unmittelbarer Ausfluss des Volkszählungsurteils und des Rechts auf informationelle Selbstbestimmung. Der Betroffene soll wissen, **wer wann welche Daten über ihn sammelt, speichert und verarbeitet**. Im Grundsatz sind Daten beim Betroffene selbst und nicht hinter seinem Rücken zu erheben. „Beim Betroffenen" bedeutet, dass die Daten mit Kenntnis oder Mitwirkung erhoben werden. Somit sind z.B. im Rahmen der Bewerbung oder im laufenden Beschäftigungsverhältnis Nachfragen bei früheren Arbeitgebern auszuschließen. Voraussetzung wäre hier eine Einwilligung des Bewerbers oder Beschäftigten oder eine der Ausnahmen würde greifen.

Das BDSG sieht Ausnahmen dahin gehend vor, wenn

- eine Rechtsvorschrift die Erhebung zwingend vorsieht oder
- der zu erfüllende Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
- die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde.

Diese Ausnahmen kommen nur dann zum Tragen, wenn keine Anhaltspunkte dafür bestehen, dass das überwiegende Schutzinteresse des Betroffenen beeinträchtigt wird. Man wird also davon ausgehen müssen, dass sowohl bei Bewerbern als auch bei Beschäftigten **eine Direkterhebung der Daten erfolgen muss.**

3.3.6 Datenvermeidung und Datensparsamkeit

Nach § 3a BDSG haben sich die Gestaltung und Auswahl von Datenverarbeitungsanlagen an dem Ziel auszurichten, **keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.** Der Grundsatz der **Datenvermeidung und -sparsamkeit** ist erstmalig in das BDSG aufgenommen worden.

Auswahl des Systems

Die Vorschrift konkretisiert den Grundsatz der Verhältnismäßigkeit für die Gestaltung der Datenverarbeitungssysteme. Eine vergleichbare Regelung findet sich in § 3 Abs. 4 Teledienstedatenschutzgesetz. Wie dort soll durch die Einführung dieses Grundsatzes bereits durch die **Auswahl des Systems** und durch die Gestaltung der Systemstrukturen die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten soweit wie möglich vermieden werden. Dadurch sollen zudem Gefahren für das informationelle Selbstbestimmungsrecht des Betroffenen von vornherein vermieden werden.

z.B.

Bei bargeldloser Bezahlung in der Betriebskantine entsprechen Kantinenabrechnungssysteme, die so angelegt sind, dass der zu zahlende Betrag im Rahmen der Lohn- und Gehaltsabrechnung vom Lohn/Gehalt abgezogen wird, nicht der Vorgabe der Datenvermeidung und -sparsamkeit. Dahingegen wird ein Kantinenabrechnungssystem, bei dem der Beschäftigte seine Magnet- oder Chipkarte an einem Automaten mit einem Geldbetrag aufladen kann und dann bei der Bezahlung ein entsprechender Geldbetrag von der Karte abgebucht wird, der Vorgabe der Datenvermeidung und -sparsamkeit gerecht, da keine bzw. u.U. nur sehr wenige personenbezogene Daten der Beschäftigten verarbeitet werden.

Anonyme und pseudonyme Formen

§ 3a Satz 2 BDSG beinhaltet den Vorrang **anonymer und pseudonymer Formen der Datenverarbeitung**, als eine von mehreren Möglichkeiten der Ausgestaltung des Systemdatenschutzes und als ein zusätzliches Mittel, dem Grundsatz der Erforderlichkeit und engen Zweckbestimmung der Datenverarbeitung Rechnung zu tragen.

3.3.7 Automatisierte Einzelentscheidungen

§ 6a BDSG stellt insoweit eine Besonderheit dar, als nicht die Zulässigkeit der Datenverarbeitung selbst geregelt wird, sondern **Entscheidungsabläufe reguliert werden**. Nach § 6a Abs. 1 BDSG dürfen Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, **nicht** ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen.

Zulässigkeit automatisierter Einzelentscheidungen

Die Vorschrift begrenzt die **Zulässigkeit automatisierter Einzelentscheidungen**. Sie beruht auf dem Grundgedanken, dass Entscheidungen, die die Bewertung einer Person beinhalten und daher das Persönlichkeitsrecht zentral berühren, nicht einem Computerprogramm überlassen werden dürfen, sondern **stets durch Personen verantwortet werden müssen**. Es geht in diesem Paragraphen also nicht um die Frage, ob Daten, die zur Bewertung einer Person beitragen können, verarbeitet werden dürfen, noch um die Frage, ob derartige Bewertungen mithilfe eines automatisiert ablaufenden Computerprogramms vorgenommen werden dürfen, sondern allein darum, wie ein solcher Vorgang gestaltet werden muss, damit der Betroffene ausreichend beteiligt ist, und zum anderen, dass aufseiten des für die Verarbeitung Verantwortlichen die persönliche Verantwortung für die zu treffende Entscheidung gesichert ist. Die Zulässigkeit der Datenverarbeitung selbst richtet sich nach den §§ 4 i.V.m. 28 BDSG.

Bewertung einzelner Aspekte einer Person

Entscheidungen i.S.d. § 6a BDSG sind solche, die auf Daten gestützt werden, die zum Zweck der **Bewertung einzelner Aspekte einer Person**, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens, erhoben werden. Hierunter fallen so genannte Scoring- oder auch Punktewertverfahren. Zu denken ist aber auch an **Persönlichkeitsprofile**. Eine Bewertung einzelner Persönlichkeitsmerkmale kann bei der Einstellung von Bewerbern aber auch bei der Personalauswahl stattfinden, wenn Fähigkeiten, Leistungen, Charaktereigenschaften oder sonstige Merkmale in die Verarbeitung eingehen und dabei zur Reihung bzw. Einstufung von Arbeitnehmern verarbeitet werden. Die hier vorausgesetzte komplexe Datenverarbeitung ist für **Expertensysteme** typisch.

Die Regelung betrifft aber nur solche Entscheidungen, die **rechtliche Folgen** für den Betroffenen nach sich ziehen oder ihn **erheblich beeinträchtigen**. Ob die rechtlichen Folgen dabei günstig oder nachteilig sind, spielt keine Rolle. Zu denken ist beispielsweise an abgelehnte Kreditgesuche oder abgelehnte Stellenbewerbungen.

Ausnahmen

§ 6a Abs. 2 BDSG enthält **Ausnahmen** zu dem verankerten Verbot. Es gilt nicht, wenn

- die Entscheidung im Rahmen des Abschlusses oder der **Erfüllung eines Vertragsverhältnisses** oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wurde oder
- die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet und dem Betroffenen von der verantwortlichen Stelle die Tatsache des Vorliegens einer für ihn **positiven Entscheidung** im Rahmen eines Vertragsverhältnisses mitgeteilt wird.

Als „**geeignete Maßnahme**" in diesem Sinne gilt insbesondere die Möglichkeit des Betroffenen, seinen Standpunkt geltend zu machen. Die verantwortliche Stelle ist dann verpflichtet, ihre Entscheidung erneut zu prüfen.

Auskunftsrecht

In § 6a Abs. 3 BDSG ist ein besonderes **Auskunftsrecht** dahin gehend verankert, dass sich bei automatisierten Entscheidungen auf den logischen Aufbau der automatisierten Verarbeitung erstrecken. In diesen Fällen wird das in § 34 BDSG verankerte Auskunftsrecht auch auf den Verarbeitungsvorgang selbst ausgeweitet. Die Probleme für die praktische Umsetzung dieser Vorgabe sind jedoch nicht zu übersehen, da die Softwareprogramme heute angesichts der rückläufigen Preise für Speicherkapazität meist äußerst umfangreich und komplex sind. In jedem Fall muss der **logische Aufbau, so wie es sich im Programmablauf vollzieht**, der betroffenen Person **verständlich** gemacht werden, sodass die Person verstehen kann, in welcher Weise aus ihren konkreten personenbezogenen Daten bestimmte Bewertungen oder Klassifizierungen abgeleitet werden und welche Bedeutung diese Werte im Verarbeitungssystem besitzen.

3.3.8 Übermittlung personenbezogener Daten ins Ausland

Grenzüberschreitender Datenverkehr

Die fortschreitende Globalisierung und die rasante Entwicklung der IuK-Technologien lassen auch den **grenzüberschreitenden Datenverkehr** selbstverständlich werden. Die Anzahl multinationaler Konzerne wächst und die weltweiten Datennetze vereinfachen den Datenaustausch, wobei die Bestrebungen und Tendenzen zu einer informationellen Verstärkung im Bereich der Unternehmen schon seit vielen Jahren bekannt sind und inzwischen realisiert werden. Dabei trägt gemäß § 4b Abs. 5 BDSG die **übermittelnde Stelle die Verantwortung für die Zulässigkeit der Überbermittlung**. Zusätzlich ist die Stelle, an die Daten übermittelt werden, darauf hinzuweisen, dass die übermitteln-

den Daten nur zu dem Zweck verarbeitet oder genutzt werden, zu dem sie übermittelt werden. Vor diesem Hintergrund bedarf die Datenübermittlung über die Grenzen der Bundesrepublik Deutschland hinaus der genaueren Betrachtung.

3.3.8.1 *Datenübermittlung bei angemessenem Schutzniveau im Drittland*

Übermittlung von Daten ins Ausland

Für die **Übermittlung von Daten ins Ausland** gelten die Vorgaben des § 4 Abs. 1 BDSG, wonach eine Übermittlung nur dann erfolgen darf, soweit das BDSG (§ 28) oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Bei grenzüberschreitendem Datenverkehr sind **zusätzlich** die Vorgaben des § 4b BDSG zu beachten. Nach Vorgabe der EG-Datenschutzrichtlinie enthält § 4b BDSG eine differenzierte Regelung. So stellt § 4b Abs. 1 BDSG den innergemeinschaftlichen dem inländischen Datenverkehr gleich. So ist ein Datentransfer von München nach Paris in Zukunft genauso zu behandeln wie ein Datentransfer von München nach Hamburg. Für die Übermittlung der Daten gelten die in § 4 i.V.m. § 28 BDSG enthaltenen Zulässigkeitsvoraussetzungen.

Drittland außerhalb der Europäischen Union

Die Datenübermittlung in ein **Drittland außerhalb der Europäischen Union** ist im Grundsatz nur dann zulässig, wenn das Drittland ein **angemessenes Datenschutzniveau** gewährleistet. Ob in dem jeweiligen Land ein angemessenes Datenschutzniveau besteht, kann die Stelle, die Daten übermitteln will, anhand der in § 4b Abs. 3 BDSG festgelegten Kriterien eigenständig prüfen. So wird die Angemessenheit des Datenschutzniveaus unter Berücksichtigung aller Umstände beurteilt werden müssen, die bei einer Datenübermittlung von Bedeutung sind. Dieses sind insbesondere

- die Art der Daten,
- die Dauer der geplanten Verarbeitung,
- das Herkunfts- und das Endbestimmungsland,
- die für die Empfänger geltenden Rechtsnormen sowie
- die für ihn geltenden Standesregeln und Sicherungsmaßnahmen.

3.3.8.2 *Datentransfer in ein Land ohne angemessenes Datenschutzniveau*

Besteht in einem Drittland **kein angemessenes Datenschutzniveau** sieht das BDSG verschiedene Möglichkeiten für eine rechtmäßige Datenübermittlung vor.

Ausnahmekatalog nach § 4c Abs. 1 BDSG

Auch wenn ein Empfängerland kein angemessenes Datenschutzniveau gewährleistet, lässt § 4c **Ausnahmen** zu, sofern

- der Betroffene seine **Einwilligung** gegeben hat,
- die Übermittlung für die **Erfüllung eines Vertrags** zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, erforderlich ist,
- die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll,
- die Übermittlung für die Wahrung eines **wichtigen öffentlichen Interesses** oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,
- die Übermittlung für die Wahrung **lebenswichtiger Interessen des Betroffenen** erforderlich ist oder
- die **Übermittlung aus einem Register** erfolgt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

Feststellung durch EU-Kommission

Die zur Feststellung der Angemessenheit erforderlichen Ermittlungen zum Datenschutzrecht in einem Drittland können sehr aufwendig sein. Deshalb sieht Artikel 25 Abs. 6 EG-Datenschutzrichtlinie vor, dass die **EU-Kommission** für ein Drittland allgemein die Feststellung in Bezug auf ein **angemessenes Datenschutzniveau** treffen kann. Entsprechendes gilt für den umgekehrten Fall, wenngleich negative Feststellungen bis jetzt nicht vorgekommen sein dürften. Positive Feststellungen wurden z.B. für Ungarn und die Schweiz getroffen.

Genehmigung durch die Aufsichtsbehörde

Die Übermittlung personenbezogener Daten in ein Land ohne angemessenes Datenschutzniveau kann nach § 4c Abs. 2 BDSG auch durch die **Aufsichtsbehörde** genehmigt werden, und zwar dann, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist. Diese Garantien können sich insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregeln ergeben.

Besonderheit USA

Im Fall der USA gibt es eine besondere Regelung. Da in den USA weder eine umfassende Datenschutzgesetzgebung besteht noch eine solche beabsichtigt ist, wäre das Feststellen eines „angemessenen Datenschutzniveaus“ wenig aussichtsreich gewesen. Gerade wegen der engen wirtschaftlichen Beziehung zwischen den Mitgliedstaaten der

EU und den USA ist ein Rechtsrahmen mit der Bezeichnung „US International Safe Harbor Principles" oder kurz „**Safe Harbor**" (sicherer Hafen) für die Daten aus Europa vereinbart worden. Am 26. Juli 2000 hat die EU-Kommission festgestellt, **dass dieser Rechtsrahmen ein angemessenes Datenschutzniveau gewährleistet**. US-Unternehmen können sich freiwillig den Regeln des Safe Harbor unterwerfen und sind dann privilegierte Empfänger personenbezogener Daten aus Europa. Für europäische Unternehmen bedeutet das eine erhebliche Erleichterung. Sie brauchen lediglich durch Einsicht in die derzeit in Vorbereitung befindliche Liste des US-Handelsministeriums davon zu überzeugen, dass ihr Geschäftspartner dem „Safe Harbor" angehört.

3.3.8.3 *Regelung über Betriebsvereinbarungen*

Die Datenübermittlung kann aber auch im Rahmen einer **Betriebsvereinbarung** geregelt werden, wobei eine Betriebsvereinbarung eine andere Rechtsvorschrift i.S.d. § 4 Abs. 1 BDSG darstellt. Inzwischen gibt es eine Reihe von Fällen, in denen durch Vereinbarung zwischen deutschen und ausländischen Unternehmen die Wahrung eines angemessenen Datenschutzstandards sichergestellt wurde.

Die Regelungsinhalte unterscheiden sich nicht grundsätzlich von den Betriebsvereinbarungen, die zu technischen Kontrollsystemen abgeschlossen werden. Wichtig ist es, zum einen den Rahmen der Datenverarbeitung transparent zu machen und auf den betrieblich erforderlichen Umfang einzugrenzen, indem eine Festlegung der

- eingesetzten Hardware,
- eingesetzten Software,
- personenbezogenen Daten,
- zugriffsberechtigten Personen,
- Schnittstellen,
- Auswertungen und
- Löschungsfristen

erfolgt.

Kontrollmöglichkeit: zusätzlicher Vertrag

Zusätzlich sollten neben Datenschutz- und Datensicherungsmaßnahmen die Rechte der Arbeitnehmer (§§ 33 bis 35 BDSG), **Kontrollmöglichkeiten** des Betriebsrats und des betrieblichen Datenschutzbeauftragten in der Betriebsvereinbarung festgelegt werden. Da im Ausland bei Datenschutzverletzungen in der Regel keine Sanktionen vorgesehen sind und zusätzlich externe Kontrollorgane wie die deut-

schen Aufsichtsbehörden dort nicht eingerichtet sind, sollten Strafen bei Vertragsverletzungen vereinbart werden. Da eine Betriebsvereinbarung nicht automatisch im Ausland seine Geltung entfaltet, müssen beide Unternehmen in einem **zusätzlichen Vertrag** die Geltung der Vereinbarung festlegen.

3.3.9 Videoüberwachung

Das vom Bundesverfassungsgericht (BVerfG) entwickelte Recht auf informationelle Selbstbestimmung findet auch auf alle Maßnahmen der Videoüberwachung Anwendung. Videoüberwachung gehört wegen der hohen Informationsdichte, die die Bildinformationen aufweisen, zu den intensivsten Formen der Erhebung, Verarbeitung und Nutzung personenbezogener Daten. So gelten auch für die Videoüberwachung die vom BVerfG hervorgehobenen Probleme: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen." (BVerfG v. 15.12.1983, NJW 8/84, S. 422)

Recht am eigenen Bild

Das aus dem allgemeinen Persönlichkeitsrecht abgeleitete Recht am eigenen Bild schützt nicht nur vor jeder Art unbefugter Verbreitung und Veröffentlichung, sondern auch vor jeder Art der unbefugten Anfertigung eines Bildes einer Person. Darunter fällt jede Art durch technische Mittel bewirkte Direktübertragung des Erscheinungsbilds einer Person, so auch die Überwachung der Arbeitnehmer bei der Arbeit durch offene oder heimliche fotografische Einzelaufnahmen, Film-, Fernseh- oder Videokameras. Der Einsatz dieser technischen Mittel kann aber zulässig sein, wenn es um die Beobachtung von Arbeitsprozessen geht oder er aus Sicherheitsgründen (Gebäudesicherung) erfolgt.

Neben der Regelung zur Videoüberwachung selbst kommen aber auch weitere Vorgaben des BDSG zum Tragen, wie z.B. die Regelung zur Datenvermeidung und Datensparsamkeit (§ 3a BDSG). In jedem Fall ist zu prüfen, ob eine Vorabkontrolle durchzuführen ist. So ist eine Vorabkontrolle dann durchzuführen, wenn Datenverarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Solche Risiken liegen regelmäßig vor, wenn Überwachungskameras nicht punktuell, sondern durch die verantwortliche Stelle in größerer Zahl und zentral kontrolliert eingesetzt werden. Ebenso kann die verwendete Technik (etwa bei schwenkbaren Kameras mit hoher Auflösung der gewonnenen Bilder) zu einem solchen Risiko führen.

3.3.9.1 Vorgaben des § 6b BDSG

In § 6b Abs. 1 BDSG ist die **Beobachtung öffentlich zugänglicher Räume** mit optisch-elektronischen Einrichtungen (Videoüberwachung) geregelt. Die Verarbeitung und Nutzung von Daten (Aufzeichnung und Speicherung) wird gesondert in § 6 Abs. 3 und 5 BDSG geregelt.

Beobachten

In § 6b BDSG wird unterschieden zwischen der Beobachtung und der Aufzeichnung in Form von Verarbeitung und Nutzung. So genügt die reine Beobachtung, ohne dass eine Aufzeichnung der Bilder erfolgen muss, für die Anwendung des § 6b BDSG aus. Unter Beobachtung ist jede Tätigkeit zu verstehen, die darauf gerichtet ist, Geschehnisse und Personen mithilfe geeigneter Geräte und Einrichtungen zu überwachen. Im Unterschied zum Erheben setzt Beobachten nicht notwendigerweise eine Erfassung personenbezogener Daten voraus. Dieses hat aber auch zur Folge, dass das Aufstellen oder Anbringen von Kameraattrappen, so genannten Dummies, nicht der Regelung des § 6b BDSG unterliegt, denn Voraussetzung ist die Beobachtung mittels einer optisch-elektronischen Einrichtung.

Öffentlich zugängliche Räume

Voraussetzung für die Anwendung dieser Regelung ist die Installation der Videoüberwachungsanlage in „öffentlich zugänglichen Räumen". Sowohl in der Rechtsprechung als auch in der Literatur gibt es keine Definition des Begriffs „öffentlich zugänglicher Raum". Meistens werden, wie auch in der Gesetzesbegründung zum BDSG, nur Beispiele aufgezählt. In der Gesetzesbegründung werden „Bahnsteige, Ausstellungsräume eines Museums, Verkaufsräume oder Schalterhallen" genannt. Entscheidend für die Anwendung der Regelung ist nicht, dass es Einrichtungen (innerhalb oder außerhalb von Gebäuden) sind, die im öffentlichen Eigentum stehen, sondern dass es sich um Bereiche handelt, **die ohne jede Voraussetzung von jedermann genutzt werden können**. Im Gegensatz dazu ist bei einem nicht öffentlich zugänglichen Raum der Kreis der Personen, die Zutritt haben, begrenzt. So sind Firmen- oder Werksgelände typischerweise keine öffentlich zugänglichen Räume. Davon ist in jedem Fall auszugehen, wenn durch Schilder am Werksgelände darauf hingewiesen wird, dass nur Befugten der Zutritt erlaubt ist. Im Einzelfall kann jedoch „Firmgelände" öffentlich zugänglicher Raum sein, wenn z.B. ein Unternehmen in seinem Eingangsbereich (Treppenhaus, Foyer) Kunstausstellungen durchführt und jede Person Zutritt hat. Hier ist es geradezu gewollt, dass diese Bereiche öffentlich zugänglich sind.

Optisch-elektronische Einrichtung

Die Kontrolle muss durch „**optisch-elektronische Einrichtungen**" erfolgen. Hierunter fallen wohl in erster Linie festinstallierte Videokameras und Webcams. Kameras, Ferngläser und moderne Fotoappa-

rate sind wohl nicht mit einzubeziehen, da es sich nicht um „Einrichtungen" handelt. Denn bei Einrichtungen muss es sich um festinstallierte oder aufgestellte Überwachungssysteme. Wie bereits erwähnt, fallen Attrappen nicht unter diese Regelung.

Zulässigkeit der Videobeobachtung

Das BDSG enthält in § 6b Abs. 1 drei Vorgaben für die Zulässigkeit von Videobeobachtung. Diese bilden die Grundlage für die rechtmäßige Verwendung von Videoanlagen. Die Videobeobachtung öffentlich zugänglicher Räume ist zulässig, soweit sie

a) zur Aufgabenerfüllung öffentlicher Stellen,
b) zur Wahrnehmung des Hausrechts oder
c) zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist.

a) **„zur Aufgabenerfüllung öffentlicher Stellen":** Die Beobachtung öffentlich zugänglicher Räume ist zulässig, soweit sie zur Aufgabenerfüllung öffentlicher Stellen (des Bundes) erforderlich ist (§ 6b Abs. 1 Nr. 1 BDSG). Unter diese erste Zulässigkeitsvariante fallen **nicht** die nicht öffentlichen Stellen (Privatbetriebe, Vereine, Stiftungen). Deshalb wird die Regelung an dieser Stelle nicht dargestellt.
b) **„zur Wahrnehmung des Hausrechts":** Die Regelung, dass die Videoüberwachung „**zur Wahrnehmung des Hausrechts** zulässig" ist, richtet sich an öffentliche und nicht öffentliche Stellen. Hierunter fallen Videobeobachtungen, die dazu dienen, die Begehung von Straftaten (Diebstahl, Sachbeschädigungen) zu verhindern oder aufzuklären. Hierzu zählt auch die Überwachung von Hausverboten. Zivilrechtlich ergibt sich das Hausrecht aus den Abwehransprüchen des Eigentümers nach §§ 859 ff., § 904, § 1004 BGB. Gründe und Schranken können sich aus spezialgesetzlichen Bestimmungen wie beispielsweise dem Mietrecht (§ 535 BGB) oder dem Wohnungseigentümergesetz (§ 21 WEG) ergeben.
c) **„zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke":** Der Begriff „**Wahrnehmung berechtigter Interessen**" ist dem § 28 Abs. 1 Nr. 2 BDSG entlehnt, der als Basis für eine rechtmäßige Datenverarbeitung dienen kann. Was im Einzelfall ein berechtigtes Interesse ist, entscheidet nicht allein die verantwortliche Stelle im eigenen subjektiven Ermessen. Nach der Gesetzesbegründung muss das Interesse objektiv begründbar sein, was auch bedeutet, dass das Interesse des Betroffenen am Schutz seines Persönlichkeitsrechts Berücksichtigung finden muss. So kann beispielsweise der Zweck der Diebstahlprävention keinesfalls die Überwachung von Toiletten oder Umkleidekabinen rechtfertigen. Zusätzlich muss die Wahrnehmung berechtigter Interessen für

konkret festgelegte Zwecke erfolgen. Dieses bedeutet, dass im Vorfeld (vor Installation der Videoanlage) die Zwecke (z.B. Verhinderung von Diebstahl) genau festgelegt werden müssen. Diese festgelegten Zwecke, die im Grunde genommen schriftlich fixiert werden müssen (auch wenn dies im BDSG nicht direkt vorgeschrieben ist), dürfen später nicht so ohne weiteres verändert oder erweitert werden. So kann eine Bank, die im Bereich der Geldautomaten und Selbstbedienungsterminals Kameras zur Verhinderung von Sachbeschädigung (Vandalismus) und Diebstahl einsetzt, die Daten nicht zur Messung (Beobachtung) von Kundenströmen nutzen.

„Zusätzliche Erforderlichkeit"

Für alle drei Zulässigkeitsalternativen setzt die Zulässigkeit der Videoüberwachung weiterhin voraus, dass sie zur Erreichung der in den einzelnen Punkten genannten Zwecke erforderlich sind. Erforderlichkeit heißt, dass mit der Videoüberwachung das beabsichtigte Ziel auch erreicht werden kann und dass die Überwachung notwendig ist. So ist beispielsweise in Warenhäusern immer zu prüfen, ob Diebstahl nicht durch andere Methoden zur Sicherung der Waren verhindert werden kann. Diese notwendige Prüfung ergibt sich u.a. auch aus dem Gebot der „Datenvermeidung und Datensparsamkeit".

Die Beweislast für die konkrete und rechtzeitige Festlegung der Zwecke liegt bei der für die Videobeobachtung verantwortlichen Stelle. Kann sie keinen ausreichenden Nachweis führen, ist die Videoüberwachung unzulässig.

3.3.9.2 Information der Betroffenen

Findet Videoüberwachung in öffentlich zugänglichen Räumen statt, „ist der Umstand der Beobachtung durch geeignete Maßnahmen erkennbar zu machen" (§ 6b Abs. 2 BDSG). Was nun geeignete Maßnahmen sind, entscheidet die Stelle, die Videoüberwachung einsetzt. Man wird davon ausgehen müssen, dass Schilder, die groß genug sein müssen und gut sichtbar angebracht werden müssen, jedenfalls dann geeignete Maßnahmen sind, wenn darauf auch Piktogramme (für Fremdsprachler) und der Name der verantwortlichen Stelle angebracht sind. Unter Umständen muss die „verantwortliche Stelle" dann nicht auf dem Hinweisschild angebracht werden, wenn dieses Schild direkt am Eingangsbereich des Gebäudes angebracht ist.

3.3.9.3 Aufzeichnung und Nutzung von Videodaten

In § 6b Abs. 3 BDSG sind die Zulässigkeitsvoraussetzungen für die über die reine Videobeobachtung hinausgehende **Verarbeitung** und **Nutzung** der im Wege der Videobeobachtung gewonnenen Daten geregelt. So kann aus der Zulässigkeit der Beobachtung nicht auch schon auf die Zulässigkeit der Verarbeitung (hierzu gehört die Speicherung und Übermittlung von Daten) und Nutzung der Daten geschlossen werden. Das heißt, dass dieses in einem gesonderten Prüfschritt festgestellt werden muss. So ist die Verarbeitung und Nutzung von Daten, die durch Videobeobachtung gewonnen worden sind, nur zulässig, **„wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen überwiegen"** (§ 6b Abs. 3 BDSG). Schutzwürdige Interessen des Betroffenen sind in besonderer Weise berührt, wenn automatisierte Verfahren beispielsweise zum Vergrößern und Herausfiltern einzelner Personen, zur biometrischen Erkennung, zum Bildabgleich oder zur Profilerstellung eingesetzt werden oder zu solchen Zwecken verfügbar sind. Denn derartige Maßnahmen greifen in besonders gravierender Weise in das informationelle Selbstbestimmungsrecht des Betroffenen ein, sodass regelmäßig das Interesse des Betroffenen überwiegt, nicht zum Objekt automatisierter Verarbeitung gemacht zu werden.

Benachrichtigungspflicht

Zusätzlich besteht eine **Benachrichtigungspflicht**, wenn die durch Videoüberwachung gewonnenen Daten einer Person zugeordnet werden (§ 6b Abs. 4 BDSG).

Daten sind unverzüglich zu löschen

Die durch Videoüberwachung gewonnenen **Daten sind unverzüglich zu löschen**, wenn sie zur Erreichung des Zweck nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen (§ 6b Abs. 5 BDSG). So werden bei einer Videoüberwachung in einem Warenhaus zur Vermeidung von Diebstählen die Daten jeden Abend gelöscht werden müssen, da die Aussicht, Personen durch nichtzeitnahe Auswertungen von Aufzeichnungen zu fassen, so gut wie ausgeschlossen ist.

3.3.9.4 Nicht öffentlich zugängliche Räume

Sollen **nicht öffentlich zugängliche Räume** überwacht werden, gilt nicht § 6b BDSG, sondern es gelten die allgemeinen Vorgaben des BDSG. Wenn die Beschäftigten von der Videoüberwachung betroffen sind, sind vor allem § 28 BDSG und § 4 Abs. 2 BDSG von Bedeutung. Nach § 4 Abs. 2 BDSG sind **personenbezogene Daten beim Betroffenen zu erheben**. Der Betroffene soll wissen, wer was wann über ihn

sammelt, speichert und verarbeitet. Durch diese Vorgabe ist eine **heimliche Videoüberwachung von Beschäftigten ausgeschlossen**.

§ 28 BDSG

Nach **§ 28 BDSG** ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig,

- wenn es der Zweckbestimmung des Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen
- soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Eine Videoüberwachung eines Beschäftigten wird man nicht aus der Zweckbestimmung seines Arbeitsvertrags herleiten können. Zugleich ist das schützwürdige Interesse des Beschäftigten gerade bei dieser Überwachungstechnik hier höher anzusiedeln als das Interesse des Arbeitgebers (verantwortliche Stelle). So wird ein Beschäftigter in der Regel von Videoüberwachung nur dann betroffen sein können, wenn es z.B. um Überwachung von Kaufhäusern, Museen, Schwimmbädern, Parkhäusern, Parkplätzen geht. Diese Videoaufzeichnung von Beschäftigten ist dann meist eine unbeabsichtigte Nebenfolge anderer Zweckbestimmungen. In diesen Fällen wird man z.B. durch den Abschluss einer **Betriebsvereinbarung** die Nutzung und Auswertung der Beschäftigtendaten unterbinden. **Besonders sensible Bereiche müssen generell von Videoüberwachung freigehalten werden.** Hierzu zählen z.B. Einzelbüros, Umkleidekabinen, Sanitärbereiche sowie Untersuchungsräume in Kliniken und Praxen.

3.3.9.5 Recht am eigenen Bild gemäß KUG

Kunsturhebergesetz, Einwilligung des Beschäftigten

Neben dem allgemeinen Persönlichkeitsrecht und den Vorgaben des BDSG kann auch das so genannte **Kunsturhebergesetz** (KUG) zum Tragen kommen. Das Recht am eigenen Bild ist in den §§ 22-24 KUG geregelt und versetzt den Abgebildeten in bestimmten Grenzen in die Lage, über die Verbreitung seines Bildnisses zu entscheiden. Es handelt sich um ein Persönlichkeitsrecht zum Schutz ungewollter Darstellung, woraus sich die Unzulässigkeit einer Veröffentlichung des Bildes einer Person schon dann ergibt, wenn sie ohne Einwilligung des Abgebildeten geschieht. Vor diesem Hintergrund kann in der Regel die Einstellung von Bildern der Mitarbeiter auf die unternehmenseigene oder behördeneigene Homepage nur mit **Einwilligung des Beschäftigten** erfolgen. Die Herstellung von Bildern, also die Videoüberwachung als solche, wird vom Wortlaut der §§ 22 f. KUG nicht erfasst. Das heißt,

das KUG erfasst nicht das Entstehen, Speichern, Verändern oder Nutzen von Bildern. Hier sind dann das allgemeine Persönlichkeitsrecht bzw. die Vorgaben des BDSG zu beachten.

3.3.10 Mobile Speichermedien

Mobile Speicher- und Verarbeitungsmedien sind Datenträger,

- die an den Betroffenen ausgegeben werden,
- auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und
- bei denen der Betroffene die Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann (§ 3 Abs. 10 BDSG).

Chipkarten, Smart Card

Unter „mobilen Speicher- und Verarbeitungsmedien" sind Datenträger mit einem Prozessorchip zu fassen, wie **Chipkarten oder Smart Card**. Es muss sich aber nicht zwingend um eine Karte handeln, sondern der Chip kann sich auch an einem Armband, an einer Halskette oder in einer Armbanduhr befinden. Durch den Begriff „mobile Speicher- und Verarbeitungsmedien" ist das BDSG technikoffen, sodass gegenwärtige und zukünftige Verarbeitungsformen erfasst werden. Zusätzlich müssen auf diesen Medien neben der Speicherung von Daten selbst **die Daten auch automatisiert** verarbeitet werden. Technisch muss der Datenträger also mit einem Prozessorchip ausgestattet sein, sodass „dumme" Speichermedien wie CDs oder Magnetkarten nicht erfasst werden.

Zudem darf der Betroffene die Datenverarbeitung auf dem Medium nur durch den Gebrauch des Mediums beeinflussen. Dieses kann der Fall sein, wenn er ein Lesegerät, das den Zugang zu einem Gebäude absichert, passiert und auf seiner Karte z.B. die Zeit und die Türnummer gespeichert werden.

Medien, die auch Daten speichern können, wie tragbare Computer oder Mobiltelefone, fallen nicht unter diese Regelung, da der Betroffene die Verarbeitungsprozesse selber steuern kann.

Auskunftspflicht gegenüber dem Betroffenen

Stellen, die diese Verarbeitungsmedien an Betroffene (z.B. Kunden oder Beschäftigte) rausgeben, haben nach § 6c BDSG eine besondere Auskunftspflicht gegenüber dem Betroffenen.

Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem

solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen

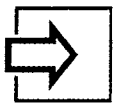
1. über ihre Identität und Anschrift,
2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,
3. darüber, wie er seine Rechte auf Auskunft, Berichtigung, Löschung oder Sperrung ausüben kann, und
4. über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen

unterrichten, soweit der Betroffene nicht auf andere Weise Kenntnis erlangt hat.

Geräte zur Wahrnehmung des Auskunftsrechts

Die verpflichtete Stelle hat dafür Sorge zu tragen, dass die erforderlichen **Geräte zur Wahrnehmung des Auskunftsrechts** unentgeltlich zur Verfügung gestellt werden.

Fazit



Neben der Regelung in Bezug auf die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten enthält das BDSG **weitere spezielle Vorgaben**, unter welchen Umständen personenbezogene Daten verarbeitet werden dürfen. Dieses sind folgende Vorgaben:

- Datenvermeidung und Datensparsamkeit – § 3a BDSG
- Automatisierte Einzelentscheidungen – § 6a BDSG
- Übermittlung personenbezogener Daten ins Ausland – §§ 4b und 4c BDSG
- Videoüberwachung – § 6b BDSG
- Mobile Speichermedien – § 6c BDSG

3.4 Technische und organisatorische Maßnahmen

Zielvorgaben

Das BDSG schreibt in § 9 technische und organisatorische Maßnahmen zum Datenschutz vor. In der Anlage zu § 9 BDSG sind **acht Zielvorgaben** aufgelistet, die bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zwingend einzuhalten sind.

3.4.1 Rechtliche Vorgaben

Nach § 9 BDSG haben nicht öffentliche Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung des BDSG, insbesondere die in der Anlage zu § 9 BDSG genannten Anforderungen, zu gewährleisten. Dabei sind Maßnahmen **nur erforderlich**, wenn ihr Aufwand in einem angemessenen Verhältnis zum Schutzzweck steht.

Datenschutz und Datensicherung

Im Zusammenhang mit dem § 9 BDSG tauchen in der einschlägigen Literatur die Begriffe „**Datenschutz**" und „**Datensicherung**" auf, wobei diese Vorschrift häufig als „Datensicherungsvorschrift" bezeichnet wird. Diese Unklarheit hat seine Ursache u.a. darin, dass bereits vor dem Inkrafttreten des ersten BDSG im Jahre 1977 die Unternehmen Datensicherungsmaßnahmen, wie den Schutz von Dateien, Datenträgern, Programmen und DV-Anlagen, ergriffen haben. Auch wenn viele Maßnahmen, die zur Datensicherung ergriffen werden, sich auch zur Ausführung der Datenschutzvorschriften eignen, bestehen jedoch in Bezug auf die Ziele grundsätzlich Unterschiede, die nicht verwischt werden sollten.

Schutzzweck

Unter **Datensicherung** versteht man die Summe an Maßnahmen zur Sicherung des ordnungsgemäßen Ablaufs der Datenverarbeitung durch Sicherung der Hard- und Software vor Verlust, Beschädigung oder Missbrauch oder unbefugtem Zugriff auf Daten. Beim **Datenschutz** geht es in erster Linie um die Verhinderung unzulässiger Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder anders ausgedrückt, geht es beim Datenschutz um den **Schutz der Persönlichkeitsrechte**, insbesondere bei der automatisierten Datenverarbeitung. Der Unterschied zwischen Datenschutz und Datensicherung ist am besten auf der Ebene des Schutzzwecks zu erkennen: Datensicherung dient dem Interesse der datenverarbeitenden Stelle (des Unternehmens); Datenschutz dagegen dient unmittelbar dem Schutz des Betroffenen (des Beschäftigten). Da das BDSG gemäß § 1 den Zweck hat, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlich-

keitsrecht beeinträchtigt wird, handelt es sich bei § 9 BDSG nicht um eine Datensicherungsvorschrift, **sondern um eine Vorschrift zum Datenschutz**. Die konkreten Datensicherungsmaßnahmen dienen im Einzelfall auch der Umsetzung des Datenschutzes. Vor diesem Hintergrund schreibt das BDSG nur Maßnahmen vor, die dem Schutzanspruch des Betroffenen dienen.

Verhältnismäßigkeitsprinzip

Die vorgeschriebenen technischen und organisatorischen Maßnahmen, die in der Anlage zu § 9 BDSG festgelegt sind, unterliegen ausdrücklich dem **Verhältnismäßigkeitsprinzip**: Die sind nur „erforderlich", d.h. von Gesetzes wegen vorgeschrieben, „wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht." Hierdurch wird klargestellt, dass nicht mit „Kanonen auf Spatzen" geschossen werden soll. Ein Missverständnis gilt es jedoch auszuschließen: Der Grundsatz der Verhältnismäßigkeit richtet sich nicht nach der Frage, **ob** die vom BDSG ausgesprochenen Ge- und Verbote zu beachten sind – damit wäre nämlich die Verbindlichkeit des BDSG aufgehoben –, sondern einzig und allein um Art und Umfang der Maßnahmen, die bewirken sollen, dass vom Gesetz gewollte Ereignisse oder Zustände auch nicht gegen den Willen der verantwortlichen Stelle (des Unternehmens) eintreten.

Technisch und organisatorisch

Die Begriffe „**technisch**" und „**organisatorisch**" sind weit auszulegen. So gehören zu den technischen Maßnahmen nicht nur diejenigen, die sich direkt auf Hard- und Software beziehen, sondern auch auf das gesamte bauliche Umfeld des Unternehmens. Organisatorische Maßnahmen gehen in der Regel auch mit personellen Regelungen (Vorkehrungen) einher, wie z.B. Zuordnung der Aufgaben, Befugnisse und Verantwortung, die Gestaltung des Arbeitsablaufs, die Zugangs- und Zugriffsregelungen oder die Vornahme von stichprobenartigen Erfolgskontrollen.

Mitbestimmung des Betriebsrats

Wegen der unterschiedlichen Verhältnisse in den einzelnen Unternehmen ist es nicht möglich, ein allgemein gültiges und für alle Unternehmen zu übernehmendes **Datenschutzkonzept** zu entwickeln. Vielmehr liegt es in der Verantwortung jeder einzelnen verantwortlichen Stelle, ein entsprechendes Datenschutzkonzept mit technischen und organisatorischen Datenschutzmaßnahmen zu erstellen. Die konkrete Umsetzung der technischen und organisatorischen Maßnahmen unterliegt der **Mitbestimmung des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG**, da bereits Maßnahmen, wie Vergabe von Passwörtern oder auch die Protokollierungen von Zugriffen, Leistungs- und Verhaltenskontrollen nach sich ziehen können. Gemäß § 31 BDSG ist zu beachten, dass personenbezogene Daten, die **ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung**

eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, nur für diese Zwecke verwendet werden dürfen.

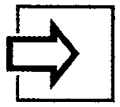
3.4.2 Technische und organisatorische Maßnahmen

Im BDSG werden **acht Zielvorgaben** genannt, deren Umsetzung dem Unternehmen obliegt. Diese Zielvorgaben ziehen an **Maßnahmen** z.B. die Sicherung des Gebäudes selbst nach sich durch Kontrolle über Pförtner oder Zugangskontrollsysteme. Zudem muss mit Zugriffsberechtigungen und Passwörtern und Protokollierungen gearbeitet werden.

„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

Fazit



Das Unternehmen hat gemäß § 9 BDSG technische und organisatorische Maßnahmen umzusetzen. Das BDSG enthält in der Anlage zu § 9 BDSG acht Zielvorgaben, die vom Unternehmen umzusetzen sind. Aus den Zielvorgaben resultieren z.B. folgende Maßnahmen:

- Vergabe von Passwörtern
- Zugriffsberechtigungskonzept
- Protokollierungen der Aktivitäten der Nutzer

Die technischen und organisatorischen Maßnahmen können Leistungs- und Verhaltenskontrollen der Beschäftigten nach sich ziehen. Durch § 31 BDSG ist dieses jedoch **nicht erlaubt**, denn die Maßnahmen dürfen nur der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage verwendet werden. Die Umsetzung der technischen und organisatorischen Maßnahmen unterliegt der **Mitbestimmung** des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG.

D

3.5 Kontrollinstanzen des Datenschutzes

Im Rahmen der Umsetzung des Datenschutzes kommt einer wirksamen Kontrolle ein hoher Stellenwert zu. Das **Kontrollsystem** umfasst die Kontrolle durch

- den Betroffenen,
- den bDSB als interne Kontrollinstanz,
- der Aufsichtsbehörde als externe Kontrollinstanz,
- den Betriebsrat.

3.6 Rechte des Betroffenen (Beschäftigten)

Informationelle Selbstbestimmung

Das BVerfG hat in seinem Urteil vom 15.12.1983 aus Artikel 1 Abs. 1 und Artikel 2 Abs. 1 GG ein Recht eines jeden Einzelnen auf informationelle Selbstbestimmung abgeleitet. Für die Existenz und Ausübung des Rechts auf informationelle Selbstbestimmung bildet die **Transparenz über die Datenverarbeitung** für den Betroffenen (Beschäftigten) eine zentrale Vorrausetzung. Das BVerfG führt dazu aus: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Lebensbereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner

Freiheit wesentlich gehemmt sein, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen, wer was bei welcher Gelegenheit über sie weiß." (BVerfG, Urteil v. 15.12.1983, Neue Juristische Wochenschrift 8/84, S. 419 ff.) Transparenz über die Verarbeitung personenbezogener Daten gehört zu den verfassungsrechtlich gewährleisteten Grundpositionen der Betroffenen (Beschäftigten). Zur möglichen Transparenz kann u.a. die Nutzung der in den §§ 33 bis 35 BDSG verankerten Rechte der Betroffenen beitragen.

Rechte der Betroffenen (Beschäftigten)

BDSG	Inhalt
§ 4 Abs. 3	Unterrichtung
§ 33	Benachrichtigung
§ 34 Abs. 1	Auskunft
§ 35	Berichtigung, Löschung, Sperrung
§ 6	Unabdingbarkeit der Rechte

Unterrichtungsrecht

Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, **zu unterrichten** über

- die **Identität der verantwortlichen Stelle**,
- die **Zweckbestimmungen** der Erhebung, Verarbeitung oder Nutzung,
- die **Empfänger von Daten** und zwar nur, soweit der Betroffene nach den Umständen des Einzelfalls nicht mit der Übermittlung an diese rechnen muss.

Recht auf Benachrichtigung

Werden erstmals personenbezogene Daten ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene gemäß § 33 Abs. 1 BDSG von

- der Speicherung,
- der Art der Daten,
- der Zweckbestimmung der Erhebung, Verarbeitung und Nutzung und
- der Identität der verantwortlichen Stelle

zu benachrichtigen.

Ausnahmen

§ 33 Abs. 2 BDSG sieht eine Fülle von **Ausnahmen** vor. So besteht z.B. eine Pflicht zur Benachrichtigung nicht, wenn „der Betroffene auf an-

dere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt" (§ 33 Abs. 2 Nr. 1 BDSG). So erhält nach allgemeiner Auffassung der Beschäftigte durch die Aushändigung seiner Lohn- oder Gehaltsabrechnung, die in der Regel automatisiert erstellt wird, „auf andere Weise Kenntnis", sodass im Arbeitsleben eine Benachrichtigungspflicht nicht beseht.

Recht auf Auskunft

Gemäß § 34 Abs. 1 BDSG kann der Betroffene Auskunft verlangen über

- die zu seiner Person gespeicherten Daten,
- die Herkunft,
- den oder die Empfänger und
- den Zweck der Speicherung.

Die Auskunft ist von der verantwortlichen Stelle (Arbeitgeber) schriftlich zu erteilen und ist nach § 34 Abs. 5 BDSG **unentgeltlich**.

Recht auf Datenkorrektur

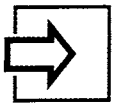
In § 35 BDSG werden die Rechte der Betroffenen auf Datenkorrektur bei unrichtiger und unzulässiger Datenverarbeitung geregelt. So bestehen unter bestimmten Umständen Rechte auf

- Berichtigung (§ 35 Abs. 1 BDSG),
- Löschung (§ 35 Abs. 2 BDSG) und
- Sperrung (§ 35 Abs. 3 und 4 BDSG).

Unabdingbarkeit der Rechte

Die Rechte der §§ 34 und 35 BDSG sind gemäß § 6 BDSG **unabdingbar und können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden**. Demzufolge sind Vereinbarungen, z.B. im Rahmen von Arbeitsverträgen oder Betriebsvereinbarungen, unwirksam, die diese Rechte ganz oder teilweise ausschließen. Da das Recht auf informationelle Selbstbestimmung (Datentransparenz) ein bedeutendes Rechtsgut ist, ist es nur konsequent, dass durch § 6 BDSG die Vertragsfreiheit eingeschränkt wird. Denn insbesondere in Abhängigkeitsverhältnissen, wie Arbeitsvertragsverhältnissen, ist der schwächere Vertragspartner (Arbeitnehmer) bereit, auf seine Rechte zu verzichten.

Fazit



Die Betroffenen (z.B. Bewerber oder Beschäftigter) haben folgende Rechte, die auch häufig in Betriebsvereinbarungen aufgenommen werden:

- Unterrichtung – § 4 Abs. 3 BDSG
- Benachrichtigung – § 33 BDSG
- Auskunft – § 34 Abs. 1 BDSG
- Berichtigung, Löschung und Sperrung § 35 BDSG

Diese Rechte sind **unabdingbar** und können somit nicht durch ein Rechtsgeschäft, z.B. durch Betriebsvereinbarung oder durch Arbeitsvertrag, ausgeschlossen werden.

3.7 Betrieblicher Datenschutzbeauftragter

Das BDSG sieht für nicht öffentliche Stellen (also für jedes Unternehmen) die Bestellung eines BDSB zwingend vor, wenn mehr als vier Beschäftigte personenbezogene Daten erheben, verarbeiten oder nutzen. Die Aufgaben des BDSB sind in § 4g BDSG in Form einer **Generalklausel** und durch eine **nicht** abschließende Aufzählung von Einzelaufgaben festgelegt.

3.7.1 Generalklausel

Nach § 4g Satz 1 BDSG hat der BDSB auf die Einhaltung des BDSG sowie anderer Vorschriften über den Datenschutz **hinzuwirken**. „Hinwirken" bedeutet, dass das Unternehmen für die Umsetzung des Datenschutzes verantwortlich ist.

Einhaltung des BDSG

Bei der Aufgabe, auf die Einhaltung des BDSG hinzuwirken, hat der bDSB

- das BDSG in **konkrete Verhaltensregeln** umzusetzen,
- die Prüfung der **Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung** vorzunehmen,
- die Vorgabe von **Datenvermeidung und Datensparsamkeit** umzusetzen,
- dafür zu sorgen, dass die **Individualrechte der Beschäftigten** auf Benachrichtigung, Auskunft, Berichtigung, Löschung und Sperrung gemäß § 33 ff. BDSG beachtet werden,

- die Umsetzung der technisch-organisatorischen Maßnahmen gemäß § 9 BDSG und der Anlage zu § 9 zu überwachen.

Einhaltung anderer Rechtsvorschriften

Der bDSB hat aber auch auf die Einhaltung **anderer Rechtsvorschriften** über den Datenschutz hinzuwirken. Hierzu zählen in Bezug auf den Beschäftigten-Datenschutz folgende Vorschriften:

- freie Entfaltung der Persönlichkeit (§ 75 Abs. 2 BetrVG)
- Informations- und Beteiligungsrechte des Betriebsrats
- Begrenzung der Fragen bei Personalfragebogen
- Begrenzung der Angaben in schriftlichen Arbeitsverträgen
- Recht auf Akteneinsicht (§ 83 BetrVG)
- Betriebsvereinbarungen und Sprüche der Einigungsstelle

3.7.2 Ausdrücklich genannte Einzelaufgaben

In § 4g Abs. 1 Satz 3 BDSG sind unter den Nummern 1 bis 2 wichtige Beispiele aufgezählt. Der Gesetzgeber konnte und wollte nur diesen **Mindestkatalog** vorschreiben, da er auf die Organisationsfreiheit des privaten Bereichs nur soweit einwirken darf, als dies unbedingt notwendig ist.

Überwachung der ordnungsgemäßen Programmanwendung

Nach § 4g Abs. 1 Nr. 1 BDSG hat der bDSB die **ordnungsgemäße Anwendung der Datenverarbeitungsprogramme**, mit deren Hilfe personenbezogene Daten verarbeitet werden, zu überwachen. In diesem Zusammenhang muss der bDSB insbesondere sicherstellen, dass datenschutzspezifische Vorschriften wie die Zulässigkeit der Datenverarbeitung und -nutzung (§ 4 Abs. 1 BDSG), die Verpflichtung auf das Datengeheimnis und die Einhaltung der technischen und organisatorischen Datenschutzmaßnahmen (§ 9 BDSG) durchgeführt werden.

Hierzu ist es notwenig, dass der bDSB rechtzeitig, d.h. bereits in der Planungsphase, über die einzuführenden Programme und Geräte vom Arbeitgeber unterrichtet wird. Die Informationen müssen daher vom Umfang und Inhalt mindestens den Informationen entsprechen, die dem Betriebsrat gegeben werden müssen. So kann der bDSB eigene Vorschläge rechtzeitig entwickeln, die dann auch Berücksichtigung finden können.

Schulung des DV-Personals

Nach § 4g Abs. 1 Nr. 2 BDSG hat der bDSB die bei der Verarbeitung personenbezogener Daten tätigen Personen mit den Vorschriften des BDSG und anderen Rechtsvorschriften über den Datenschutz vertraut zu machen. Dadurch soll bei den Beschäftigten, die personenbezogene Daten verarbeiten, das Bewusstsein für Bedeutung und Notwendigkeit

des Datenschutzes geschaffen werden. Da dieses die ausdrückliche und alleinige Aufgabe des bDSB ist, ist er im Rahmen seiner Weisungsfreiheit berechtigt, unter Berücksichtigung der Erfordernisse des Unternehmens selbst zu bestimmen, **welches die geeigneten Maßnahmen zur Schulung der Mitarbeiter sind**.

Erforderliche Mittel, Verpflichtung der Beschäftigten

Der Arbeitgeber hat die **erforderlichen Mittel**, Räume usw. bereitzustellen, wobei die Schulungen während der Arbeitszeit stattzufinden haben. Die Schulung der Mitarbeiter ist sowohl wesentliche Voraussetzung für die konsequente Umsetzung des BDSG überhaupt als auch für eine Verpflichtung der Beschäftigten auf das Datengeheimnis. So sollte die **Verpflichtung der Beschäftigten gemäß § 5 BDSG** nur nach einer entsprechenden Schulung erfolgen. Da es sich bei den Schulungen um betriebliche Fortbildung handelt, unterliegen diese Maßnahmen der Beteiligung des Betriebsrats nach den §§ 96 bis 98 BetrVG.

Vorabkontrolle

Über die ohnehin vorgegebene Zulässigkeitsprüfung nach § 4 BDSG hinaus ist bei der Datenverarbeitung mit **besonderen Risiken für die Betroffenen** gemäß § 4d Abs. 5 BDSG eine Vorabkontrolle durchzuführen. Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen diese der Prüfung vor Beginn der Verarbeitung. Eine **Vorabkontrolle ist insbesondere dann durchzuführen**, wenn

- **besondere Arten personenbezogener Daten** verarbeitet werden oder
- die Verarbeitung personenbezogener Daten dazu bestimmt ist, die **Persönlichkeit des Betroffenen zu bewerten**, einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens.

In beiden Fällen ist die Vorabkontrolle nur dann durchzuführen, wenn der Verarbeitung weder eine gesetzliche Verpflichtung noch eine Einwilligung zugrunde liegt und sie auch nicht im Rahmen eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses erfolgt. Das bedeutet, dass im Bereich des Beschäftigten-Datenschutzes nur dann eine Vorabkontrolle stattfinden muss, wenn der Arbeitgeber Datenverarbeitung betreiben will, **die möglicherweise über die Zweckbestimmung des Vertragsverhältnisses hinausgehen soll**. Bei der Planung von Datenverarbeitungssystemen in der betrieblichen Praxis ist dieses häufig der Fall.

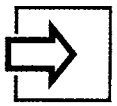
Führen von Übersichten

Nach § 4g Abs. 2 BDSG hat der Arbeitgeber dem bDSB **Übersichten zur Verfügung zu stellen**. Es handelt sich dabei um Übersichten über

- Name oder Firma der verantwortlichen Stelle,

- Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung befassten Personen,
- Anschrift der verantwortlichen Stelle,
- Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung,
- eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten,
- Empfänger, denen die Daten mitgeteilt werden können,
- Regelfristen für die Löschung von Daten,
- eine geplante Übermittlung in Drittstaaten,
- eine allgemeine Beschreibung, die es ermöglicht, vollständig zu beurteilen, ob die Maßnahmen nach § 9 BSDG angemessen sind,
- zugriffsberechtigte Personen.

Fazit



Der bDSB hat auf die Umsetzung des BDSG und anderer Rechtsvorschriften zum Datenschutz hinzuwirken. Der bDSB somit beratene Funktion und hat vom BDSG her nicht die Befugnis, Maßnahmen zum Datenschutz umzusetzen. Die Verantwortung für die Umsetzung des BDSG einschließlich der Haftung liegt beim Unternehmen (bzw. beim Geschäftsführer).

3.8 Die Aufsichtsbehörde

Neben der internen Kontrolle durch die Beschäftigten selbst, durch den betrieblichen Datenschutzbeauftragten oder durch den Betriebsrat sieht das BDSG eine so genannte Fremdkontrolle vor. Für diese Fremdkontrolle im nicht öffentlichen Bereich ist die **Aufsichtsbehörde für den Datenschutz zuständig**.

Im Internet

Nach § 38 Abs. 6 BDSG hat der Bund diese Aufgaben den Bundesländern übertragen. Etliche Bundesländer haben diese Aufgabe ihren Innenministerien (z.B. Baden-Württemberg, Brandenburg, Mecklenburg-Vorpommern, Saarland) oder den Regierungsbezirken (z.B. Bayern, Hessen, Sachsen) übertragen. In anderen Ländern wie Berlin, Bremen, Hamburg, Niedersachen oder Nordrhein-Westfalen ist die Kontrollaufgabe den Landesbeauftragen für den Datenschutz zugewiesen worden. In Schleswig-Holstein ist sowohl für den öffentlichen als auch für den nicht öffentlichen Bereich das Unabhängige Landes-

zentrum für den Datenschutz zuständig. Die aktuellen Adressen sind unter www.bund.de/anschriften/index.html abrufbar.

3.8.1 Überblick über Aufgaben und Befugnisse

Aufgaben und Befugnisse

Die Aufsichtsbehörde hat die Aufgabe, die Ausführung des BDSG sowie anderer Vorschriften über den Datenschutz zu kontrollieren. Dabei darf die Aufsichtsbehörde die von ihr gespeicherten Daten nur für die Zwecke der Aufsicht verarbeiten und nutzen. Die Aufsichtsbehörde hat u.a. folgende Aufgaben und Befugnisse:

- Sie führt ein **Register** über bestimmte Datenverarbeitungen, die ihr gemäß § 4d Abs. 1 BDSG zu melden sind.
- Sie ist **Beschwerdestelle**, an die sich jedermann wenden kann, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch nicht öffentliche Stellen (Privatbetriebe) in seinen Rechten verletzt worden zu sein.
- Darüber hinaus hat die Aufsichtsbehörde ein umfassendes Kontrollrecht, was bedeutet, dass sie unabhängig von einer vorliegenden Beschwerde oder eines sonstigen Anhaltspunkts für Datenschutzverstöße, also aus eigener Initiative, Kontrollen durchführen kann. Das heißt, die Aufsichtsbehörde kann **anlassunabhängige Kontrollen** jederzeit durchführen.
- Zur Wahrnehmung dieser Aufgaben hat die Aufsichtsbehörde **umfangreiche Kontrollbefugnisse**. Sie hat das Recht,
  - Auskünfte zu verlangen,
  - Grundstücke und Geschäftsräume zu besichtigen,
  - dort Prüfungen durchzuführen und
  - Einsicht in die Datenverarbeitungsprogramme zu nehmen.
- Das betroffene Unternehmen hat dementsprechende Auskunfts-, Duldungs- und Mitwirkungspflichten.
- Stellt die Aufsichtsbehörde Datenschutzverstöße fest, stehen ihr verschiedene **Sanktionsmöglichkeiten** zur Verfügung. Dieses umfasst die Anordnung zur Beseitigung technischer und organisatorischer Mängel (§ 9 BDSG) bis hin zur Einleitung eines Bußgeldverfahrens und zur Stellung eines Strafantrags gegenüber der für das Unternehmen verantwortlichen Person.
- Bestimmte Datenübermittlungen in Staaten außerhalb der Europäischen Union, bei denen kein angemessenes Datenschutzniveau besteht, bedürfen der vorherigen **Genehmigung** der Aufsichtsbehörde.
- Die Aufsichtsbehörde hat auch **Beratungs- und Informationsaufgaben**.

3.8.2 Führen von Registern

Register Die Aufsichtsbehörde führt ein **Register** der meldepflichtigen Datenverarbeitungen mit den nach § 4e BDSG benötigten Angaben. Meldepflichtig sind nur die Stellen, die **geschäftsmäßig** personenbezogene Daten speichern. Geschäftsmäßige Datenverarbeitung liegt dann vor, wenn diese der Werbung, der Tätigkeit von Auskunfteien, dem Adresshandel oder der Markt- und Meinungsforschung dient. Die von der Aufsichtsbehörde geführten Register können von jedermann eingesehen werden.

3.8.3 Beschwerdestelle

Bearbeitung von Eingaben Die **Bearbeitung von Eingaben** gehört zu den Hauptaufgaben der Aufsichtsbehörde. In § 21 BDSG wird deutlich gemacht, dass sich jedermann (hierzu gehören natürlich auch Mitglieder des Betriebsrats oder auch einzelne Beschäftigte) an die Aufsichtsbehörde wenden kann, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten in seinen Rechten verletzt worden zu sein. Die Anrufung ist **an keine Form oder Frist** gebunden. Sie kann also auch mündlich erfolgen. Dabei darf die Aufsichtsbehörde gegenüber der verantwortlichen Stelle (also z.B. gegenüber dem Unternehmen) den Betroffenen weder nennen noch Angaben machen, die Rückschlüsse auf seine Person zulassen.

Wird die Eingabe von dem Betroffenen nicht bei der zuständigen Aufsichtsbehörde getätigt, so darf diese zwar die Eingabe wegen Unzuständigkeit zurückweisen, muss sie aber an die zuständige Kontrollstelle weiterleiten.

3.8.4 Kontrolle von Amts wegen

Kontrollbefugnisse Die Aufsichtsbehörde hat die Aufgabe, die Ausführung des BDSG und anderer Vorschriften über den Datenschutz zu kontrollieren. Die **Kontrollbefugnisse** der Aufsichtsbehörde umfassen das Recht,

- Auskünfte zu verlangen,
- Grundstücke und Geschäftsräume zu besichtigen,
- dort Prüfungen durchzuführen und
- Einsicht in die Datenverarbeitungsprogramme zu nehmen.
- Auskunftspflichten der verantwortlichen Stelle

3.8.5 Die Auskunftspflichten der verantwortlichen Stelle

Auskunftsverweigerungsrecht

Gemäß § 38 Abs. 3 BDSG sind die der Kontrolle unterliegenden Stellen zu allen erforderlichen Auskünften verpflichtet. Auch wenn der betriebliche Datenschutzbeauftragte dabei nicht ausdrücklich erwähnt wird, ist es sinnvoll, ihn an der Prüfung der Aufsichtsbehörde zu beteiligen. Die Auskunft hat **unverzüglich** zu erfolgen, wobei sie **vollständig und wahrheitsgemäß** sein muss. Der Auskunftspflichtige hat nur dann nach § 38 Abs. 3 Satz 2 BDSG ein **Auskunftsverweigerungsrecht**, wenn er sich oder einen Angehörigen i.S.d. § 383 Abs. 1 Nr. 1 bis 3 Zivilprozessordnung durch die Beantwortung bestimmter Fragen der Gefahr der Strafverfolgung oder der Belangung wegen einer Ordnungswidrigkeit aussetzen würde. Der Auskunftspflichtige ist von den Mitarbeitern der Aufsichtsbehörde darauf hinzuweisen. Eine Verletzung dieser Belehrung würde die Kontrollergebnisse rechtswidrig machen und könnte zu einem Verwertungsverbot führen.

Ordnungswidrigkeit

Kommen die geprüften Unternehmen ihrer Auskunftspflicht nicht nach, ist dies eine **Ordnungswidrigkeit** nach § 43 Abs. 1 Nr. 10 BDSG, es sei denn, dass ein Auskunftsverweigerungsrecht vorliegt.

3.8.6 Besichtigungs- und Prüfungsrechte

Prüfungen und Besichtigungen

Die von der Aufsichtsbehörde beauftragten Personen sind befugt, Grundstücke und Geschäftsräume während der Geschäftszeiten zu betreten und dort **Prüfungen und Besichtigungen** vorzunehmen. Sie können auch geschäftliche Unterlagen einsehen. Hierzu gehören insbesondere die von der verantwortlichen Stelle zu führenden Übersichten, die Datenverarbeitungsprogramme sowie die gespeicherten personenbezogenen Daten. Die Stelle – also die Auskunftspflichtige – hat die Maßnahmen zu dulden.

3.8.7 Abberufung des betrieblichen Datenschutzbeauftragten

Die Aufsichtsbehörde hat zudem die Befugnis, die **Abberufung des betrieblichen Datenschutzbeauftragten** zu verlangen, wenn dieser die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt. In der Regel wird die Aufsichtsbehörde bei fehlender Fachkunde des Datenschutzbeauftragten aufgeben, entsprechende Schulungen zu besuchen. Bestehen jedoch Zweifel an der Zuverlässigkeit und zwar in Bezug auf mögliche Interessenkonflikte, wenn der Datenschutzbeauftragte beispielsweise auch die Leitung der EDV innehat, wird die Abberufung durch die Aufsichtsbehörde angeordnet werden.

3.8.8 Kontrolle der Datenübermittlung in Drittstaaten

Angemessenes Datenschutz-Niveau

Wollen Unternehmen personenbezogene Daten in Staaten außerhalb der Europäischen Union bzw. an Staaten übermitteln, die nicht zu den Staaten des Europäischen Wirtschaftsraums gehören (das BDSG spricht hier von Drittstaaten), muss entweder in den Staaten ein **angemessenes Datenschutz-Niveau** bestehen oder aber die Unternehmen können auf die Ausnahmen in § 4c BDSG zurückgreifen.

Vertragliche Regelungen

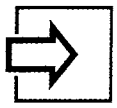
Sind diese Möglichkeiten für das Unternehmen nicht gegeben, kann die zuständige Aufsichtsbehörde einzelne Übermittlungen oder bestimmte Arten von Übermittlungen genehmigen. Dazu muss die verantwortliche Stelle hinsichtlich des Schutzes der Persönlichkeitsrechte ausreichende Garantien vorweisen. Diese Garantien können durch **vertragliche Regelungen** oder durch **verbindliche Unternehmensregeln** (z.B. bei weltweit agierenden Konzernen) geschaffen werden.

3.8.9 Aufsichtsbehörde als Beratungs- und Informationsstelle

Umfassendes Beratungsrecht

Der Beratung der Aufsichtsbehörde kommt gerade wegen der komplizierten Gesetzeslage eine große Bedeutung zu. So kann sich der betriebliche Datenschutzbeauftragte in Zweifelsfällen – z.B. bei Unsicherheiten in Bezug auf die Auslegung des BDSG – an die Aufsichtsbehörde wenden (§ 4g Abs. 1 BDSG). Gemäß § 4d Abs. 6 BDSG muss er sich sogar an die Aufsichtsbehörde wenden, wenn sich bei der Durchführung einer Vorabkontrolle Zweifelsfragen ergeben. Auch wenn in § 38 BDSG keine gesetzliche Regelung für die Beratung enthalten ist, **hat die Aufsichtsbehörde jedoch ein umfassendes Beratungsrecht**. Nach ihrem Selbstverständnis sehen sich die Aufsichtsbehörden überwiegend zu dieser Dienstleistung gegenüber Bürgern und Unternehmen verpflichtet. Den Servicecharakter kann man auch an der sehr umfangreichen Präsenz der Aufsichtsbehörden im Internet ablesen. Darüber hinaus veröffentlichen die Aufsichtsbehörden regelmäßig, spätestens alle zwei Jahre, einen **Tätigkeitsbericht**.

Fazit



Als externe Instanz für die Kontrolle der Einhaltung des BDSG ist die Aufsichtsbehörde zuständig. Sie hat folgende Aufgaben und Funktionen:

- Führen von Registern
- Beschwerdestelle
- Kontrolle der Unternehmen
- Besichtigungs- und Prüfungsrechte
- Abberufung des bDSB
- Kontrolle der Datenübermittlung in Drittstaaten
- Beratungs- und Informationsstelle

Jedermann, also auch Beschäftigte und Betriebsräte, kann sich an die Aufsichtsbehörde wenden.

4 Handlungsmöglichkeiten des Betriebsrats

Die Individualrechte des einzelnen Beschäftigten, die sich aus dem BDSG ergeben, werden durch die **Beteiligungsrechte des Betriebsrats** verstärkt.

D

BetrVG	Inhalt der Bestimmung
§ 75 Abs. 2	Schutz und Förderung der freien Entfaltung der Persönlichkeit
§ 80 Abs. 1 Nr. 1	Kontrolle der Einhaltung der zugunsten der Arbeitnehmer bestehenden Datenschutzregelungen
§ 80 Abs. 2	rechtzeitige und umfassende Unterrichtung anhand von Unterlagen
§ 90	Unterrichtung und Beratung bei der Einführung von technischen Anlagen
§ 87 Abs. 1 Nr. 6	Mitbestimmung bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, Leistung und Verhalten der Arbeitnehmer zu überwachen
§ 94 Abs. 1	Mitbestimmung bei Personalfragebogen
§ 77	Betriebsvereinbarungen

4.1 Schutz der Persönlichkeitsrechte

- Freie Entfaltung der Persönlichkeit schützen und fördern
- Heimliches Mithören von Telefongesprächen
- Heimliche Videoüberwachung

Nach § 75 Abs. 2 BetrVG haben der Arbeitgeber und der Betriebsrat die **freie Entfaltung der Persönlichkeit** der im Betrieb beschäftigten Arbeitnehmer **zu schützen und zu fördern**. Bereits nach Artikel 2 Abs. 1 GG hat jeder Beschäftigte das Recht auf freie Entfaltung der Persönlichkeit. Dieser Grundsatz hat seinen Niederschlag in das BetrVG gefunden, da die freie Entfaltung der Persönlichkeit u.a. durch Technisierung, Rationalisierung und die zunehmende Verarbeitung personenbezogener Daten in besonderem Maße gefährdet ist. Rechtswidrige Eingriffe in die Persönlichkeitssphäre können bei der Durchführung von betrieblichen Kontrollmaßnahmen erfolgen. Auch wenn die Kontrolle insbesondere der Mitbestimmung des Betriebsrats nach

§ 87 Abs. 1 Nr. 1 und 6 BetrVG unterliegt, sind dennoch bestimmte Kontrollmaßnahmen unzulässig. Die Zulässigkeit von Eingriffen in die Persönlichkeitsrechte kann auch durch das Mitbestimmungsrecht nicht erweitert werden. So ist stets eine akustische Überwachung der Arbeitnehmer durch Abhörgeräte oder Tonbandaufnahmen unzulässig. Das Gleiche gilt für das Abhören oder **heimliche Mithören von Telefongesprächen** (vgl. BVerfG, Beschluss v. 19.12.1991 – 1 BVR 382/85 –, RDV 3/92, S. 121 ff.) oder für **heimliche Videoüberwachung**. Das BDSG hat in einem konkreten Einzelfall unter bestimmten Voraussetzungen die heimliche Videoüberwachung für zulässig gehalten (vgl. BAG, Urteil v. 27.03.2003 – 2 AZR 51/02 –, RDV 6/03, S. 293 ff.).

In einem aktuellen Urteil will das Bundesarbeitsgericht die Verwertung von verdeckter Videoüberwachung zulassen, und zwar dann, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zulasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind, die verdeckte Videoüberwachung praktisch das einzig verbleibende Mittel darstellt und insgesamt nicht unverhältnismäßig ist (vgl. BAG, Urteil v. 27.3.2003 – 2 AZR 51/02 –, RDV 6/2003, S. 293 ff.).

4.2 Überwachungsrecht

Mögliche rechtswidrige Eingriffe in die Persönlichkeitssphäre können durch die weitreichenderen Überwachungs- und Mitbestimmungsrechte abgewehrt werden. Nach § 80 Abs. 1 Nr. 1 BetrVG **hat der Betriebsrat darüber zu wachen**, dass die zugunsten der Arbeitnehmer geltenden Gesetze, Verordnungen, Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen durchgeführt werden. Ein Gesetz i.S.d. § 80 Abs. 1 Nr. 1 BetrVG bildet das BDSG. So hat der Betriebsrat, um nur einige Beispiele aufzuführen, die Pflicht, **folgende Aspekte zu überwachen**:

z.B.

- *die Rechtmäßigkeit der Verarbeitung personenbezogener Daten (§ 4 BDSG)*
- *Datenvermeidung und Datensparsamkeit (§ 3a BDSG)*
- *die Umsetzung der technischen und organisatorischen Datenschutzmaßnahmen (§ 9 BDSG)*
- *die Gewährleistung der Rechte der Betroffenen (§§ 33 bis 35 BDSG)*
- *die Aufgabenerfüllung des bDSB (§§ 4f und g BDSG)*

Die Überwachungsrechte und -pflichten beinhalten auch eine Schutzfunktion in Bezug auf den bDSB. So wird der Betriebsrat aktiv werden müssen, wenn z.B die Weisungsfreiheit des bDSB beeinträchtigt ist oder Verstöße gegen das Benachteiligungsverbot zu erkennen sind.

Zutrittsrecht zu allen Räumen

Zur Prüfung der Einhaltung der zugunsten der Arbeitnehmer geltenden Vorschriften hat der Betriebsrat **ein Zutrittsrecht zu allen Räumen und Betriebsteilen**, wobei dem Arbeitgeber kein Prüfungsrecht zusteht, ob das Betreten dieser Räume im Einzelfall notwendig ist. Stellt der Betriebsrat Rechtsverstöße fest, hat er den Arbeitgeber darauf hinzuweisen und auf Abhilfe zu drängen. Der Betriebsrat hat jedoch nicht die Möglichkeit, die Einhaltung der Vorschriften kraft eigenen Rechts im Beschlussverfahren durchzusetzen (vgl. BAG v. 10.6.1986, EzA Nr. 26). Er kann sich jedoch bei Verstößen gegen das Datenschutzrecht an die Aufsichtsbehörde wenden, wenn der Arbeitgeber keine Abhilfe schafft.

Das Überwachungsrecht des Betriebsrats wird nicht dadurch berührt, dass auch dem bDSB die Sicherstellung des BDSG und anderer datenschutzrechtlicher Vorschriften obliegt.

4.3 Informationsrecht

Um der Überwachungspflicht und auch der Umsetzung entsprechender Mitbestimmungsrechte nachzukommen, steht dem Betriebsrat ein **umfassendes Informationsrecht** zu. Nach § 80 Abs. 2 BetrVG ist der Betriebsrat **rechtzeitig und umfassend** zu unterrichten. Ihm sind auf Verlangen jederzeit die zur Durchführung seiner Aufgaben erforderlichen Unterlagen zur Verfügung zu stellen. Die Unterrichtung durch den Arbeitgeber soll den Betriebsrat in die Lage versetzen, **in eigener Verantwortung zu prüfen**, ob sich für ihn Aufgaben ergeben und ob er zur Wahrnehmung dieser Aufgaben tätig werden muss. In Bezug auf die Einführung und Anwendung von DV-Systemen, u.a. zur Wahrnehmung seines Überwachungs- aber auch des Mitbestimmungsrechts, hat das BAG (vgl. BAG, Beschluss v. 17.3.1987 – 1 ABR 59/85 –, Arbeitsrecht im Betrieb 12/87, S. 287 ff.) festgestellt, dass der Betriebsrat insbesondere über folgende Punkte zu informieren ist bzw. ihm **folgende Unterlagen zur Verfügung zu stellen sind**:

Folgende Unterlagen

- Übersicht über alle bestehenden Dateien, in denen personenbezogene Daten der bei ihm beschäftigten Arbeitnehmer gespeichert sind, gleichgültig, ob die Speicherung im eigenen Unternehmen oder bei einem anderen Unternehmen erfolgt

- personenbezogene Daten, die beim Arbeitgeber selbst verarbeitet werden
- personenbezogene Daten, die an andere Unternehmen übermittelt werden
- Maßnahmen, die getroffen werden, um sicherzustellen, dass die an andere Unternehmen übermittelten Daten nur zu den vereinbarten Zwecken verarbeitet werden
- die eingesetzten Programme mit Namen und Kurzbeschreibung
- das Pflichtenheft, den Datenflussplan und die Systembeschreibung

Vorabkontrolle, angemessenes Datenschutzkonzept

Zu den Informationen gehören auch **die Ergebnisse einer Vorabkontrolle**, die der bDSB durchzuführen hat. Zudem müssen die Unterlagen auch ein **angemessenes Datenschutzkonzept** (vgl. BVerwG, Beschluss v. 8.11.1989 – BVerwG 6 9 7.87 –, RDV 3/90, S. 141 ff.), wie Zugriffsberechtigungskonzept, Umfang der Protokollierungen, Löschungsfristen etc., erkennen lassen.

Diese Informationen entsprechen in Teilen den Übersichten nach § 4e BDSG, die dem bDSB gemäß § 4g BDSG vom Unternehmen zur Verfügung zu stellen sind.

4.4 Informations- und Beratungsrecht

§ 90 BetrVG enthält ebenfalls ein Informationsrecht und zusätzlich ein Beratungsrecht des Betriebsrats. Nach § 90 Abs. 1 hat der Arbeitgeber den Betriebsrat über die **Planung**

- von Neu-, Um- und Erweiterungsbauten von Fabrikations-, Verwaltungs- und sonstigen betrieblichen Räumen,
- von technischen Anlagen,
- von Arbeitsverfahren und Arbeitsabläufen oder
- der Arbeitsplätze

rechtzeitig unter Vorlage der erforderlichen Unterlagen zu unterrichten.

Zu den technischen Anlagen gehören auch die IuK-Techniken, wobei die Unterrichtung **rechtzeitig über die Planung zu erfolgen hat**. Da der Plan das Ergebnis der Planung ist, muss demnach der Betriebsrat **vor der eigentlichen Planerstellung unterrichtet werden**. Der Betriebsrat hat zusätzlich ein Beratungsrecht insbesondere über die vorgesehenen Maßnahmen und ihre Auswirkungen auf die Arbeitnehmer, auf die Art ihrer Arbeit sowie die sich daraus ergebenden Anforderungen an die Arbeitnehmer. Bei den Beratungen sollen Ar-

beitgeber und Betriebsrat die **gesicherten arbeitswissenschaftlichen Erkenntnisse** über die menschengerechte Gestaltung der Arbeit berücksichtigen. Zu den arbeitswissenschaftlichen Erkenntnissen gehört auch die Rechtsprechung und herrschende Meinung zum Datenschutz. Neben Informations- und Beratungsrecht hat der Betriebsrat nach § 91 BetrVG ein **korrigierendes Mitbestimmungsrecht**, das, soweit ersichtlich, in der Praxis nicht genutzt wird.

4.5 Mitbestimmungsrechte

Die zentralen **Mitbestimmungsrechte** für Regelungen im Bereich des Beschäftigten-Datenschutzes sind für die Erhebung von Daten der § 94 BetrVG und für die Verarbeitung und Nutzung von Daten der § 87 Abs. 1 Nr. 6 BetrVG.

4.5.1 Personalfragebogen

Nach § 94 Abs. 1 BetrVG **bedürfen Personalfragebogen der Zustimmung des Betriebsrats.** Kommt eine Einigung über den Inhalt nicht zustande, so entscheidet die Einigungsstelle. Der Spruch der Einigungsstelle ersetzt die Einigung zwischen Arbeitgeber und Betriebsrat.

Präventiver Schutz der Persönlichkeitsrechte

Das Mitbestimmungsrecht soll sicherstellen, dass die Fragen des Arbeitgebers im Rahmen des Einsatzes von Personalfragebogen auf die Umstände und Gegenstände beschränkt bleibt, für die ein berechtigtes Interesse des Arbeitgebers besteht. Das Mitbestimmungsrecht dient dem **präventiven Schutz der Persönlichkeitsrechte bei der Datenerhebung**. So sollen der Arbeitnehmer und auch der **Bewerber** um einen Arbeitsplatz davor bewahrt werden, dem Arbeitgeber mehr aus ihrer Privat- und Intimsphäre an Informationen preisgeben zu müssen, als dies für die Zweckbestimmung des Arbeitsverhältnisses bzw. vertragsähnlichen Vertrauensverhältnisses erforderlich ist. Neben dem Schutz der Persönlichkeitsrechte soll das Mitbestimmungsrecht zu einer **Versachlichung und zu einer Objektivierung der betrieblichen Personalführung beitragen**. Das Mitbestimmungsrecht ist als Zustimmungserfordernis ausgestattet, d.h., dass der Betriebsrat kein Initiativrecht besitzt. Da § 94 Abs. 1 BetrVG keine Pflicht zur Einführung eines Fragebogens statuiert, kann der Betriebsrat dies auch nicht erzwingen, wobei er jedoch sehr wohl die Einführung anregen kann.

Keine Definition

Das BetrVG selbst enthält keine Definition dafür, was unter einem Personalfragebogen zu verstehen ist. Es wird jedoch allgemein anerkannt, dass unter einem Personalfragebogen die formularmäßige Zusammenfassung von Fragen über die persönlichen Verhältnisse, insbe-

sondere über Eignung, Kenntnisse und Fähigkeiten einer Person zu verstehen ist.

Das Mitbestimmungsrecht beschränkt sich nicht nur auf formularmäßige, schematisierte Fragen des Arbeitgebers, die vom Bewerber/Arbeitnehmer selbst auszufüllen sind. Es handelt sich auch dann um einen Personalfragebogen, wenn auf andere Art und Weise Bewerber oder Arbeitnehmer **standardisierte Fragen** zu beantworten haben, insbesondere wenn es sich um die schriftliche formularmäßige Zusammenfassung von Fragen über persönliche Eignung handelt. So ist die allgemeine Meinung, dass § 94 BetrVG auch dann anwendbar ist, wenn die Fragen an den Bewerber bzw. dann den Arbeitnehmer anhand eines standardisierten Fragenkatalogs, einer **Checkliste vom Arbeitgeber** mündlich gestellt und die Antworten vom Fragenden festgehalten werden. Das Mitbestimmungsrecht bezieht sich nicht nur auf Fragebogen im engeren Sinne, also auf schriftlich niedergelegte Fragen, die ein Beschäftigter oder ein Bewerber schriftlich beantwortet. Die Vorschrift findet vielmehr auf **alle formalisierten, standardisierten Informationserhebungen des Arbeitgebers** im Hinblick auf Arbeitnehmerdaten Anwendung. Es kann also nicht darauf ankommen, auf welche technische Art und Weise die Befragung eines Bewerbers bzw. Arbeitnehmers erfolgt. Ansonsten würde § 94 Abs. 1 BetrVG zu einer für die Arbeitnehmer belanglosen Norm degenerieren, könnte der Arbeitgeber die ihn interessierenden Fragen, die er mangels Zustimmung des Betriebsrats nicht unterbringen konnte, am Betriebsrat vorbei in einem Personalinterview stellen.

Beantwortung der Fragen wird freigestellt

Für die Anwendung des Mitbestimmungsrechts nach § 94 Abs. 1 BetrVG ist es ebenfalls unerheblich, ob die Fragen von einem Beschäftigten aus der Personalabteilung oder einem Dritten im Rahmen einer Organisationsuntersuchung gestellt werden. Das Mitbestimmungsrecht besteht ebenfalls dann, wenn den Beschäftigten die Beantwortung der Fragen freigestellt wird.

Testverfahren jeglicher Art

Das Mitbestimmungsrecht kommt auch bei **Testverfahren** jeglicher Art, **Mitarbeitergesprächen** und Zielvereinbarungen, **Personalbeurteilungen, Gemeinwertkostenanalysen, Krankengesprächen und -analysen,** betriebsinternen **Sicherheitsprüfungen** und **Assessmentcentern** zum Tragen. Gleiches gilt, wenn Kunden, Patienten etc. über das Personal befragt werden. Wie bereits erwähnt, sind Einwilligungserklärungen gemäß § 4 Abs. 1 BDSG ebenfalls mitbestimmungspflichtige Personalfragebogen.

4.5.2 Technische Überwachungseinrichtungen

Das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG hat sich zur zentralen Norm bei der Einführung und Anwendung von IuK-Techniken herauskristallisiert. Danach unterliegt die Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, der Mitbestimmung.

Mit dem Mitbestimmungsrecht sollen **drei Ziele verfolgt werden**:

1. Es soll in erster Linie als **präventiver Schutz** rechtlich unzulässige Eingriffe in den Persönlichkeitsbereich der Arbeitnehmer bereits im Vorfeld verhindern.
2. Es sichert dem Betriebsrat ein **Mitbeurteilungsrecht** bei der oft schwierigen Ermittlung der Grenze zwischen zulässigen und unzulässigen Eingriffen, ohne dass dadurch die Grenzen der Zulässigkeit verändert werden können.
3. Es gewährleistet eine **Mitgestaltung des Betriebsrats** im Rahmen rechtlich zulässiger Eingriffe: Dabei müssen sich die Eingriffe auf das durch die betrieblichen Notwendigkeiten unbedingt erforderliche Maß beschränken.

Technische Einrichtung

Voraussetzung für die Anwendung des Mitbestimmungsrechts ist es, dass die Überwachung durch eine technische Einrichtung erfolgt. IuK-Systeme jeder Art sind ohne Einschränkung als technische Einrichtung zu qualifizieren, wobei Hard- und Software als Gesamteinrichtung anzusehen sind.

Einführung und Anwendung

Das Mitbestimmungsrecht besteht sowohl bei der Einführung als auch bei der Anwendung einer technischen Einrichtung. Dabei ist die **Einführung** der Moment der Entscheidung des Arbeitgebers, dass eine entsprechende Installation erfolgen soll. So wird auch die **Probephase** erfasst. Unter **Anwendung** wird u.a. verstanden, welche Daten erhoben und verarbeitet werden, wer Zugriff auf die gespeicherten Daten hat, wie die Daten geschützt werden, wann eine Löschung zu erfolgen hat, welche Abfrage- und Auswertungssprachen genutzt und welche Auswertungen erstellt werden.

Überwachung

Eine weitere Voraussetzung für die Anwendung des Mitbestimmungsrechts ist, dass die technische Anlage **zur Überwachung bestimmt ist**. Der Überwachungsprozess von **Leistung oder Verhalten** der Arbeitnehmer ist ein Vorgang, der verschiedene Prozesse durchlaufen kann, nämlich die Ermittlungs- bzw. Erhebungsphase, die Verarbeitungsphase oder die Beurteilungs- und Bewertungsphase. Denkbar ist, dass mittels einer technischen Einrichtung alle diese drei Phasen verwirk-

licht werden können. Dem Wortsinn des § 87 Abs. 1 Nr. 6 BetrVG nach ist dieses jedoch nicht die Voraussetzung für die Anwendung des Mitbestimmungsrechts, weil es nur auf die Bestimmung, d.h. auf die technische Eignung ankommt. Diese ist auch gegeben, wenn nur eine oder einzelne Phasen des Überwachungsvorgangs technisch durchgeführt werden. Deshalb fällt beispielsweise die bloße Erhebung von leistungs- oder verhaltensrelevanten Daten der Arbeitnehmer, z.B. durch Einscannen von Daten, unter das Mitbestimmungsrecht. Das hat das BAG bereits vor über 20 Jahren festgestellt: „Auch in der Literatur ist durchweg anerkannt, dass eine Überwachung im Sinne des § 87 Abs. 1 Nr. 6 BetrVG schon dann vorliegt, wenn durch technische Einrichtungen Informationen erhoben und aufgezeichnet werden." (BAG, Beschluss v. 6.12.1983 – 1 ABR 43/81 –, EzA zu § 87 BetrVG, Bildschirmarbeitsplatz Nr. 1, S. 37)

„Dazu bestimmt"

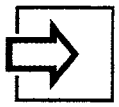
Entgegen des Wortlauts „**dazu bestimmt**" ist es nicht erforderlich, dass die technische Einrichtung ausschließlich oder überwiegend die Überwachung der Arbeitnehmer zum Ziel hat. Insbesondere braucht der Arbeitgeber eine Überwachung der Arbeitnehmer nicht zu beabsichtigen. Entsprechend dem **Zweck des Mitbestimmungsrechts**, die Arbeitnehmer präventiv vor Eingriffen in ihrem Persönlichkeitsbereich zu schützen, genügt es, wenn die Einrichtung aufgrund der technischen Gegebenheiten und ihres konkreten Einsatzes **objektiv zur Überwachung geeignet ist**. Der Arbeitgeber muss die Überwachung der Arbeitnehmer auch nicht beabsichtigen. Das BAG hat dieses in seiner Rechtsprechung entsprechend so gesehen: „Der Senat hat § 87 Abs. 1 Nr. 6 BetrVG in seiner bisherigen Rechtsprechung dahingehend verstanden, dass es trotzt des Wortes ‚bestimmt nicht auf die subjektive Überwachungsabsicht des Arbeitgebers ankommt, sondern allein entscheidend sie, ob die technische Einrichtung objektiv geeignet ist, Verhalten und Leistung der Arbeitnehmer zu überwachen, d.h. Verhaltens- und Leistungsinformationen über den Arbeitnehmer zu erheben und aufzuzeichnen." (BAG, Beschluss v. 6.12.1983 – 1 ABR 43/81 –, EzA zu § 87 BetrVG, Bildschirmarbeit Nr. 1, S. 38 f.) Es kommt also nicht darauf an, ob die mittels solcher Einrichtungen erhobenen und aufgezeichneten Daten bei entsprechender Eignung durch die Einrichtung ausgewertet werden. Das Mitbestimmungsrecht setzt nicht voraus, dass die technische Einrichtung selbst die Beurteilung ermöglicht; so kann auch z.B. aufgrund des Überwachungsergebnisses durch den Vorgesetzten vorgenommen werden. Maßgeblich für das Mitbestimmungsrecht ist es also, dass das technische System **objektiv geeignet** ist, Leistung oder Verhalten zu überwachen.

Verhaltens- und leistungsrelevante Daten

Die Überwachung durch die technische Einrichtung muss sich auf das Verhalten oder die Leistung der Arbeitnehmer beziehen. **Verhaltens-**

und leistungsrelevante Daten sind z.B. Beginn und Ende der täglichen Arbeitszeit, Einzelheiten der Vertragserfüllung, erbrachte Arbeitsleistung, Abwesenheitszeiten, betriebliche Darlehen, Pfändungen. Bei IuK-Techniken reicht es für das Mitbestimmungsrecht aus, dass Informationen erhoben und gespeichert werden, die für sich allein noch keine Aussage über Leistung oder Verhalten zulassen, die jedoch in Verknüpfung mit anderen Daten eine Kontrolle ermöglichen können.

Fazit



Der Betriebsrat kann über seine Beteiligungsrechte nach dem BetrVG den Datenschutz der Beschäftigten nachhaltig mitgestalten. Dabei sind jedoch zwingend die Vorgaben des BDSG einzuhalten. Der Betriebsrat hat in Bezug auf den Datenschutz insbesondere folgende Beteiligungsrechte:

- Informationsrecht – § 80 Abs. 2 und § 90 Abs. 1 BetrVG
- Beratungsrecht – § 90 Abs. 2 BetrVG
- Überwachungsrecht – § 80 Abs. 1 Nr. 1 BetrVG
- Mitbestimmung bei Personalfragebogen – § 94 BetrVG
- Mitbestimmung bei technischen Überwachungseinrichtungen – § 87 Abs. 1 Nr. 6 BetrVG
- Abschluss von Betriebsvereinbarungen – § 77 BetrVG

4.6 Durchsetzung der Rechte des Betriebsrats

Wichtige Instrumente zur Umsetzung und Durchsetzung der Mitbestimmungsrechte sind die **Einigungsstelle** (§ 76 BetrVG) und das **arbeitsgerichtliche Beschlussverfahren** (§ 2a Arbeitsgerichtsgesetz).

Einigungsstelle

Die Einigungsstelle kann als eine Art Schlichtungsstelle sowohl vom Arbeitgeber als auch vom Betriebsrat angerufen werden, wenn die Verhandlungen über eine mitbestimmungspflichtige Angelegenheit im Betrieb scheitern. Eine Einigungsstelle wird im Einzelfall gebildet, ist **paritätisch** zusammengesetzt, wobei ein Vorsitzender hinzukommt, auf den sich beide Seiten einigen müssen. Der Spruch der Einigungsstelle muss schriftlich niedergelegt, vom Vorsitzenden unterschrieben und dem Arbeitgeber und Betriebsrat zugeleitet werden. Die Kosten für die Einigungsstelle trägt der Arbeitgeber, was in der betrieblichen Praxis ein geeignetes Druckmittel des Betriebsrats sein

kann, um die Meinungsverschiedenheiten in den betrieblichen Verhandlungen zu lösen.

Arbeitsgerichtliches Beschlussverfahren

Das **arbeitsgerichtliche Beschlussverfahren** folgt grundsätzlich der Unterscheidung zwischen Individualarbeitsrecht einerseits und dem kollektiven Arbeitsrecht andererseits. Für Streitigkeiten im Verhältnis Arbeitgeber und Arbeitnehmer ist das Arbeitsgericht im **Urteilsverfahren** zuständig (§ 2 Abs. 1 Nr. 3 ArbGG). Das **Beschlussverfahren** greift bei betriebsverfassungsrechtlichen Streitigkeiten zwischen Arbeitgeber und Betriebsrat, soweit es sich nicht um Straf- und Ordnungswidrigkeiten nach den §§ 119 bis 121 BetrVG handelt.

Die Anträge im Beschlussverfahren können z.B. darauf gerichtet sein, durch das Arbeitsgericht feststellen zu lassen, ob in einer bestimmten Frage ein Mitbestimmungsrecht besteht. Nach § 85 Abs. 2 ArbGG ist in dieser Frage auch der Erlass einer einstweiligen Verfügung zulässig, sodass die geplante Einführung oder Inbetriebnahme einer technischen Überwachungseinrichtung gestoppt werden kann, wenn der Betriebsrat nicht entsprechend den Vorgaben des BetrVG beteiligt wurde.

Einstweilige Verfügungen

Einstweilige Verfügungen haben stark an Bedeutung gewonnen. Denn oftmals kann nur durch ihren Erlass verhindert werden, dass Rechte des Betriebsrats nicht „leer laufen". Insbesondere gilt dieses bei der Einführung von neuen Techniken. So kann der Betriebsrat sein Beratungs- und Mitbestimmungsrecht nur dann wahrnehmen, wenn er rechtzeitig und umfassend alle erforderlichen Unterlagen erhält. Sind aber bereits technische Einrichtungen im Betrieb installiert, wird man schon im Hinblick auf die investierten Beträge davon nicht ausgehen können, dass der Betriebsrat noch seine Mitbestimmungsrechte angemessen im Interesse der Beschäftigten wahrnehmen kann.

5 Praxis

5.1 Betriebsvereinbarungen

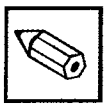
Betriebsräte nehmen ihr Mitbestimmungsrecht gemäß § 87 Abs. 1 Nr. 6 BetrVG in der Regel nicht durch bloße Zustimmung wahr, sondern regeln die Verarbeitungsbedingungen im Rahmen von **Betriebsvereinbarungen** (§ 77 BetrVG). Der Abschluss einer solchen formellen Vereinbarung ist geboten, weil eine Regelung über die Begrenzung bestehender Überwachungsmöglichkeiten dauerhafte Verbindlichkeit nur bekommen kann, wenn sie zum Inhalt einer Betriebsvereinbarung gemacht wurde. Der konkrete Regelungsinhalt von entsprechenden Betriebsvereinbarungen bleibt den beiden Betriebspartnern, Arbeitgeber und Betriebsrat, überlassen. In Bezug auf die datenschutzrechtlichen Regelungen beim Einsatz von Personalabrechnungssystemen, Zeiterfassungssystemen, Telefonnebenstellenanlagen etc. werden von Betriebsräten so genannte Positivregelungen angestrebt. Das heißt, dass in einer Betriebsvereinbarung eine abschließende Festschreibung der eingesetzten Hardware mit den Standorten, der eingesetzten Software, der gespeicherten personenbezogenen Daten, der Auswertungen mit Verteiler, der zugriffsberechtigten Personen und der Schnittstellen zu anderen DV-Systemen erfolgt. Jede Änderung und Erweiterung wird zusätzlich der Mitbestimmung des Betriebsrats unterworfen.

Die Inhalte einer Betriebsvereinbarung betreffen unmittelbar die Aufgabenstellung des bDSB, denn bei einer Betriebsvereinbarung handelt es sich um eine „andere Rechtsvorschrift" i.S.d. § 4 Abs. 1 BDSG, deren Einhaltung gemäß § 4g BDSG der bDSB sicherzustellen hat. Zudem hat der bDSB auf die Einhaltung der Mitbestimmungsrechte zu achten, denn die unter Verletzung der Beteiligungsrechte des Betriebsrats durchgeführte Datenverarbeitung ist nicht nur kollektiv-, sondern auch individualrechtlich unzulässig. Werden personenbezogene Daten ohne Zustimmung des Betriebsrats erhoben und gespeichert, so muss der bDSB auf die Beendigung der rechtswidrigen Vorgänge und die Löschung der Daten hinwirken. Zusätzlich kann aber auch der Betriebsrat mithilfe des Gerichts und u.U. per einstweiliger Verfügung die Datenverarbeitungsvorgänge stoppen lassen.

5.2 Beispiele von Betriebsvereinbarungen

Grundsätzlich hat der Betriebsrat die Möglichkeit zu jedem einzelnen technischen System, das der Mitbestimmung nach § 87 Abs. 1 Nr. 6

BetrVG unterliegt, eine Betriebsvereinbarung abzuschließen. In der betrieblichen Praxis schließen Arbeitgeber und Betriebsrat in der Regel eine übergreifende Rahmenbetriebsvereinbarung ab. In Ergänzung zu dieser Rahmenvereinbarung werden Einzelvereinbarungen abgeschlossen zu Themen wie E-Mail-/Internet-Nutzung, Zeiterfassung, Zugangskontrolle oder Videoüberwachung. Durch den Abschluss einer Betriebsvereinbarung soll zum einen Transparenz über die Verarbeitung personenbezogener Daten geschaffen werden und zum anderen die Verarbeitung personenbezogener Daten auf das betrieblich erforderliche Maß beschränkt werden. Nachfolgend sind Eckpunkte einer Rahmenvereinbarung und Eckpunkte einer Einzelvereinbarung (Zeiterfassung) exemplarisch dargestellt.



Eckpunkte einer Rahmenvereinbarung zum Einsatz in Informations- und Kommunikationstechnik (IuK)

1. Präambel

2. Gegenstand und Geltungsbereich

räumlich und sachlich

3. Begriffsbestimmungen

- personenbezogene Daten
- Verarbeitung
- automatisierte Datenverarbeitung

4. Grundsätze der Beteiligung des Betriebsrats

4.1 Unterrichtung

- rechtzeitige und umfassende Unterrichtung des Betriebsrats
- Einsatzort und Leistungsumfang des Systems einschließlich geplanter
  - Vernetzungen
  - geplante Verarbeitung personenbezogener Daten der Beschäftigten
  - mögliche Auswertungen mit personenbezogenen Daten
  - Zulässigkeitsprüfung und Vorabkontrolle des Datenschutzbeauftragten
  - Auswirkungen auf Arbeitsablauf und Arbeitsorganisation
  - geplante organisatorische und zeitliche Projektabwicklung

4.2 Kontroll- und Überwachungsrechte

- Überwachung der Einhaltung der Betriebsvereinbarung
- Überwachung der Einhaltung bestehender Gesetze
- Hinzuziehung von Sachverständigen

4.3 Mitbestimmung

Mitbestimmung bei Änderungen und Erweiterungen

5. Dokumentation/Bestandsverzeichnis

Dokumentation der eingesetzten IuK-Technik in Anlagen zur Betriebsvereinbarung

- Bezeichnung des Systems
- eingesetzte Software
- Kurzbeschreibung
- Einsatzzweck
- gespeicherte personenbezogene Daten der Beschäftigten
- Rahmen und Umfang der Auswertungen
- zugriffsberechtigte Personen
- Löschungsfristen

6. Rechte der Beschäftigten

- rechtzeitige und umfassende Informationen über neue IuK-Techniken in ihrem Arbeitsbereich
- Recht auf Auskunft, Berichtigung, Löschung und Sperrung

7. Datenschutz

7.1 Grundsätze

- Verarbeitung personenbezogener Daten für konkret festgelegte Zwecke
- Regelungen der Verarbeitung sind nachvollziehbar
- Datenverarbeitung nur in einer sehr engen Zweckbestimmung bezogen auf das Arbeitsverhältnis

7.2 Leistungs- und Verhaltenskontrolle

- Ausschluss von Leistungs- und Verhaltenskontrolle
- Ausnahmen bedürfen der Regelung in einer Betriebsvereinbarung oder der vorherigen Zustimmung des Betriebsrats

7.3 Betrieblicher Datenschutzbeauftragter

- Bestellung und Abberufung unterliegen der Zustimmung des Betriebsrats
- kann als sachkundige Person vom Betriebsrat hinzugezogen werden

7.4 Systemadministratoren

- Verpflichtung zur Einhaltung der Betriebsvereinbarung
- keine Weitergabe personenbezogener Daten an andere Personen
- schalten sich nicht ohne Wissen und Zustimmung der Beschäftigten auf die PCs auf
- Ausnahmen bedürfen der Zustimmung des Betriebsrats

8. Verwertungsverbot

Daten, die unter Verletzung der Bestimmungen von Betriebsvereinbarungen gewonnen wurden, unterliegen einem Verwertungsverbot.

9. Änderungen, Erweiterungen und Neueinführungen

vorherige Zustimmung des Betriebsrats

10. Meinungsverschiedenheiten

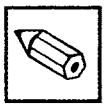
Bei Meinungsverschiedenheiten in Bezug auf die Anwendung und Auslegung der Betriebsvereinbarung kann jede Seite die Einigungsstelle anrufen.

11. Einzelvereinbarungen

Betriebsrat kann zu allen Systemen Einzelvereinbarungen initiieren

12. Inkrafttreten und Kündigung

- Inkrafttreten
- Kündigung
- Nachwirkung bei Kündigung
- Salvatorische Klausel



Eckpunkte einer Einzelvereinbarung zur automatisierten Zeiterfassung

1. Gegenstand und Geltungsbereich

räumlich und sachlich

2. Einsatzzweck

abschließende Festlegung des Einsatzzwecks

- Erfassung und Verwaltung der Arbeitszeiten
- Erstellung von Auswertungen, wie in dieser Vereinbarung festgelegt
- (*Einsatzzweck muss u.U. ergänzt werden*)

3. Beschreibung des Systems

- abschließende Beschreibung des Systems
- Dokumentation des Systems in Anlagen zur Betriebsvereinbarung

3.1 Hardware

eingesetzte Hardware mit Standorten (Anlage 1)

3.2 Personenbezogene Daten

gespeicherte personenbezogene Daten (Anlage 2), gegliedert nach Stammdaten, Abwesenheitsdaten und Buchungsdaten

3.3 Auswertungen

Auflistung und Dokumentation der Auswertungen (Anlage 3)

3.4 Zugriffsberechtigte Personen

zugriffsberechtigte Personen (Anlage 4)

3.5 Schnittstellen

Schnittstellen (Anlage 5) mit übertragenen Daten

3.6 Löschungsfristen

Festlegung der Löschungsfristen

4. Rechte der Beschäftigten

- Recht auf Auskunft, Berichtigung, Löschung oder Sperrung personenbezogener Daten
- Aushändigung des Monatsjournals

5. Rechte des Betriebsrats

- Überwachung der Einhaltung der Betriebsvereinbarung
- Leserecht in Bezug auf die Arbeitszeiten

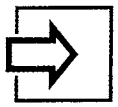
6. Änderungen und Erweiterungen

Änderungen und Erweiterungen des Systems unterliegen der Mitbestimmung des Betriebsrats.

7. Inkrafttreten und Kündigung

- Inkrafttreten
- Kündigung
- Nachwirkung bei Kündigung
- Salvatorische Klausel

Fazit



Durch den Abschluss von Betriebsvereinbarungen kann der Datenschutz der Beschäftigten abgesichert werden. Betriebsvereinbarungen sollten Transparenz über die Verarbeitung personenbezogener Daten schaffen und zugleich die Datenverarbeitung eingrenzen und festlegen. Betriebsvereinbarungen sollten mindestens Folgendes regeln:

- eingesetzte Hard- und Software
- gespeicherte personenbezogene Daten
- Auswertungen mit Verteiler
- zugriffsberechtigte Personen
- Schnittstellen mit übertragenen Daten
- Löschungsfristen

Literatur

Abel, Horst G. (Hrsg.): Praxishandbuch Datenschutz. Loseblatt

Auernhammer, Herbert: Bundesdatenschutzgesetz. 3. Auflage, 1993

Bäumler, Helmut (Hrsg.): Der neue Datenschutz. 1998

Bergmann, Wolfgang/Möhrle, Roland/Herb, Armin: Datenschutzrecht. Loseblatt

Däubler, Wolfgang: Gläserne Belegschaften? Datenschutz in Betrieb und Dienststelle. 4. Auflage, 2002

Däubler, Wolfgang/Kittner, Michael/Klebe, Thomas (Hrsg.): Betriebsverfassungsgesetz. 9. Auflage, 2004

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter: Bundesdatenschutzgesetz. 1996

Dammann, Ulrich/Simitis, Spiros: EG-Datenschutzrichtlinie. Kommentar, 1997

Draf, Oliver: Die Regelung der Übermittlung personenbezogener Daten in Drittländer nach Art. 25, 26 der EG-Datenschutzrichtlinie. 1999

Fabricius, Fritz/Kraft, Alfons/Wiese, Günther/Kreutz, Peter/Oetker, Hartmut/Raab, Thomas/Weber Christoph: Betriebsverfassungsgesetz. Band I und II, 7. Auflage, 2002

Fitting, Karl/Engels, Gerd/Schmidt, Ingrid/Trebinger, Yvonne/Linsenmaier, Wolfgang: Betriebsverfassungsgesetz. 22. Auflage, 2004

Gola, Peter/Schomerus, Rudolf: Bundesdatenschutzgesetz. 8. Auflage, 2005

Gola, Peter/Klug, Christoph: Grundzüge des Datenschutzrechts. 2003

Gola, Peter/Wronka, Georg: Handbuch zum Arbeitnehmerdatenschutz. 3. Auflage, 2004

Halser, Ulrich: Die Betriebsvereinbarung. 2. Auflage, 1995

Schneider, Wolfgang: § 87 BetrVG – Rechtsgrundsätze und Mitbestimmungspraxis. 2004

Koch, Hans-Dietrich (Hrsg.): Der betriebliche Datenschutzbeauftragte. 5. Auflage, Frechen2002

Panzer, Andrea: Mitarbeiterkontrolle und neue Medien. 2003

Roßnagel, Alexander (Hrsg.): Handbuch Datenschutzrecht. 2003

Schaffland, Hans-Jürgen/Wiltfang, Noeme: Bundesdatenschutzgesetz. Losblatt

Simitis, Spiros (Hrsg.): Kommentar zum Bundesdatenschutzgesetz. 5. Auflage, 2003

Speichert, Horst: Praxis des IT-Rechts. 2004

Tinnefeld, Marie-Theres/Ehmann, Eugen/Gerling, Rainer: Einführung in das Datenschutzrecht. 4. Auflage, 2005

Wächter, Michael: Datenschutz im Unternehmen. 3. Auflage, 2003

Weißgerber, Michael: Arbeitsrechtliche Fragen bei der Einführung und Nutzung vernetzter Computerarbeitsplätze. 2003

Wolhgemuth, Hans H.: Datenschutzrecht. 1992

Wohlgemuth, Hans H.: Datenschutz für Arbeitnehmer. 2. Auflage, 1988