Wer Zeitung liest und erst recht, wer einschlägige Fachzeitschriften durchblättert, muß den Eindruck gewinnen, daß Datenschutz in dieser, unserer Gesellschaft einen besonders hohen Stellenwert hat. Ob es um große oder kleine Lauschangriffe, um Krankenversichertenkarten oder um im Hausmüll auftauchende Akten geht – immer läßt man die Datenschützer zu Worte kommen, stets wird ›der Datenschutz‹ beschworen. Die Praxis allerdings steht dazu in einem oft krassen Gegensatz. Vor allem in Betrieben und Unternehmen bleiben bisweilen selbst die simpelsten ›Gebote des Datenschutzes‹ unbeachtet – eine Aufgabe auch und vor allem für Betriebs- und Personalräte. Bruno Schierbaum stellt sie vor, die …

10 Gebote des Datenschutzes

Bei der Einführung und Anwendung der sich immer mehr ausbreitenden informationstechnischen Systeme muß nicht nur der Betriebs- oder Personalrat beteiligt werden, sondern es besteht auch die Verpflichtung zur Umsetzung des Bundesdatenschutzgesetzes (BDSG) oder auch der Landesdatenschutzgesetze. Nach § 4 BDSG etwa müssen Betriebe vor der Verarbeitung personenbezogener Daten jedes einzelne dieser Daten einer ***Zulässigkeitsprüfung*** unterziehen. Und die Verarbeitung ist nur dann zulässig, wenn der Betroffene eingewilligt hat, wenn eine Rechtsvorschrift dieses erlaubt oder sogar vorschreibt, oder wenn das BDSG selbst dieses vorsieht. Zudem müssen die ***Rechte der Betroffenen*** (Beschäftigten) auf Benachrichtigung, Auskunft, Berichtigung, Löschung und Sperrung (§§ 33 bis 35 BDSG) gewährleistet sein. Darüberhinaus müssen gemäß § 9 BDSG alle nicht-öffentlichen Stellen (Privatbetriebe) und öffentlichen Stellen, jedenfalls soweit sie personenbezogene Daten verarbeiten, ***technische und organisatorische Maßnahmen*** zum Datenschutz treffen (die Landesdatenschutzgesetze, die für die öffentlichen Stellen der Länder gelten, enthalten entsprechende Vorschriften).

Im § 9 BDSG heißt es dazu wörtlich: »Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemesssenen Verhältnis zu dem angestrebten Schutzzweck steht.«

Die Details der Datenschutzbestimmungen

Personenbezogene Daten … sind nach § 3 Abs. 1 BDSG »Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person«. Alle Daten also, die einer Person zugeordnet werden können, sei es durch die Aussagekraft der Daten selbst oder beispielsweise durch das Zusatzwissen eines Sachbearbeiters, sind personenbezogene Daten im Sinne des BDSG.

Der Begriff ›personenbezogene Daten‹ geht deshalb weit über die sogenannten Personalstammdaten (Name, Geburtsdatum, Adresse, Abteilung …) hinaus und umfaßt unter anderem auch Leistungs- und Verhaltensdaten ebenso wie Werturteile und Qualifikationsdaten im weitesten Sinne. Entsprechende Daten werden nicht nur in sogenannten Personalabrechnungs- und Informationssytemen (wie z. B. PAISY) gespeichert, sondern auch in Betriebsdaten- (BDE) und Zeiterfassungssystemen, in Produktionsplanungs- und Steuerungssystemen (PPS), durch Telefonnebenstellenanlagen und auch durch Textverarbeitungssysteme. Praktisch bedeutet das, daß bei so gut wie allen informationstechnischen Systemen die technischen und organisatorischen Datenschutzmaßnahmen nach § 9 BDSG zu treffen sind.

Datenschutz und Datensicherung … sind zwei Begriffe, die immer wieder verwendet werden, und sehr oft so, als handele es sich dabei um ein und dasselbe. Häufig wird sogar der § 9 BDSG als ›Datensicherungsvorschrift‹ bezeichnet, obwohl dieser Begriff selbst dort gar nicht vorkommt. Das mag daran liegen, daß Betriebe und Rechenzentren natürlich bereits vor Inkrafttreten des BDSG im Jahre 1977 aus Eigeninteresse Datensicherungsmaßnahmen durchgeführt, also ihre Dateien, Datenträger, Programme und DV-Anlagen vor Verlust oder unbefugtem Zugriff geschützt haben. Aber: Auch wenn sich viele der Maßnahmen, die zur Datensicherung ergriffen werden, ebenfalls zur Ausführung der Datenschutzvorschriften eignen, haben Datenschutz und Datensicherung dennoch ganz unterschiedliche Zielsetzungen, die auch nicht verwischt werden sollten.

Daten***sicherung*** zielt darauf, den ordnungsgemäßen Ablauf der Datenverarbeitung dadurch sicherzustellen, daß Hard- und Software und Daten vor Verlust, Beschädigung und Mißbrauch geschützt werden. Beim Daten***schutz*** aber geht es um die Verhinde-

rung unzulässiger Verarbeitung und Nutzung personenbezogener Daten.

Anders ausgedrückt: Die Datensicherung dient dem Interesse der datenverarbeitenden Stelle (des Unternehmens, der Verwaltung …), der Datenschutz dient direkt oder indirekt dem Interesse der Betroffenen (der Beschäftigten, der Bürger …). Und da das BDSG gemäß seinem § 1 den Zweck hat, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird, handelt es sich beim § 9 BDSG eben nicht um eine Datensicherungs-

Zuständigkeit von Aufsichtsbehörde, Bundes- und Landesdatenschutzbeauftragten

datenverarbeitende Stelle	*rechtl. Grundl.*	*interne Kontrollinstanz*	*externe Kontrollinstanz*
Behörden und sonstige öffentliche Stellen des Bundes	BDSG 2. Abschn.	–	Datenschutzbeauftragter des Bundes
Behörden und sonstige öffentliche Stellen der Länder und Gemeinden	jeweiliges Landesdatenschutzgesetz	behördlicher Datenschutzbeauftragter (vorgeschrieben nur in Niedersachsen, Berlin, Hessen)	Landesbeauftragter für den Datenschutz (nach Landesdatenschutzgesetz)
nicht-öffentliche Stellen, öffentlich-rechtliche Wettbewerbsunternehmen	BDSG 3. Abschn.	betrieblicher Datenschutzbeauftragter §§ 36–37 BDSG	Aufsichtsbehörde nach § 38 BDSG (siehe Liste in CI 2/93 Seite 24)

sondern um eine Datenschutzvorschrift – auch wenn es bei den konkreten technisch-organisatorischen Maßnahmen zu Überschneidungen kommt. Deshalb schreibt das BDSG auch nur Maßnahmen vor, die dem Schutzanspruch der Betroffenen dienen.

Verhältnismäßigkeitsprinzip … Die technischen und organisatorischen Maßnahmen, die in der Anlage zu § 9 BDSG als Zielvorgaben formuliert sind, sind dabei ausdrücklich dem Verhältnismäßigkeitsprinzip unterstellt: Sie sind nur »erforderlich« (also 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. Es geht also nicht darum, bei jedem DV-System die gleiche Liste von Schutzmaßnahmen ›abzuhaken‹, sondern es geht darum, den jeweiligen Schutzzweck zu erreichen. Und dabei spielt natürlich die Art der Daten, ihre ***Schutzwürdigkeit***, eine entscheidende Rolle.

Um nun entscheiden zu können, welche konkreten Maßnahmen bei einem bestimmten informationstechnischen System ›erforderlich‹ sind, werden die zu speichernden Daten oft in Schutzklassen eingeteilt – je ›sensibler‹ die Daten, desto höher die Anforderungen an den technisch-organisatorischen Datenschutz (siehe dazu auch die CI-Serie ›Stichwort: Sicherheit‹ ab CI 9/94 Seite 21).

Der Grad der Sensibilität wird danach bemessen, ob bei Mißbrauch oder Verlust der Daten ›Wohl oder Leben‹ der Betroffenen ***nicht, beträchtlich oder sehr stark*** (mit Gefahr für Leib und Leben) beeinträchtigt werden.

Eine solche Einteilung der Daten kann in der Praxis auch durchaus als Orientierungshilfe dienen, ist aber dennoch problematisch. So hat das Bundesverfassungsgericht (BVerfG vom 5.12.1983, NJW 1984, Heft 8, Seite 419 ff.) im sogenannten Volkszählungsurteil festgestellt, daß es unter den Bedingungen der automatisierten Datenverarbeitung überhaupt kein ›belangloses Datum‹ mehr gibt. Und dem ist auch nachdrücklich zuzustimmen, da selbst vermeintlich belanglose Daten durch die Verknüpfung mit anderen Daten eine neue Qualität und damit ›Sprengkraft‹ erhalten können.

Technische und organisatorische Maßnahmen … Die Begriffe ›technisch‹ und ›organisatorisch‹ sind weit auszulegen. So gehören zu den technischen Maßnahmen nicht nur die, die sich direkt auf Geräte und Programme beziehen, sondern auch das gesamte baulich-räumliche Umfeld. Und organisatorische Maßnahmen gehen in der Regel auch mit personellen Regelungen (Vorkehrungen) einher, wie beispielsweise der Verteilung von Aufgaben, Befugnissen und Verantwortungen. Die Gestaltung des Arbeitsablaufs gehört ebenso dazu wie die Zugangs- und Zugriffsregelungen oder die Vornahme stichprobenartiger Erfolgskontrollen.

Da die Verhältnisse bei den datenverarbeitenden Stellen sehr unterschiedlich sind, ist es natürlich nicht möglich, ein allgemeingültiges Datenschutzkonzept zu entwickeln, das als Vorgabe für die Praxis dienen kann. Vielmehr liegt es in der Verantwortung jeder einzelnen Stelle, ein ›angepaßtes‹ Datenschutzkonzept mit angemessenen technischen und organisatorischen Maßnahmen zu erstellen.

Umsetzung und Kontrolle der Maßnahmen

Für den Datenschutz und damit auch für die Umsetzung der technischen und organisatorischen Maßnahmen ist ›die speichernde Stelle‹ verantwortlich, also beispielsweise das Unternehmen. Kontrollfunktionen in bezug auf den Arbeitnehmerdatenschutz kann ein betrieblicher (oder behördlicher) Datenschutzbeauftragter, die Aufsichtsbehörde (z. B. das Innenministerium des Landes), der Bundesdatenschutzbeauftragte, der jeweilige Landesdatenschutzbeauftragte (siehe Kasten oben), der Betriebs- oder Personalrat und nicht zuletzt natürlich die Betroffenen selber ausüben. Besteht die Verpflichtung, gemäß § 36 BDSG einen ***betrieblichen Datenschutzbeauftragten*** zu bestellen, gehört es zu dessen Aufgaben,

Die zehn Gebote des Datenschutzes in der Übersicht

Anforderungen	*Maßnahmen im Rechenzentrum*	*Maßnahmen bei Personal Computern*
1. Zugangskontrolle **Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.**	- Schaffung von Sicherheitsbereichen - Festlegung befugter Personen - Berechtigungsausweise, Schlüssel, Codearten, Besucherausweise - Anwesenheitsaufzeichnungen - Regelung für betriebsfremde Personen - ›Closed-Shop‹-Betrieb (›abgeschlossener Laden‹)	- Ab- bzw. Verschließen der Hardware und der Räume - Festlegung der berechtigten Benutzer - Zugangskontrolle durch Ausweisleser - Sperren der Geräte durch Einbau einer zusätzlichen Hardware-Baugruppe - Raumsicherung
2. Datenträgerkontrolle **Es ist zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können.**	- Absicherung der Bereiche, in denen Datenträger aufbewahrt werden - Festlegung befugter Personen - Maßnahmen gegen unbefugtes Entfernen - Ausgabe von Datenträgern nur an autorisierte Personen - Kennzeichnung eigener Datenträger zur Unterscheidung von fremden Datenträgern - Bestandskontrollen - Lagerung der Datenträger in einem Sicherheitsbereich (Dateiarchiv, Sicherheitsschränke, Tresor) - Kontrollierte Vernichtung von Datenträgern mit Protokollierung - Regelung der Anfertigung von Kopien	- Kontrolle der Disketten und mobilen Festplatten sowie der Druckausgaben und deren sichere Verwahrung - Führung eines Datenträgerverzeichnisses - Kennzeichnung von Datenträgern - Festlegung von Aufbewahrungsregeln und fristen - Einsatz diskettenloser Arbeitsplatzrechner im LAN (Server-Konzept) - Sperrung des Copy-Befehls - physisches Löschen nicht mehr benötigter Daten und Dateien, wobei dafür geeignete Dienstprogramme einzusetzen sind
3. Speicherkontrolle **Die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten ist zu verhindern.**	- Einsatz von Benutzercodes (Paßworte) für Dateien und Programme - Regelung über Vergabe, Verwendung und Änderung von Benutzercodes - Einsatz von Verschlüsselungsroutinen für Dateien, Sicherungssoftware - Differenzierte Zugriffsregelung für Prozeduren, Steuerkarten, Verfahren zur Ablaufsteuerung, Befugnis zum Katalogisieren von Programmen - Richtlinien für die Dateiorganisation - Protokollierung der Dateibenutzung - Schriftliche Anweisungen für Wiederanlaufverfahren - Automatisches Abschalten der Datenstationen (log off) nach längerer Zeit der Nichtbenutzung	- Zwang zur Verwendung von Benutzerkennung und Paßwort - Sicherung durch PC-Schloß - Einsatz diskettenloser LAN-Stationen - Sperrung der Diskettenlaufwerke - Unterbrechung der Stromzufuhr nach Verlassen des PC - Festlegen des berechtigten Benutzerkreises und Vergabe der Benutzerrechte - Protokollierung der Programm- und Dateibenutzung - Auswertung der Ablaufinformationen (Log-Dateien) - Kontrolle des Hilfsprogramm-Einsatzes - Einsatz geeigneter Sicherheitssoftware
4. Benutzerkontrolle **Es ist zu verhindern, daß Datenverarbeitungssysteme mit HIlfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können.**	- Abschließbarkeit von Datenstationen und dezentralen Datenverarbeitungssystemen - Identifizierung des Terminals/Nutzers gegenüber dem DV-System - Automatisches Abschalten der Datenstationen (›log off‹) bei drei fehlerhaften Paßworteingaben - Regelung der Benutzerberechtigung - Vergabe und Sicherung von Identifizierungsschlüsseln - Zuordnung einzelner Terminals nur für bestimmte Funktionen - Funktionelle und/oder zeitlich beschränkte Nutzung von Terminals - Auswertung von Protokollen	- Einsatz von Authentisierungsverfahren - Festlegen von Benutzerrechten (Benutzerprofilen) - Revisionsfähige Dokumentation der Benutzerberechtigungen - Ergreifen von Sanktionen bei Sicherheitsverletzungen (Sperren von Bildschirm bzw. Benutzer) - Erstellung eines Sicherheitsberichts - Einsatz von geeigneter Sicherheitssoftware - Einsatz von geprüften Verschlüsselungsverfahren
5. Zugriffskontrolle **Es ist zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.**	- Anlegen von revisionsfähigen Benutzerprofilen - Funktionelle und/oder zeitlich beschränkte Nutzung von Terminals - Datenstationen mit Funktionsberechtigungsschlüsseln (Regelung der Zugriffsberechtigung) - direkter Zugriff, Stapelbetrieb, Zugriff auf Arbeitsbereiche - Maschinelle Überprüfung der Berechtigung (Identifizierungsschlüssel) - Auswertung von Protokollen - Teilzugriffsmöglichkeit auf Datenbestände und Funktionen	- Eindeutige Identifizierung des PC bei Netzanschluß - Zeitliche Begrenzung der Zugriffsmöglichkeit - Sperren der Betriebssystemebene - Kontrollierter Einsatz der Betriebssystemfunktionen und Betriebsmittel - Einsatz von geeigneter Sicherheitssoftware

Fortsetzung nächste Seite

Anforderungen	*Maßnahmen im Rechenzentrum*	*Maßnahmen bei Personal Computern*
6. Übermittlungskontrolle **Es ist zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können.**	- Dokumentation der Abruf- und Übermittlungsprogramme - Festlegung der Übermittlungswege und der Datenempfänger - Protokollierung der Datenübermittlung - Auswertungsmöglichkeiten der Übermittlungsprotokolle, um die Empfänger oder Abrufenden gezielt feststellen zu können	- Dokumentation der Abruf- und Übermittlungsprogramme - Netzwerkdokumentation - Einsatz einheitlicher und sicherheitsgeprüfter Protokolle - Erstellung einer Datenstromanalyse als Dokumentation für den Datenschutzbeauftragten - Protokollierung der Datenübermittlungen - Kontrolle der Online-Abrufe - Dokumentation der Empfänger
5. Eingabekontrolle **Es ist zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind.**	- Datenerfassungsanweisungen - Plausibilitätskontrollen - Protokollierung der Eingaben - Speicherung des Erfassers bei den Eingaben - Vorgangsprotokollierung für jeden Einzelfall	- Protokoll der Zugriffsrechte - Protokollierung (Verarbeitungsprotokoll) aller Aktivitäten - Wer hat wann was eingegeben? - Verarbeitungsprotokolle - Transaktionsprotokolle - Einsatz von geeigneter Sicherheitssoftware
8. Auftragskontrolle **Es ist zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.**	- Sorgfältige Auswahl der Auftragnehmer - Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und -geber (Datensicherungsmaßnahmen, Transportregelungen, Aufbewahrungsvorschriften, Vertragsverletzungen, Versicherung) - Formalisierung der Auftragserteilung - Kontrolle der ordnungsgemäßen Vertragsausführung	- Eindeutige Vertragsgestaltung - Kontrolle der Vertragsausführung durch gelegentliche Inspektionen - Sorgfältige Auswahl des Auftragnehmers - Vereinbarung von Vertragsstrafen bei weisungswidriger Ausführung - Ausschluß von Subunternehmern
9. Transportkontrolle **Es ist zu verhindern, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden.**	- Verpackungs- und Versandvorschriften (geschlossene Behältnisse) - Verschlüsselung - Direktabholung, Kurierdienst, Transportbegleitung - Sorgfältige Auswahl des Transportpersonals - Vollständigkeits- und Richtigkeitsprüfung	- Vereinbarung von Verpackungs- und Versandvorschriften - Festlegung der Transportwege - Nutzung besonderer Versandarten - Transport durch Direktabholung, Kurierdienst - Durchführung von Vollständigkeitsprüfungen - Verwendung des Kopierschutzes
10. Organisationskontrolle **Die innerbehördliche oder innerbetriebliche Organisation ist so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird.**	- Funktionstrennung in räumlicher, organisatorischer und personeller Sicht - Vier-Augen-Prinzip (kein Operator oder Programmierer mit Zugriff auf personenbezogene Daten allein im Betrieb) - Richtlinien, Arbeitsanweisungen, Verfahrensbeschreibung, Regelung von Programmierung, Test und Freigabe - Regelung zur System- und Programmprüfung - Datensicherungskonzept, -plan, -katalog - Katastrophenplanung - Auflagen zur sicheren Behandlung und Aufbewahrung von Eingabelisten und Ausdrucken	- Beachtung der Funktionstrennung (soweit möglich) - Vergabe von Bedienungs- und Benutzeranweisungen - Dokumentation der zugelassenen Software im ›Software-Kataster‹ - Erfassen der Aufstellungsorte im ›PC-Kataster‹ - Festlegung der Verfahren zur Datenträgerverwaltung - Revisionsfähige Dokumentation der Benutzerrechte (User-Management) - Einheitliches Verfahren zur Beschaffung, Installation und Betreuung von PCs - Einrichtung eines Benutzerservice - Vorgabe und Prüfung der Einhaltung von Teststrategien - Schulung der Benutzer - Festlegung von Aufbewahrungsrichtlinien - Kontrollmaßnahmen zur Einhaltung erlassener Richtlinien - Erstellung eines Backup-Konzeptes

angelehnt an: Aus der Kontrollpraxis der Aufsichtsbehörden (RDV 3/91); und an: Abel/Schmök, PC-Sicherheit im Unternehmen, München 1992

auf der Basis der betrieblichen Gegebenheiten ein angemessenes Datenschutzkonzept für einzelne DV-Anwendungen zu entwickeln.

Für die öffentlichen Stellen des Bundes ist nach dem BDSG die Bestellung eines ***behördlichen Datenschutzbeauftragten*** übrigens nicht vorgesehen. Nur die Landesdatenschutzgesetze Hessens (§ 5 Abs. 2 HDSG), Berlins (§ 19 Abs. 5 BlnDSG) und Niedersachsens (§ 8 Abs. 3 NDSG) verpflichten die öffentlichen Stellen dieser Länder, einen behördlichen Datenschutzbeauftragten zu bestellen. Ist die Bestellung eines internen Datenschutzbeauftragten nicht gesetzlich vorgeschrieben, kann es sich für die Behörde dennoch als notwendig erweisen, einen Datenschutzbeauftragten zu bestellen, weil anders die Anforderungen der Datenschutzgesetze nicht umzusetzen sind.

Die Aufsichtsbehörde … überprüft gemäß § 38 BDSG als externe Kontrollinstanz die Ausführung des Datenschutzgesetzes bei nicht-öffentlichen Stellen (Privatbetriebe). Stellt die Aufsichtsbehörde im Rahmen ihrer Prüftätigkeit fest, daß Versäumnisse bei der Erfüllung der Auflagen aus § 9 BDSG vorliegen, so kann sie die Abstellung der Mängel anordnen.

Ist dies geschehen, hat aber nicht zu dem erwarteten Ergebnis geführt, dann greift ein abgestuftes Verfahren: Die Aufsichtsbehörde kann jetzt die Beseitigung der Mängel unter Setzung einer angemessenen Frist bei Verhängung eines Zwangsgeldes durchsetzen. Wird die speichernde Stelle (das Unternehmen) auch in dieser Frist nicht tätig, so hat die Aufsichtsbehörde das Recht, den Einsatz einzelner Verfahren (z. B. die Verarbeitung von Gesundheitsdaten) zu untersagen.

Kein Mangel an Kontrollinstanzen

Für die Kontrolle bei öffentlichen Stellen des Bundes ist der ***Bundesbeauftragte für den Datenschutz*** (BfD) zuständig. Für die öffentlichen Stellen der Länder übernimmt der jeweilige ***Landesbeauftragte für den Datenschutz*** (LfD) diese Aufgabe.

Aber auch die einzelnen Beschäftigten können eine gewisse Kontrollfunktion ausüben, indem sie von ihrem Recht auf Benachrichtigung, Auskunft, Berichtigung, Löschung und Sperrung Gebrauch machen. Von entscheidender Bedeutung ist jedoch, daß die Beschäftigten, die mit personenbezogenen Daten umgehen, durch intensive Schulung dazu gebracht werden, die notwendigen und festgelegten Datenschutzmaßnahmen ernstzunehmen und umzusetzen. So läßt beispielsweise ein unter die Tastatur geklebter Zettel mit dem Paßwort auch die beste technische Zugriffsregelung ›ins Leere laufen‹. Damit der Datenschutz nicht an der Akzeptanz der Beschäftigten scheitert, dürfen die Daten zum Datenschutz gemäß § 9 BDSG, wie § 31 BDSG vorschreibt, nicht ›zweckentfremdet› werden.

So dürfen etwa die ›Zwangsprotokollierungen‹ nur zur Umsetzung von Datenschutz- und Datensicherungsmaßnahmen, ***nicht*** aber zur Kontrolle der Beschäftigten genutzt werden.

Datensicherheit – auch der Betriebsrat ist dabei

Der ***Betriebsrat*** hat nach § 80 Abs. 1 Nr. 1 BetrVG die Einhaltung des BDSG zu überwachen. Darüberhinaus hat er gemäß § 87 Abs. 1 Nr. 6 BetrVG aber auch ein Mitbestimmungsrecht bei der Einführung und Anwendung technischer Einrichtungen, soweit sie geeignet sind, Leistung oder Verhalten der Beschäftigten zu überwachen. Dieses Mitbestimmungsrecht gilt natürlich auch für die Arbeitsplätze, an denen personenbezogene Daten verarbeitet werden und damit auch für die technisch-organisatorischen Datenschutzmaßnahmen nach § 9 BDSG.

Denn was auf der einen Seite dem Datenschutz der Beschäftigten dient (z. B. Zugangskontrolle, Benutzerkontrolle, Eingabekontrolle), kann auf der anderen Seite dazu benutzt werden, das Verhalten der Beschäftigten zu kontrollieren, die mit diesen Daten arbeiten. Mitbestimmung heißt auch in diesem Falle zwar nicht, daß eine gesetzlich vorgeschriebene Maßnahme außer Kraft gesetzt werden könnte, aber gerade bei den technisch-organisatorischen Maßnahmen kann ja die speichernde Stelle (das Unternehmen, die Verwaltung …) über die Auswahl der konkreten Maßnahmen entscheiden – hier also kann auch Mitbestimmung wirksam werden. Bei organisatorischen Maßnahmen kann im übrigen auch das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG bestehen. Die Mitbestimmungsrechte der Personalräte sind ähnlich ausgestaltet.

Bruno Schierbaum
Beratungsstelle für Technologiefolgen und Qualifizierung
26123 Oldenburg, Donnerschweer Straße 84