

6

FACHHOCHSCHULE ULM  
Fachbereich Technische Informatik  
Datenschutz-Seminar

Auswahl aus den bisher durchgeführten Veranstaltungen und Exkursionen:

1. Arbeitsweise des Bundesbeauftragten für den Datenschutz (Besuch der Dienststelle in Bonn).
2. Diskussion mit Datenschutzexperten der Fraktionen des Deutschen Bundestages in Bonn.
3. Diskussion mit Vertretern des PARLAKOM-Ausschusses des Deutschen Bundestages.
4. Arbeitsweise der Landesbeauftragten für den Datenschutz (Besuch der Dienststelle in Stuttgart).
5. Untersuchung eines Personalinformationssystems. Diskussion mit den Betroffenen (Personalabteilung, Arbeitnehmer, Gewerkschaftsvertreter).
6. Datenschutz und AIDS.  
Diskussion mit Mitgliedern einer AIDS-Hilfe-Gruppe.
7. Genom-Analyse und ihre Herausforderung für den Datenschutz.  
Diskussion mit den Mitarbeitern der Abteilung Anthropologie und Wissenschaftsforschung der Universität Ulm.
8. Diskussion mit betrieblichen Datenschutzbeauftragten verschiedener Betriebe.
9. Teilnahme an mehreren Seminaren zum Thema „Informations- und Kommunikationstechnologien und Datenschutz“ in der Theodor-Heuss-Akademie Gummersbach der Friedrich-Naumann-Stiftung.
10. Durchführung mehrerer Seminare, gemeinsam mit der Evangelischen Akademie Bad Boll und dem Institut für Kommunikationsökologie, Dortmund über Datenschutzprobleme von Datenbanken und Expertensystemen/Datenschutz in Europa/Datenschutz in der Zukunftswerkstatt.
11. Diskussionsveranstaltungen mit Prof. Dr. Joseph Weizenbaum, Massachusetts Institute of Technology (MIT), Cambridge, USA über die Gesellschaftliche Verantwortung des Informatikers/Die Sozialethik des Datenschutzes.

## Der Wirtschaftsinformatiker als Datenschutzbeauftragter

Dr. jur. Lic. theol. Thomas Hoeren, Münster

### I. Gang der Darstellung

### II. Berufsbild des Wirtschaftsinformatikers

1. Amtliche Darstellung
2. Schnittstellenkompetenz

### III. Diplom-Studiengang Wirtschaftsinformatik

1. Vorhandene Ausbildungsangebote
2. Studienablauf
3. Vorlesung „Recht für Wirtschaftsinformatiker“

### IV. Übungsveranstaltung „Betriebliches Datenschutzrecht“

1. Anforderungsprofil des Datenschutzbeauftragten
2. Einrichtung einer Übungsveranstaltung
3. Ablauf der Übungsveranstaltung
4. Erwerb eines Zertifikats

### V. Praktikum

1. Vorhandene Möglichkeiten
2. Ängste der Unternehmen
3. Betreuung der Praktikanten

### VI. Abschließende Überlegungen

1. Erweiterung der Ausbildungsangebote
2. Erfahrungsaustausch

### I. Gang der Darstellung

Nachdem die Möglichkeiten zum Einsatz von Anwälten und FH-Informatikern als Datenschutzbeauftragte skizziert worden ist, soll im folgenden dargelegt werden, welches enorme datenschutzrechtliche Potential in dem neuen Studiengang der Wirtschaftsinformatik liegt. Dabei soll zunächst das Berufsbild des Wirtschaftsinformatikers skizziert werden (II.), um anschließend auf die Studienpläne dieses Fachs vorzustellen (III.). Nach diesen einleitenden Bemerkungen soll dann das im Sommersemester 1991 begonnene Modell „Betriebliches Datenschutzrecht“ präsentiert werden (IV.-VI.).

## II. Berufsbild des Wirtschaftsinformatikers

### 1. Amtliche Darstellung

Nach den „Blättern für Berufskunde“ der Bundesanstalt für Arbeit zeichnet sich das Berufsbild eines „Diplom-Wirtschaftsinformatikers“ durch folgende Aufgaben aus:

„Der Wirtschaftsinformatiker beschäftigt sich mit der Anwendung der Informationstechnologie in betrieblichen Abläufen. Das Aufgabenspektrum, das sich dabei eröffnet, umfaßt

- den Entwurf und die Einführung betrieblicher Informationssysteme und deren Fortentwicklung
- die Erarbeitung und Einführung von Organisationskonzepten
- die Entwicklung und Einführung (für betriebswirtschaftliche Aufgabenbereiche) der Anwendungssoftware
- die Durchführung theoretischer und angewandter Forschung zur Anwendung der Informationstechnologie
- die Ausarbeitung neuer Methoden und Verfahren zur Entwicklung von Informationssystemen
- den Vertrieb von Hard- und Software-Produkten und die Unterstützung der Anwender bei der Planung, Implementierung und dem Einsatz entsprechender Produkte
- die Konzeption und Durchführung von Schulungen für die Benutzung betrieblicher Informationssysteme sowie Aus- und Weiterbildungsmaßnahmen für Hersteller, Anwender und private oder öffentliche Bildungseinrichtungen
- die Wahrnehmung von Führungsaufgaben für DV-Abteilungen, Fachabteilungen, Projekte oder für DV-Unternehmen und Beratungsfirmen.“<sup>1</sup>

### 2. Schnittstellenkompetenz

Der Wirtschaftsinformatiker steht demnach an der Schnittstelle von *Informatik und Betriebswirtschaft*. Er muß insbesondere zwischen der *Ein-/Verkaufsabteilung*, dem *EDV-Vertrieb* und der *EDV-Abteilung*

1 Blätter zur Berufskunde 2 - I A 32. Vgl. hierzu ergänzend Peter Stahlknecht, Ausbildungswege. Berufsbilder und Arbeitsmarkt für Wirtschaftsinformatiker in: Peter Mertens u.a. (Hg.), Studien- und Forschungsführer Wirtschaftsinformatik, 4. A. 1992, 8 ff.

vermitteln und in dieser Gemengelage verschiedenster Denkweisen DV-Projekte organisieren und strukturieren. Allgemein werden Wirtschaftsinformatiker aufgrund seiner umfassenden Ausbildung in zwei Disziplinen beste Aufstiegschancen in allen Bereichen des Informationsmanagements prophezeit.

## III. Diplom-Studiengang Wirtschaftsinformatik

### 1. Vorhandene Ausbildungsangebote

Der *universitäre* Diplom-Studiengang Wirtschaftsinformatik ist von der Ausbildung an Fachhochschulen und der *Universitätsausbildung* in Wirtschaftsinformatik innerhalb wirtschaftswissenschaftlicher Studiengänge abzugrenzen. Bei letzter Studienform geht es nur um eine Spezialisierung auf Datenverarbeitung im Hauptstudium der Betriebs- oder Volkswirtschaft. Der *FH-Studiengang* „Wirtschaftsinformatik“ ist hingegen kürzer und anwendungsorientierter angelegt als der *universitäre* Diplom-Studiengang.<sup>2</sup>

Wirtschaftsinformatik wird derzeit als Studiengang an folgenden *Universitäten* bzw. *Technischen Hochschulen* angeboten: Bamberg, Braunschweig, Darmstadt, Essen, Köln, Mannheim und Paderborn. Seit dem Sommersemester 1990 kann auch an der *Westfälischen Wilhelms-Universität Münster* Wirtschaftsinformatik studiert werden. Hierzu wurde ein eigenes „Institut für Wirtschaftsinformatik“ gegründet, das derzeit mit fünf Professoren besetzt ist:

- Prof. Dr. Jörg Becker (Lehrstuhl für Informationssysteme)
- Prof. Dr. Heinz Lothar Grob (Lehrstuhl für Allgemeine Wirtschaftsinformatik)
- Prof. Dr. Karl Kurbel (Lehrstuhl für Wirtschaftsinformatik)
- Prof. Dr. Ulrich Müller-Funk (Lehrstuhl für Quantitative Methoden der Wirtschaftsinformatik)
- Prof. Dr. Taudes (Lehrstuhl für Informatik)
- Prof. Dr. Rainer Unland (Lehrstuhl für Praktische Informatik in der Wirtschaft).

2 Vgl. hierzu auch die Broschüre der Bundesanstalt für Arbeit „Berufe in der Datenverarbeitung“, Blätter zur Berufskunde 0-2200, Stand 1990, S. 88 ff. sowie Rainer Bischoff, Wirtschaftsinformatik an Fachhochschulen, 2. Aufl. 1992.

## 2. Studienablauf<sup>3</sup>

Die *Regelstudienzeit* bis zum Abschluß der Diplomprüfung beträgt neun Semester. Davon entfallen je vier Semester auf das Grund- und das Hauptstudium. Während des Grundstudiums sind je zwei Vor-diplomscheine in den Fächern Wirtschaftsinformatik, Informatik, Quantitative Methoden, BWL und VWL zu erwerben. Hinzu kommen zwei propädeutische Scheine in Buchführung und „Recht für Wirtschaftsinformatiker“; auf letzteres wird unten noch ausführlicher eingegangen. Im *Hauptstudium*, das insgesamt 80 Semesterwochenstunden umfaßt, zählen Wirtschaftsinformatik, Informatik und Entscheidungslehre zu den Pflichtfächern. Zusätzlich kann der Student zwischen BWL und VWL wählen und ein weiteres Wahlpflichtfach aus folgenden Gebieten aussuchen:

- Industrieinformatik (PPS; CIM; Logistik u.a.)
- Praktische Informatik (Wissensverarbeitung; multimediale und verteilte Systeme u.a.)
- Spezielle Betriebs- und Volkswirtschaftslehren (Marketing; Wirtschaftsprüfung; Organisation und Personal u.a.).

Am Abschluß des Studiums steht dann die Diplomprüfung, die aus einer Diplomhausarbeit, Klausuren und einer mündlichen Prüfung besteht.<sup>4</sup>

## 3. Vorlesung „Recht für Wirtschaftsinformatiker“

Ziel der (nur im Wintersemester stattfindenden) vierstündigen Vorlesung ist die Vermittlung von *Grundkenntnissen* im Bereich des EDV-Rechts. Die Vorlesung gliedert sich in folgende Abschnitte:

- a) Rechtsschutz bei EDV-Produkten
  - Schutz von Hardware (insbesondere Patent- und Chipschutz)
  - Urheberrechtlicher Schutz von Software und Datenbanken

3 Vgl. hierzu auch die vom Präsidium der Gesellschaft für Informatik an Universitäten am 17. Januar 1992 verabschiedete Rahmenempfehlung für Diplom-Studiengänge Wirtschaftsinformatik an Universitäten, Informatik-Spektrum 15 (1992), 101 ff. Siehe auch *Karl Kurbel*, Studienplanempfehlungen für Diplom-Studiengänge und Schwerpunktfächer Wirtschaftsinformatik, in: Peter Mertens u.a. (Hg.), *Wirtschaftsinformatik* (FN 1), 14 ff.

4 Einzelheiten zum Studienablauf können einem „Studienführer Wirtschaftsinformatik“ entnommen werden, der bei Fachschaft Wirtschaftswissenschaft, Universitätsstr. 14-16, 4400 Münster, erhältlich ist.

- Wettbewerbs- und Warenzeichenrecht
- Der angestellte Programmierer und seine Rechte am Programm
- EG-Richtlinie zum Softwareschutz und deren Umsetzung
- Internationaler Schutz nach RBÜ und WUA
- b) EDV-Vertriebsrecht
  - Gesellschaftsrechtliche Vorfragen (Recht der OHG, GmbH und AG)
  - Grundstrukturen des EDV-Vertriebs (OEM, VAR u.a.)
  - Gewerbe- und Steuerrecht
  - Aufbau und Elemente des GWB
  - EG-Kartellrecht
- c) EDV-Vertragsrecht
  - Arten von EDV-Verträge/Bestimmung ihrer Rechtsnatur
  - Verwendungsbeschränkungen (CPU-Klauseln, LAN-Verbote)
  - Hard- und Softwarefehler/Gewährleistungsrecht
  - Haftung bei Mängeln/Produkthaftungsrecht
  - Schutzhüllenverträge
  - Vertragsgestaltung
- d) Computerstrafrecht
  - Strafvorschriften für Softwarepiraterie
  - Das Computerstrafrecht des StGB (insbesondere § 202a StGB)
  - Strafbarkeit von Hacking
- e) Datenschutz (insbesondere betriebliches Datenschutzrecht)
- f) Grundprinzipien des Telekommunikationsrechts

Im Rahmen der Vorlesung nehmen die Studenten an *Gerichtsterminen* beim Amts- und Landgericht teil; es finden ferner Gastvorträge von deutschen und ausländischen EDV-Rechtlern statt. Die Vorlesung schließt mit einer (für Studenten der Wirtschaftsinformatik obligatorischen) Klausur ab.

## IV. Übungsveranstaltung „Betriebliches Datenschutzrecht“

### 1. Anforderungsprofil des Datenschutzbeauftragten

Nach dem *Bundesdatenschutzgesetz* haben alle Unternehmen die Pflicht, einen betrieblichen Datenschutzbeauftragten zu bestellen. Da aber derzeit wenige die EDV-technischen und rechtlichen Vorkenntnisse für diese Tätigkeit besitzen, besteht ein großer Bedarf an ge-

eignetem Personal. Allerdings darf nach § 36 II BDSG zum betrieblichen Datenschutzbeauftragten nur berufen werden, wer die zur Erfüllung der anstehenden Aufgaben erforderliche *Fachkunde* und Zuverlässigkeit besitzt. Was unter dem Begriff „Fachkunde“ zu verstehen ist, kann abstrakt wohl kaum festgelegt werden. Wie bereits das rheinland-pfälzische Innenministerium im Dezember 1987 betont hat, hängt das Ausmaß der erforderlichen Fachkunde von der Art und Größe des Unternehmens ab. Gerade deshalb habe der Gesetzgeber „bei Verabschiedung des Bundesdatenschutzgesetzes ausdrücklich davon abgesehen, für den betrieblichen Datenschutzbeauftragten eine bestimmte Ausbildung zu fordern oder spezifische Anforderungen an seine Fachkunde gesetzlich festzulegen“.<sup>5</sup>

Die *Aufsichtsbehörden* gehen regelmäßig davon aus, daß drei verschiedene Wissensbereiche vom Datenschutzbeauftragten abgedeckt werden müssen:

- betriebswirtschaftliche Kenntnisse (einschließlich eines Grundwissens über die Organisationsstruktur des Betriebes)
- Kenntnisse der Datenverarbeitung/EDV (allerdings abgestuft nach den spezifischen Gegebenheiten des Unternehmens)
- gute Kenntnisse im Datenschutz- und Datensicherheitsrecht.<sup>6</sup>

## 2. Einrichtung einer Übungsveranstaltung

Diese *Konkretisierung* des Begriffs „Fachkunde“ macht sofort deutlich, warum eine Zusatzausbildung im betrieblichen Datenschutzrecht für angehende Diplom-Wirtschaftsinformatiker sinnvoll ist: Diese Studentengruppe erwirbt während ihres Studiums sehr weitreichende Kenntnisse in Betriebswirtschaft und Informatik. Kommen Kenntnisse im betrieblichen Datenschutzrecht hinzu, ist der Wirtschaftsinformatiker der optimale Datenschutzbeauftragte.

Diese Überlegungen waren auch der Grund, warum am Institut für Wirtschaftsinformatik in Münster zum *Sommersemester 1991* erstmals eine Übung zum betrieblichen Datenschutzrecht angeboten

5 LT-Drs Rheinland-Pfalz 11/462 vom 14. Dezember 1987, zitiert nach CR 1990, 622.

6 Vgl. S. 4 f. der Checkliste für Auftragsrechenzentren des Regierungspräsidenten Arnsberg. Mein besonderer Dank geht an Herrn Ahlers für die Bereitstellung dieser Checkliste.

wurde. Die Resonanz auf dieses Angebot war sehr gut: Von den achtzig Erstsemestern nahmen ca. 70 Studenten freiwillig an der Übung teil. Im Sommersemester 1992 stieg die Zahl der Teilnehmer auf knapp 100. Die Übung findet nur im Sommersemester an zwei Stunden pro Woche statt. *Teilnahmeberechtigt* sind nur Studenten, die im vorangegangenen Wintersemester die Klausur „Recht für Wirtschaftsinformatiker“ bestanden haben.<sup>7</sup> Diese Zulassungsbeschränkung hat große Vorteile: Diejenigen, die mit Erfolg die Vorlesung im Wintersemester besucht haben, verfügen bereits über Grundkenntnisse im Datenschutzrecht. Darüber hinaus haben sie einen Überblick über die Grundstruktur des Handels- und Gesellschaftsrechts und können dadurch einige datenschutzrechtliche Fragen (z.B. die Outsourcing-Thematik oder die Frage der Übermittlung im Konzern) besser nachvollziehen.

## 3. Ablauf der Übungsveranstaltung

Das *Ziel* der Übung besteht in dem Erwerb der rechtlichen Grundkenntnisse, die für eine Beschäftigung als Datenschutzbeauftragter notwendig sind. Der Kurs beschäftigt sich daher vorwiegend mit dem neuen Bundesdatenschutzgesetz (BDSG). Darüber hinaus werden die Grundzüge des künftigen europäischen Datenschutzrechts sowie die betriebsverfassungsrechtlichen Komponenten des Datenschutzes ausführlich erörtert. Ausgespart bleiben Fragen der technischen Datensicherheit, die Vermittlung dieses Bereichs ist Gegenstand anderer Vorlesungen während des Studiums.<sup>8</sup>

In der Übung geht es nicht darum, alle Detailprobleme des Datenschutzrechts vorzutragen. Vielmehr sollen die Studenten am Ende der Übung in der Lage sein, Fälle aus der betrieblichen Praxis anhand des BDSG zu lösen. Vermittelt werden soll aus diesem Grund vor allem die juristische Subsumtions- und Gutachtentechnik; denn nur diese Technik erlaubt es in der Praxis, auch unvorgesehene und unbekannte Sachverhaltsfragen anhand einer methodisch präzisen Analyse des

7 Hinzu kommen allerdings aufgrund besonderer Zulassung Praktiker aus verschiedenen Wirtschaftsunternehmen (vor allem der Versicherungsbranche) sowie einige Studenten anderer Universitäten (besonders aus Bochum, Duisburg und Köln).

8 Einen Einblick in die inhaltliche Struktur der Übungsveranstaltung bietet die als Anhang abgedruckte Gliederung der Veranstaltung.

Gesetzestextes zu lösen. Wichtig ist hierbei didaktisch die *Bildung von Kleingruppen*: Erfahrungsgemäß ermüdet der frontale Vortrag über datenschutzrechtliche Fragen sehr schnell die Zuhörer. Die komplizierte Regelungstechnik des BDSG macht es zwingend erforderlich, daß einfache Fälle von Studenten in kleineren Gruppen (max. 6-7 Personen) gelöst werden. Diese Gruppenarbeit macht einen Teil der Übungsstunde aus. Daneben waren die Studenten aber auch bereit, sich privat zu treffen und über weitere Fälle zu diskutieren. Hinzu kommen sog. „Moot Courts“: Mehrere Studenten erklären sich z. B. freiwillig bereit, in die Rolle des Betriebsrates und der Unternehmensleitung zu „schlüpfen“ und eine Auseinandersetzung um betriebsverfassungsrechtliche Mitbestimmungsfragen bei der Einführung von Personalinformationssystemen zu spielen. Dabei soll das Spiel möglichst authentisch sein. Daher bereiten die Parteien vorab schriftliche Rechtsgutachten und Stellungnahmen vor, die der anderen Seite zugestellt werden. In einer öffentlichen Sitzung vor den anderen Studenten wird der Fall noch einmal vorgeführt und zur Entscheidung durch eine Schlichtungsgruppe gebracht, nachdem die Zuhörer vorher noch um ihr Votum geben worden sind.

Die Studenten erhalten zu Beginn des Semesters ein *Skriptum*, das neben einigen Materialien (BDSG; Entwurf der EG-Datenschutzrichtlinie; Auszüge aus dem BetrVG sowie zentrale Aufsätze) auch Aufbauschemata für die Lösung datenschutzrechtlicher Fälle enthält. Zusätzlich wurde den Studenten die Lektüre der Abhandlung „Der Datenschutzbeauftragte“ von Müller/Wächter<sup>9</sup> und des Werkes „Datenschutzrecht“ von Wohlgemuth<sup>10</sup> empfohlen.<sup>11</sup> Dabei wird angeregt, daß die Studenten sich parallel zur Vorlesung mit dem Skriptum beschäftigen. Hierzu haben die Studenten bislang in freiwilliger Initiative Kleingruppen gebildet, die sich privat treffen und datenschutzrechtliche Fragen diskutieren.

9 2. Aufl. 1991.

10 Hans H. Wohlgemuth, Datenschutzrecht. Eine Einführung mit praktischen Fällen, 1992.

11 Die Empfehlung beruht – unabhängig von den Vorzügen und Nachteilen dieser Werke – auf dem traurigen Umstand, daß zum neuen BDSG kaum Einführungsliteratur vorhanden ist. Diese Lücke vermag vielleicht künftig das jetzt erschienene Werk von Tinnefeld/Ehmann, Einführung in das Datenschutzrecht, München/Wien, 1992 zu schließen.

#### 4. Erwerb eines Zertifikats

Im Anschluß an die Übung besteht die Möglichkeit, an einer Klausur teilzunehmen und ein „Zertifikat Betriebliches Datenschutzrecht“ zu erwerben. Dieses Zertifikat bestätigt, daß der Student die rechtlichen Grundkenntnisse für eine Tätigkeit als betrieblicher Datenschutzbeauftragter besitzt.

Anders als beim *Ulmer Modell*<sup>12</sup> wird damit nicht das Vorhandensein aller Voraussetzungen für die Fachkunde attestiert. Vielmehr beschränkt sich das Münsteraner Modell auf die rechtliche Komponente der Fachkunde, alles weitere müssen die Studenten durch ihren Studienabschluß bzw. später durch ihre Aneignung betriebsinternen Organisations-Know-Hows selber nachweisen.

### V. Praktikum

#### 1. Vorhandene Möglichkeiten

Als äußerst *sinnvoll* hat es sich erwiesen, daß die Übungsteilnehmer im Anschluß an die Veranstaltung (während der Sommerferien und teilweise im Anschluß an das Wintersemester) an einem Betriebspraktikum teilnehmen und „vor Ort“ die Tätigkeit betrieblicher Datenschutzbeauftragter kennenlernen. Allerdings standen bislang nur *wenige Praktikumsplätze* zur Verfügung.<sup>13</sup> Dies hängt einmal damit zusammen, daß das Münsteraner Modell noch zu neu und unbekannt ist. Auf der anderen Seite aber scheuen sich manche Unternehmen, Studenten in einen solch sensiblen Bereich wie dem Datenschutzrecht einen Einblick zu verschaffen.

#### 2. Ängste des Unternehmens

Oftmals findet sich die (unberechtigte) Angst, Studenten würden auf datenschutzrechtliche Mißstände stoßen oder sich mit dem Betriebsrat gegen die Unternehmensleitung solidarisieren. Hinter dieser Angst

12 Siehe dazu den Beitrag von *Kongehl* in diesem Band, S. 123 ff.

13 Der Verfasser dieses Beitrags würde sich daher sehr freuen, wenn sich weitere Unternehmen zur Einrichtung eines Praktikumsplatzes bereit erklären könnten. Rückfragen werden erbeten an: Dr. Thomas Hoeren, Institut für Kirchenrecht, Universitätsstr. 14-16, 4400 Münster.

verbirgt sich eine Unsicherheit darüber, ob das Unternehmen alle Anforderungen des Datenschutzrechts und des Betriebsverfassungsrechts erfüllt. Meist gelingt es jedoch, diese Angst zumindest teilweise mildern.

### 3. Betreuung der Praktikanten

Hierzu hat es sich als zweckmäßig erwiesen, eine intensive *Vor- und Nachbereitung* des Praktikums durchzuführen. Die beteiligten Unternehmen werden vorab gebeten, ein Anforderungs- und Aufgabenprofil des Praktikanten zu erstellen. Auf dieser Grundlage werden gezielt Studenten ausgewählt, die dann auch auf die späteren Aufgaben (insbesondere Schulungstätigkeiten) vorbereitet werden.

Während des Praktikums findet laufend *Rücksprache* mit dem unternehmensinternen Betreuer des Praktikanten statt. Ferner werden abschließend schriftliche Berichte von den Studenten angefordert, auch die Unternehmensleitung wird um eine Beurteilung gebeten. Nur auf diese zeitintensive Art und Weise kann ein Vertrauensverhältnis zwischen Praktikant, Unternehmen und Universität entstehen, das eine effiziente Ausbildung der Studenten „vor Ort“ erst ermöglicht.

## VI. Abschließende Überlegungen

### 1. Erweiterung der Ausbildungsangebote

Gerade angesichts der guten Erfahrungen mit dem Münsteraner Modell wäre es von großer Bedeutung, wenn auch an *anderen Hochschulen* Kurse und Übungen zum Datenschutzrecht eingerichtet werden könnten. Noch bestehen sehr wenige Angebote zur universitären Schulung auf diesem Gebiet.

### 2. Erfahrungsaustausch

Ferner wäre es für die Zukunft wünschenswert, daß sich alle *Übungsleiter und Dozenten*, die im datenschutzrechtlichen Bereich tätig sind, zum Erfahrungsaustausch treffen. In Großbritannien besteht seit Jahren eine sehr erfolgreiche Vereinigung von EDV-rechtlich orientier-

ten Hochschuldozenten.<sup>14</sup> In Deutschland war es bislang nicht möglich, eine solche Vereinigung ins Leben zu rufen.

Dies ist um so bedauerlicher, als *viele Fragen* nur in einem offenen Vergleich der verschiedenen Lehrkonzepte und einem Gespräch aller Datenschutzdozenten zu klären sind:

- Wie können zum Beispiel Didaktik<sup>15</sup>, Erwachsenenpädagogik<sup>16</sup> und universitäre Ausbildung im Datenschutz miteinander verbunden werden?
- Wie können die Ergebnisse der modernen Lerntheorie für die Vermittlung der komplizierten Strukturen des BDSG genutzt werden?
- Wie können Studenten – etwa in medienpädagogischer Hinsicht<sup>17</sup> – auf ihre späteren Schulungsaufgaben (vgl. § 37 I 2 Nr. 2 BDSG) vorbereitet werden?

14 Die sog. „British and Irish Legal Education and Technology Association“ (BILETA); vgl. zu den Konferenzen dieser Organisation den letzten Bericht in *Computers and Law*, March 1992, 31 ff.

15 Vgl. B. Adl-Amini/R. Künzli (Hg.), *Didaktische Modelle und Unterrichtsplanung*, 1980 mit weit. Nachw.

16 Vgl. hierzu die Nachweise bei Klaus W. Döring, *Lehren in der Weiterbildung*. Ein Dozentenleitfaden, 3. Aufl. 1990, 293 ff.

17 Vgl. J.H. Schoeps/R. Proske/F. Greiner (Hg.), *Weiterbildung durch Medien*, 1982 mit weit. Nachw.

## Anhang: Inhaltliche Struktur der Übung „Betriebliches Datenschutzrecht“

- I. Historische Entwicklung des Datenschutzrechts
  1. Die Anfänge in Schweden und den USA
  2. Die Regelungen in Hessen
  3. Das Bundesdatenschutzgesetz 1977 und die Ländergesetze
  4. Das Volkszählungsurteil
  5. Bereichsspezifische Regelungen (SGB, MRRG)
  6. Europäische Überlegungen
  7. Das Bundesdatenschutzgesetz 1991
- II. Grundbegriffe des BDSG
  1. Zweck des BDSG
  2. Die rechtliche Grundstruktur des BDSG
    - a) Der Aufbau des BDSG
    - b) Die Abgrenzung von öffentlicher und nicht-öffentlicher Stelle
    - c) Exemptionsvorschriften (§§ 40 ff.)
    - d) Das Verhältnis des BDSG zu anderen Gesetzen
  3. Die §§ 1 – 3 BDSG / Begriffsbestimmungen
    - a) Personenbezogene und anonymisierte Daten
    - b) Akten und Dateien
    - c) Automatisierte und nicht-automatisierte Dateien
    - d) Die DV-Phasen (§ 3 IV – VII)
    - e) Das Problem des „Dritten“ im Sinne des § 3 IX
  4. Die Magna Charta des Datenschutzes / Zur Bedeutung des § 4
  5. Unabdingbare Rechte des Betroffenen (§ 6)
  6. Schadensersatz im DV-Bereich (insbesondere § 8)
  7. Die Problematik der Online-Verfahren (§ 10)
  8. Technisch-organisatorische Maßnahmen
    - a) Datensicherheit (Anlage zu § 9)
    - b) Datengeheimnis (§ 5)
  9. Strafvorschriften
- III. Das BDSG und die Datenverarbeitung im Privatbereich (§§ 27 ff.)
  1. Zulässigkeit der Datenspeicherung (§§ 28 ff.)
  2. Zulässigkeit der Datenübermittlung/-nutzung (§ 28)
  3. Meldepflichten (§ 32)
  4. Rechte des Betroffenen (§ 33 ff.)

5. Die Aufgaben des betrieblichen Datenschutzbeauftragten (§§ 36 ff.)
6. Die Befugnisse der Aufsichtsbehörde (§ 38)
- IV. Betriebsverfassungsrechtliche Probleme
  1. Grundbegriffe des Betriebsverfassungsrechts
  2. Die Rechtsprechung des BAG zu § 87 I Nr. 6 BetrVG
  3. Kooperation von Betriebsrat und Datenschutzbeauftragten
  4. Die Betriebsvereinbarung als Regelungsinstrument im Datenschutz
- V. Bereichsspezifische Datenschutzregelungen
  1. Das SGB X
  2. Sonderregelungen im Forschungsbereich
  3. Sonderregelungen im Pressebereich
- VI. Europäische Regelungen
  1. Die Aktivitäten der OECD
  2. Die Datenschutz-Konvention des Europarates (1985)
  3. Der Entwurf einer EG-Richtlinie über die Angleichung des Datenschutzrechts
  4. Verträge über grenzüberschreitenden Datentransfer/EDI
- VII. Wichtige Institutionen und Hilfsmittel
  1. GDD (Köln)/FH Ulm
  2. Monographien
  3. Zeitschriften
  4. Didaktische Hinweise zur Durchführung von Schulungen

## Musterklausur Datenschutzrecht

von Dr. Thomas Hoeren, Münster  
und Florian Walter, Münster

I. Vorbemerkung  
II. Text der Klausuraufgabe

III. Originallösung eines  
Studenten

### I. Vorbemerkung

Die folgende Klausur ist im *Sommersemester 1992* am Institut für Wirtschaftsinformatik in Münster im Rahmen der Übung „Betriebliches Datenschutzrecht“ gestellt worden. Im Anschluß an den Klausurtext findet sich der Lösungsversuch eines Studenten, dessen Klausur mit „gut“ bewertet wurde.

Der ursprüngliche *Stil* des Lösungsversuchs wurde (abgesehen von Rechtschreib- und Zeichensetzungsfehlern) beibehalten. Lediglich der Fettdruck einzelner Begriffe entspricht nicht dem Original und wurde vom Herausgeber veranlaßt. Von einer „Glättung“ der Darstellungsform wurde bewußt abgesehen, doch hat der Herausgeber die vier Zwischenüberschriften eingefügt, damit sich der Leser leichter zurechtfindet.

In den *Fußnoten* finden sich Hinweise zur Korrektur der Arbeiten sowie ergänzende Kommentierungen. Die in der Klausur wiedergegebenen Wertungen stammen vom Bearbeiter der Klausur; sie lassen daher keine Rückschlüsse auf die Wertungen des Klausurkorrektors zu.

Für die Klausur standen als *Bearbeitungszeit* 120 Minuten zur Verfügung; den Studenten wurde neben dem Klausurtext ein Exemplar des BDSG überreicht.<sup>1</sup> Entsprechend der Bearbeitungszeit wurde auch ein Maximum von 120 Punkten festgesetzt; jeder Bearbeiter wußte demnach, wieviel Bearbeitungszeit der Aufgabensteller für die einzelnen Fragen vorgesehen hatte.

Das *Ergebnis* war erfreulich: Nur etwa 40 % der Studenten bestanden die Prüfung nicht. Im übrigen gab es ca. 35 % Klausuren mit der Benotung „Ausreichend“, 15 % mit „Befriedigend“ und 10 % mit „Gut“.

<sup>1</sup> Mein besonderer Dank geht an dieser Stelle an die Pressestelle des Bundesbeauftragten für den Datenschutz, die uns großzügig mit Texten versorgt hat.

### II. Text der Klausuraufgabe

**Frage 1:** Das Unternehmen S soll wegen datenschutzrechtlicher Verstöße ein *Bußgeld* in Höhe von 50.000,- DM zahlen (vgl. § 44 BDSG). Hintergrund hierfür waren folgende Vorfälle:

- Ein Mitarbeiter der S hatte die Daten von Stellenbewerbern in einer (nur für ihn bestimmten) Handkartei gesammelt, ohne die Betroffenen über diesen Vorgang zu informieren.
- Der Regierungspräsident in Arnberg hatte der S die Verwendung eines bestimmten Softwareproduktes wegen schwerer technischer Mängel des Programms untersagt. Die S hat die Software dennoch weiter eingesetzt.

S hält die Verhängung des Bußgeldes für unzulässig. Zu Recht? (35 P.)

**Frage 2:** Der *Betriebsrat* des Unternehmens S möchte Daten von Arbeitnehmern (Name, Anschrift) an die Gewerkschaft zwecks Mitgliederwerbung weitergeben. Der Datenschutzbeauftragte der S legt hiergegen Protest ein. Wer hat Recht?

Würde sich die Rechtslage ändern, wenn die Weitergabe an die Gewerkschaft in einer Betriebsvereinbarung geregelt worden wäre? (40 P.)

**Frage 3:** In welchem Umfang haftet der *betriebliche Datenschutzbeauftragte* für datenschutzrechtliche Verstöße innerhalb des Betriebes? (15 P.)

**Frage 4:** Inwieweit kann ein *Betriebsrat* Einfluß auf die Einführung von Software in einem Betrieb nehmen? Beschreiben Sie ausführlich und unter kritischer Würdigung der Rechtsprechung alle in Betracht kommenden Möglichkeiten! (30 P.)

### III. Originallösung eines Studenten

#### 1) Lösung von Frage 1:

1. „Stellenbewerber-Handkartei“

Ein Bußgeld müßte nach § 44 I Nr. 3 verhängt werden, wenn die Bewerber *entgegen* § 33 nicht benachrichtigt worden wären.<sup>2</sup> Hierzu

<sup>2</sup> Die Formulierung ist sprachlich mißglückt. Ein Bußgeld *ist* zu verhängen, wenn gegen § 33 verstoßen worden *ist*. Der Gebrauch des Konjunktivs



wäre zu prüfen, ob das BDSG überhaupt anzuwenden ist, und wenn ja, ob ein Verstoß gegen § 33 vorliegt. Gem. § 3 I ist das Gesetz auf *personenbezogene Daten* anwendbar. Hier ist anzunehmen, daß es sich um Daten wie Name, Anschrift, Qualifikation, angestrebte Tätigkeit, Gehaltsvorstellung und ähnliches handelt. Insofern liegen personenbezogene Daten vor. Weiterhin muß eine *Verarbeitung oder Nutzung* der Daten vorliegen. Hier kann eine Verarbeitung in der Ausprägung der Speicherung (§ 3 V 1)<sup>3</sup> angenommen werden.<sup>4</sup> Der personelle *Anwendungsbereich des BDSG* ist hier der nicht-öffentliche Bereich, da es sich um ein privatrechtlich organisiertes und handelndes Unternehmen zu handeln scheint. Nicht-öffentliche Stellen müssen gemäß § 1 II 3 die Daten geschäftsmäßig oder für berufliche/gewerbliche Zwecke nutzen. Bei Bewerberdaten von Bewerbern, die später evtl. angestellt werden sollen, ist von einer Verarbeitung der Daten zu gewerblichen Zwecken auszugehen.

Weiterhin müssen die Daten „in oder aus Dateien“ (§ 1 II 3) verarbeitet werden. Eine Datei muß nicht notwendigerweise automatisiert verarbeitet werden können. Nach § 3 II 2 kann auch z.B. eine Kartei eine sog. „nicht-automatisierte Datei“ sein, wenn sie „nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann“. Das ist bei Karteien (auf Karteikarten o.ä.) üblicherweise gegeben und hier insbesondere anzunehmen, weil erstens mehrere Daten für jeden Bewerber gespeichert werden (s.o.) und die Speicherung für den Mitarbeiter der S nur sinnvoll ist, wenn er die Bewerberdaten z.B. nach der Qualifikation oder nach dem Beschäftigungswunsch auswerten kann.

Allerdings enthält § 1 III 2 eine *Einschränkung*: Nicht automatisierte Dateien, die nicht zur Weitergabe bestimmt sind, fallen (mit Ausnahme der §§ 5, 9, 39 und 40) nicht unter das BDSG. Dieser Fall ist

[Irrealis!] zeigt eine Unsicherheit des Studenten und ein gestörtes Verhältnis zur Wirklichkeit. Allerdings sind auch gestandene Rechtsprofessoren vor solchen Fehlern nicht gefeit; vgl. *Diederichsen*, Die BGB-Klausur, 4. Aufl. 1978.

- 3 Es macht den Studenten immer wieder Schwierigkeiten, die entsprechende Passage des Gesetzes richtig zu zitieren. Hier hätte es 3 V 2 Nr. 1 heißen müssen.
- 4 Hinzu kommt auch die Nutzung der Daten im Bereich der Personalabteilung, vgl. § 3 VI.

laut Sachverhalt hier gegeben. Insofern ist das BDSG nicht anwendbar und ein Bußgeld nicht angebracht.<sup>5</sup>

## 2. Programmstilllegung

Eine *Bußgeldverhängung* könnte gemäß § 44 I Nr. 7 BDSG geboten sein. Aus dem Sachverhalt geht nicht hervor, ob mit dem Programm personenbezogene Daten oder andere Daten verarbeitet werden. Geht man von letzterem aus, greift das BDSG nicht (vgl. § 1 II und § 3 I). Im folgenden wird aber angenommen, daß die Regelungen des BDSG zum Zuge kommen. Für ein Bußgeld gemäß § 44 I Nr. 7 müßte eine *Anordnung* nach § 38 V 1 ignoriert worden sein. Gem. § 38 V 1 kann die Aufsichtsbehörde Maßnahmen zur Beseitigung technischer und organisatorischer Mängel verlangen. Da in Satz 2 desselben Paragraphen die Stilllegung eines Programms noch explizit erwähnt wird, ist anzunehmen, daß das keine Maßnahme im Sinne des Satz 1 ist. Die Stilllegung kann erst nach dem Unterbleiben von Maßnahmen und nach Verhängung eines Zwangsgeldes angeordnet werden. Davon ist anscheinend nichts geschehen. Im übrigen erlaubt § 44 I Nr. 7 eine Bußgeldverhängung nur bei Zuwiderhandlung gegen eine *vollziehbare Anordnung* nach § 38 V 1. Der Regierungspräsident kann sich demnach nicht auf § 38 V 2 für das Bußgeld berufen. Denn Straf- und Bußgeldvorschriften sind eng auszulegen und dürfen auch über eine Analogie nicht extensiv ausgelegt werden.<sup>6</sup>

Insofern ist die Bußgeldverhängung im Falle der Bewerberkartei zu *Unrecht* und im Falle der Stilllegung des Programms verfrüht und somit ebenfalls zu Unrecht erfolgt.

- 5 Es fiel zahlreichen Studenten erstaunlicherweise schwer, auf das Vorliegen einer internen Datei gem. § 1 III Nr. 2 zu kommen. Die meisten übersahen diese Vorschrift, obwohl bereits die Fragestellung überdeutlich war. Was statt dessen erörtert wurde, war teilweise erschreckend: Einige Studenten prüften, ob die Verarbeitung der Daten im Sinne von § 28 BDSG rechtmäßig war und begründeten ein Bußgeld mit der Unzulässigkeit der Speicherung.
- 6 Die Frage des Bußgeldes (§ 44) war während der Übung nicht ausführlicher mit den Studenten erörtert worden. Dennoch war die Lösung dieser Teilfrage sicherlich nicht allzu schwer; sie erforderte nur eine genaue Lektüre des Gesetzes. Genau um diese Genauigkeit ging es didaktisch bei der Fragestellung.

## 2) Lösung von Frage 2:

Gem. § 4 BDSG ist jede Datenverarbeitung grundsätzlich verboten, es sei denn, es liegt eine Ausnahme vor, d.h., daß der Betroffene eingewilligt hat oder eine Rechtsvorschrift dies erlaubt. Zunächst ist aber die *Anwendbarkeit des BDSG* zu prüfen. Es handelt sich um personenbezogene Daten gem. § 3 I, nämlich um Name, Anschrift und Betriebszugehörigkeit einer natürlichen Person. Verarbeitet werden die Daten hier in dem besonderen Sinne einer *Übermittlung* an Dritte (§ 3 IV 3); denn die Daten werden der Gewerkschaft bekanntgegeben. Die Gewerkschaft ist organisatorisch völlig getrennt vom Betriebsrat. Eine gemeinsame Aufgabenerfüllung, die Gewerkschaft und Betriebsrat zu einer funktionalen Stelle machen könnte, ist auch nicht anzunehmen. Weder Gewerkschaft noch Betriebsrat sind öffentliche Stellen im Sinne von § 2 I-III. Somit sind hier die Regelungen für Datenverarbeitung im nicht-öffentlichen Bereich anzuwenden. Hierzu müssen die Daten *in oder aus Dateien* verarbeitet werden. Da die Daten von Arbeitnehmern angesichts der vielfältigen Nutzung in Unternehmen (Lohnzahlung, Rente, Sozialversicherung, Jubiläen...) nur in Dateien sinnvoll zu speichern sind, ist anzunehmen, daß die Daten aus Dateien entnommen werden.

Weiterhin muß die Datenverarbeitung im privaten Bereich *geschäftsmäßig* oder für berufliche und gewerbliche Zwecke erfolgen. Berufliche und gewerbliche Zwecke scheiden hier aus, da der Betriebsrat keine Ertragsziele verfolgt und seine Betriebsrat-Tätigkeit auch nicht als Beruf zu sehen ist. Nach hM reicht für eine geschäftsmäßige Datenverarbeitung schon ihr routinemäßiges, gewöhnliches Vorkommen.<sup>7</sup> Da die Mitgliederwerbung der Gewerkschaft ein ständiges Anliegen ist, ist hier eine geschäftsmäßige Verarbeitung anzunehmen. Somit kann das BDSG angewendet werden. Insofern ist die Weitergabe der Daten verboten, es sei denn, die Betroffenen hätten eingewilligt oder ein Gesetz erlaubt die Weitergabe. Von einer *Einwilligung* ist nichts zu erkennen, zumal diese gemäß § 4 II schriftlich vorliegen müßte.

Da hier eine Datenübermittlung für eigene Zwecke vorliegt, könnte die Weitergabe *gemäß § 28* zulässig sein. § 28 I Nr. 1: Ist nicht anzu-

<sup>7</sup> Vgl. zum Meinungsbild *Bergmann/Möhrle/Herb*, Datenschutzrecht, § 1 Rdnr. 37 f.; *Mallmann* in *Simitis/Dammann/Geiger/Mallmann/Walz*, Kommentar zum Bundesdatenschutzgesetz, 4. Aufl., Loseblattausgabe. Stand 1992, § 29 Rdnr 7 ff. mit weiteren Nachweisen.

nehmen, da zwischen dem Arbeitnehmer und dem Betriebsrat kein Vertrag und auch kein vertragsähnliches Vertrauensverhältnis besteht. Auch der Arbeitsvertrag zwischen Arbeitgeber und Arbeitnehmer rechtfertigt keine Übermittlung von Daten an die Gewerkschaft.<sup>8</sup>

§ 28 I Nr. 2: Ob ein berechtigtes Interesse des Betriebsrates an der Weitergabe der Daten besteht, ist fraglich, da sich die Interessen der Gewerkschaft und des Betriebsrates keinesfalls decken müssen. Das mag auch dahingestellt bleiben, weil im zweiten Halbsatz der Ziffer 2 gefordert ist, daß „kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Verarbeitung ... überwiegt.“ Hier ist also den Interessen des Betroffenen ein großes Gewicht einzuräumen. Daß ein schutzwürdiges Interesse besteht, kann hier angenommen werden, da neben der Anschrift auch implizit das Arbeitsverhältnis mit angegeben wird.<sup>9</sup>

§ 28 I Nr. 3: Die Daten stammen insofern nicht aus allgemein zugänglichen Quellen, als zwar Namen und Adressen oft (nicht bei jedem!) im Telefonbuch ersichtlich sind. Ob jedoch jemand bei der S angestellt ist, kann auf keinen Fall als öffentlich zugänglich angesehen werden. Diese Information ist aber bei jedem Namen, der übermittelt wird, zumindest implizit beigegeben. § 28 II 1 lit. b): Denkbar wäre auch, daß es sich hier um eine Übermittlung zusammengefaßter Daten handelt. Auch wenn die Vorschrift ursprünglich vor allem für die Werbe- und Marketingbranche konzipiert worden ist, bestehen keine Bedenken, sie auch auf das Verhältnis Betriebsrat-Gewerkschaft anzuwenden.

Offensichtlich<sup>10</sup> erhält die Gewerkschaft hier eine *Liste* von Arbeitnehmerdaten. Dabei sind Name, Anschrift und Betriebszugehörigkeit

<sup>8</sup> Diese Ausführungen sind etwas kurz und klingen stark nach „Urteilsstil.“

<sup>9</sup> Der Verfasser spielt hier auf § 28 II Nr. 1 S. 2 an. Diese Vorschrift im Rahmen von § 28 I anzuwenden, ist vertretbar, dies hätte aber einer sorgfältigeren Subsumtion bedurft. Unten wird ausführlicher auf diesen Mangel eingegangen. Im Ergebnis machte es vielen Studenten Schwierigkeiten, die im Rahmen von §§ 28, 29 erforderliche Interessenabwägung in concreto mit Leben zu füllen. Im Rahmen der Klausur kam es daher zumeist zu bloßen Behauptungen hinsichtlich einer Beeinträchtigung der Interessen der Betroffenen.

<sup>10</sup> Solche Füllwörter sind gefährlich, da sie meist psychologisch auf eine Unsicherheit des Studenten verwiesen; dieser will jeder Diskussion und Kritik durch den Einsatz einer solchen Redewendung umgehen. Ähnliches gilt auch für Begriffe wie „zweifelsohne“ oder „selbstverständlich“.

von der Aufzählung in § 28 II 1 lit. b) gedeckt. Es fragt sich aber, ob hier nicht „Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.“<sup>11</sup> Hier ist zu beachten, daß nach § 28 II Daten über arbeitsrechtliche Verhältnisse im Regelfall nie weitergegeben dürfen, da es sich um besonderes sensible Daten handelt.<sup>12</sup> Insofern kann vorliegend davon ausgegangen werden, daß auch die Übermittlung einer Liste an die Gewerkschaft die schutzwürdigen Interessen des Betroffenen verletzt und deswegen unzulässig ist. Insgesamt ist die Übermittlung der Daten vom Betriebsrat an die Gewerkschaft als unzulässig anzusehen.

*Zusatzfrage:* Änderung, wenn eine Betriebsvereinbarung bestünde? Laut höchstrichterlicher *Rechtsprechung des BAG* haben Tarifverträge und Betriebsvereinbarungen bezüglich der Regelungen des BDSG den Rang eines Gesetzes, das die Verarbeitung von Daten erlauben kann. Diese Auffassung ist als höchst fragwürdig anzusehen, da in diesem Fall Arbeitgeber und Betriebsrat ohne gesetzliche Schranken über die eigentlich geschützten Belange des Arbeitnehmers entscheiden können. In diesem Fall wäre also die Übermittlung von Daten und Betriebsrat an die Gewerkschaft zulässig, wenn eine Betriebsvereinbarung sie gestatten würde.

### 3) Lösungen von Frage 3:

Im Prinzip haftet dem Betroffenen jeder an einer schadensersatzpflichtigen Rechtsgutverletzung Beteiligte gemäß § 823 I BGB. Der Betroffene kann also sowohl den betreffenden Sachbearbeiter als auch das Unternehmen als auch den Datenschutzbeauftragten oder alle drei (oder zwei davon) verklagen. Streitig ist allerdings, ob der Datenschutzbeauftragte aus § 823 II BGB iVm § 37 BDSG wegen Verletzung seiner Pflichten haftet.

- 11 Der Gesetzeswortlaut darf nicht abgeschrieben werden. Dies macht naturgemäß vielen Studenten (auch der Jurisprudenz) Schwierigkeiten, die in ihrer Unsicherheit froh sind, durch Zitieren des Gesetzes erst einmal etwas aufs Papier gebracht zu haben.
- 12 Dies ist nun allerdings zumindest von der Argumentation unzutreffend. § 28 II Nr. 1 S. 2 enthält mehrere Voraussetzungen, von denen der Verfasser nur eine kurz erwähnt. Im übrigen greift diese Regelung nur bei „Übermittlung durch den Arbeitgeber“. Die Frage wäre hier gewesen, ob der Betriebsrat hier als unselbständiger Teil des Arbeitgebers angesehen werden kann; dieses Problem wird von der Literatur unterschiedlich gelöst.

Im *Innenverhältnis* kann es aber sein, daß der Arbeitgeber für seine Arbeitnehmer einstehen muß, auch wenn sie eigentlich für die Verletzung ihrer arbeitsvertraglichen Pflichten aus pVV haften.<sup>13</sup>

Dazu hat das BAG den Begriff der „*gefährgeneigten Arbeit*“ herausgebildet. Hier hat der Arbeitgeber, in dessen Interesse sich die Arbeitnehmer der Gefahr aussetzen, die Risiken zu tragen, sofern nicht Vorsatz oder schwere Fahrlässigkeit vorliegt (Tinnefeld<sup>14</sup>). Bei mittlerer Fahrlässigkeit (die im Einzelfall zu konkretisieren wäre) wird die Haftung aufgeteilt. Bei leichtester Fahrlässigkeit muß der Arbeitgeber im Innenverhältnis für alle vom Arbeitnehmer verursachten Schäden aufkommen; der Arbeitnehmer hat insofern auch einen Freistellungsanspruch.<sup>15</sup>

Im Falle eines einfachen *Sachbearbeiters* ist eine gefährgeneigte Arbeit stets anzuwenden, da der AG für die Schulung des AN zuständig ist und dem AN nicht zuzumuten ist, daß er sich bis ins letzte in der komplexen DS-Materie auskennt.

Das ist andererseits gerade dem *betrieblichen Datenschutzbeauftragten* zuzumuten. Seine Aufgabe ist es ja gerade, die Datenschutzbelange in jeder Hinsicht wahrzunehmen und zu schützen. Die Anwendbarkeit der Grundsätze der gefährgeneigten Arbeit des Datenschutzbeauftragten wird kontrovers diskutiert. Einerseits ist auch der Datenschutzbeauftragte nicht vor Fehlern gefeit, eine Gefahr besteht also auch für ihn. Andererseits wäre natürlich eine Beteiligung an der Haftung auch ein Impetus, die Einhaltung der Datenschutzgesetze streng zu prüfen. Hat ein Arbeitnehmer einen gewissen Überblick über die Folgen seines Tuns, ist ihm auch eine gewisse Verantwortung zuzumuten. Ein höchstrichterliches Urteil bliebe also abzuwarten.

- 13 Den meisten Studenten fiel es schwer, das Verhältnis von unbegrenzter Haftung im Außenverhältnis und begrenzter Haftung in Innenverhältnis zu begreifen. Sie wollten die Grundsätze der gefährgeneigten Arbeit auch im Verhältnis zum Betroffenen anwenden.
- 14 Der Verfasser der Klausur bezieht sich hier auf einen Aufsatz von Marie-Theres Tinnefeld, Haftung des Arbeitnehmers bei betriebsbedingter Tätigkeit im EDV-Bereich, in: DuD 1992, 177 ff. Dieser Aufsatz war den Studenten während der Vorlesung als Pflichtlektüre angegeben worden. Der Verfasser geht im übrigen auf die Härteklausele nicht ein, was zu einem Punkteabzug führen mußte.
- 15 Die Formulierung ist natürlich ungeschickt; auch bei mittlerer Fahrlässigkeit steht dem Arbeitnehmer im Rahmen der vorzunehmenden Quotelung (der Verfasser spricht ungenau von Aufteilung) einen Freistellungsanspruch.

Allerdings versucht das BAG sowieso, auf das Element der Gefahrgeneigtheit der Arbeit zu verzichten und statt dessen jeden Arbeitnehmer in obigem Rahmen von der Haftung für Fehler zu befreien. Derzeit muß darüber der oberste Senat des Gerichts entscheiden.<sup>16</sup>

Als Ergänzung sei noch bemerkt, daß bei Bestellung eines *externen Datenschutzbeauftragten* (also zum Beispiel eines unabhängigen Rechtsanwaltes) der Begriff der gefahrgeneigten Arbeit nicht angewandt werden kann, da kein Arbeitsverhältnis besteht. Es fragt sich hier aber, ob die Bestellung externer Datenschutzbeauftragter wirklich sinnvoll ist. Rechtsanwälte sind meist in Sachen der Informatik und Betriebsorganisation unerfahren und daher allenfalls in Kleinbetrieben als Datenschutzbeauftragter einsetzbar.<sup>17</sup>

#### 4) Lösung von Frage 4:

Die *Einflußnahmemöglichkeiten* des Betriebsrats lassen sich generell aufteilen in Informations-, Beratungs- und Mitbestimmungsrechte. Die Aufgaben und Rechte des Betriebsrats sind im Betriebsverfassungsgesetz (BetrVG) geregelt.

§ 80 BetrVG<sup>18</sup> sieht vor, daß der Betriebsrat die Einhaltung der zum Schutz des AN geltenden Gesetze überwacht. Ein solches Gesetz stellt das BDSG dar. Dabei kann der Betriebsrat zwecks Durchführung dieser Aufgabe verlangen, vom Arbeitgeber unterrichtet zu werden<sup>19</sup> und alle wichtigen Unterlagen zu erhalten.

16 Der Verfasser meint den Großen Senat des BAG. – In der Zwischenzeit hat sich auch der Große Senat für einen Verzicht auf die Voraussetzung der Gefahrgeneigtheit ausgesprochen (Beschluß vom 12. Juni 1992 – GS I/89). Da der Senat aber damit von der Rechtsprechung des BGH abweichen würde, hat er die Rechtsfrage dem Gemeinsamen Senat der Obersten Gerichtshöfe des Bundes zur Entscheidung vorgelegt.

17 Diese Ansicht ist sicherlich höchst streitig, vgl. auch die Ausführungen von Helfrich in seinem Beitrag „Der Anwalt als externer Datenschutzbeauftragter“, S. 106 ff. in diesem Band. Daß der Student aber (ohne daß darüber in der Übung gesprochen worden wäre) auf diese Argumente kommt, ist natürlich löblich.

18 Genauer: § 80 I Nr. 1.

19 Die Formulierung ist nicht ganz ungefährlich. Sie suggeriert, daß der Arbeitgeber nur auf besondere Anforderung des Betriebsrats tätig werden muß. Statt dessen hat der Arbeitgeber aber von sich aus den Betriebsrat zu unterrichten (arg. ex § 80 II 2). – Den Studenten ist allerdings zugute zu halten, daß ihnen während der Klausur kein Text des BetrVG zur Verfügung stand.

§ 90 BetrVG verpflichtet die Unternehmensleitung, den Betriebsrat u.a. von der Planung neuer technischer Anlagen zu unterrichten. Nach Rechtsprechung des BAG ist hierunter auch und insbesondere die Einführung von neuer Software auf schon bestehender oder neuer Hardware zu verstehen. Der Betriebsrat hat hier also in jedem Fall ein Informationsrecht.<sup>20</sup>

Gemäß § 87 I Nr. 6 BetrVG kann der Betriebsrat bei der Einführung und Anwendung technischer Einrichtungen mitbestimmen, die dazu bestimmt sind, das Verhalten oder die Leistung eines Arbeitnehmers zu überwachen.<sup>21</sup>

a) *Einführung und Anwendung* impliziert auch jeweils Einführung oder Anwendung, wobei die nackte Einführung von Software ohne die Absicht der Anwendung eine eher akademische Fragestellung ist.

b) *Technische Einrichtungen* sind Softwareprodukte nach herrschender Meinung in jedem Fall.<sup>22</sup>

c) „Dazu bestimmt ... zu überwachen“ können diese Einrichtungen auch sein, wenn der Arbeitgeber gar nicht die Absicht hat, die Überwachung auch vorzunehmen. Das BAG stellt hier auf den objektiven Überwachungsbegriff ab. Dabei genügt es, wenn Daten ermittelt werden, deren Auswertung allein oder unter Zuhilfenahme externer Daten Aussagen über Verhalten oder Leistung ermöglichen würde. Ob diese Auswertung regelmäßig, in Einzelfällen oder gar nicht stattfindet oder vorgesehen ist, ist ohne Belang.

Wichtig ist in diesem Zusammenhang allerdings das vom BAG aufgestellte Erfordernis der *Unmittelbarkeit*: Die Einrichtung muß bereits in ihrem Kern unmittelbar zur Überwachung geeignet sein. Eine Anlage, die nur Daten auswerten kann, fällt nicht unter § 87. Später hat das BAG dieses Merkmal unter Hinweis auf das Persönlichkeitsrecht des Arbeitnehmers wieder aufgegeben. Dadurch ist die Rechts-

20 Der Verfasser der Klausur übersieht, daß § 90 BetrVG auch ein Beratungsrecht des Betriebsrates vorsieht. Im übrigen bezieht sich § 90 neben den technischen Anlagen auch auf die Planung von Arbeitsverfahren und Arbeitsabläufen.

21 Die Studenten haben sich im Vorfeld mit § 87 I Nr. 6 BetrVG insbesondere dadurch beschäftigt, daß sie einen Aufsatz von Michael Kort, EDV und betriebsverfassungsrechtliche Mitbestimmung, CR 1987, 300 ff. gelesen und miteinander diskutiert haben.

22 Das ist sehr knapp; hier wären weitere Erläuterungen durchaus sinnvoll gewesen.

lage bei § 87 sehr unklar und schwammig geworden; es ist damit zu rechnen, daß fast jede Anlage, die Verhaltens- oder Leistungsdaten von Arbeitnehmern erheben, speichern oder auswerten kann, unter das Mitbestimmungsrecht des Betriebsrats fällt.

d) Verhalten oder Leistung eines AN

Zu beachten ist, daß es um Daten gehen muß, die einem einzelnen Arbeitnehmer *zugeordnet* werden können. Gruppenverhalten oder Gruppenleistung ist nicht geschützt (anderer Ansicht aber neuerdings das BAG wegen des Überwachungsdrucks). Das BAG achtet aber streng darauf, daß bei der Einteilung in Gruppen jede (!) Gruppe größer als 2 Personen ist, da sonst bei Kenntnis der Daten des ersten Rückschlüsse auf den zweiten möglich wären.<sup>23</sup> Eine abteilungsweise Datenerfassung wäre also mitbestimmungspflichtig, wenn es Ein- oder Zwei-Mann/Frau-Abteilungen gäbe.

Wie sich Verhalten und Leistung zueinander verhalten, ist streitig („Verhalten“ als Oberbegriff?); der Streit hierüber ist aber letztlich akademisch und ohne praktische Relevanz. Verhalten ist ein willensgestütztes Tun. Darunter fallen also nicht unbewußte Gestik und Mimik, körperliche Gebrechen, Sprachfehler o.ä.

Nach *neuerer Rechtsprechung* stellt aber krankheitsbedingtes Fehlen ein Verhalten dar, weil unabhängig von dem objektiven Krankheits-tatbestand das Kommen oder Fehlen einen Willensakt darstellt. Diese Argumentation ist gefährlich: Hier schützt sie den Arbeitnehmer. An anderer Stelle gefährdet sie den Arbeitnehmer, da sie „Krankfeiern“ und „Drückebergertum“ sowie „streberhaftes Verhalten“ suggeriert.<sup>24</sup>

Nicht zu Verhalten oder Leistung zählen allgemeine Statusdaten (Name, Anschrift, Familienstand).<sup>25</sup>

23 Natürlich „achtet“ nicht das BAG auf die Größe einer Gruppe; dies sollte der Arbeitgeber unter Berücksichtigung der BAG-Rechtsprechung tun.

24 Was der Verfasser der Klausur damit meint, ist mir nicht hinreichend klar geworden. Seine Ausführungen dürften wohl so zu verstehen sein, daß der Verfasser auf der einen Seite den Schutz des erkrankten Arbeitnehmers über § 87 BetrVG als positiv empfindet, andererseits aber die Gefahr einer Speicherbarkeit von Krankheitsdaten sieht. Auf jeden Fall ist der Versuch einer eigenen Argumentation auch dann lobenswert, wenn die Argumente nicht sehr deutlich und überzeugend wirken.

25 Der Klausur merkt man an diesem Punkt an, daß ihrem Verfasser die Zeit knapp wurde. So fehlen wichtige Differenzierungen zu § 87; auf §94 BetrVG geht der Verfasser nicht mehr ein.

## Stichwortverzeichnis

- Angestellte, leitende
  - Bestellung zum Datenschutzbeauftragten 43
  - Bestimmungskriterien 43
  - Datenschutzbeauftragter als leitender Angestellter 54
  - Notwendigkeit eigenen Entscheidungsspielraums 44
- Anlaßaufsicht
  - Verhältnis zwischen Datenschutzbeauftragtem und Aufsichtsbehörde 77
  - Aufsichtsbehörde und Beratungsfunktion 86
- Anstellung
  - des Datenschutzbeauftragten und zugrundeliegende Rechtsakte 38
  - des Datenschutzbeauftragten und Mitbestimmung des Betriebsrats 38
  - Unterschied zur Bestellung 38
- Arbeitnehmerdatenschutzgesetz
  - Haltung der Bundesregierung 28
  - Zusammenarbeitsgebot zwischen Datenschutzbeauftragten und Betriebsrat 28
- Aufsichtsbehörde
  - Abberufung des Datenschutzbeauftragten 33, 79, 87
  - Ahndung von Ordnungswidrigkeiten 81
  - Amtsaufsicht 77
  - Anlaßaufsicht 77
- Anordnungs- und Untersagungsbefugnisse 17, 79
- Aufgaben 77
- Ausweitung des Aufgabenbereiches 78
- Befugnisse nach der EG-Datenschutzrichtlinie 17
- Beratungs- und Informationstätigkeit 80, 85
- Beratungsfunktion und Anlaßaufsicht 86
- Bestreiten der wirksamen Bestellung des Datenschutzbeauftragten 88
- EG-Datenschutzrichtlinie 17
- Eingriffsbefugnis 17
- Nationale Vorbilder 18
- Registerführung 21, 80
- Registrar des Data Protection Act 1984 als Vorbild 18
- Schlichtungsfunktion 85
- Unabhängigkeit 17
- Unterstützungsfunktion 85
- Untersuchungsbefugnis 17
- Verhängung von Bußgeldern 7, 81
- Verhältnis zum Datenschutzbeauftragten 85, 86
- Ausbildung des Datenschutzbeauftragten
  - Anforderungsprofil 11
  - Ausbildungsangebote 145, 156
  - Ausbildungswege 12
  - Mängel 11
  - Musterklausur 160