



SCHLESWIG-HOLSTEINISCHER LANDTAG

10. Wahlperiode

Drucksache 10/791

20. 12. 84

Anlage zur Drucksache 10/791

## Bericht

der Landesregierung

Datenschutzkontrolle in der Wirtschaft

Landtagsbeschluß vom 22. November 1983

Drucksache 10/163

Bericht

der Landesregierung Schleswig-Holstein

über den

Datenschutz in der Wirtschaft

Federführend ist der Innenminister

QQD 10/791

1

Inhaltsverzeichnis

	<u>Seite</u>
Vorbemerkungen	7
1. Beurteilung der vom Bundesdatenschutzgesetz festgeschriebenen Form der staatlichen Aufsicht über die personenbezogene Datenverarbeitung in der Wirtschaft	8
1.1 Organisation der Datenschutzaufsicht in Schleswig-Holstein	10
1.2 Personal- und Sachmitteleinsatz	11
1.3 Bisheriges Überwachungs- und Prüfungsvolumen	11
2. Gegenstand und Zielrichtung von Beschwerden der Bürger	15
2.1 Schwerpunkte der Eingaben und Beschwerden	15
2.1.1 Lösungsverlangen gegenüber Auskunftsteilen	15
2.1.2 Adressenhandel - eine Ursache für die Belästigung durch Werbesendungen	17
2.1.3 Lösungsverlangen unmittelbar nach Beendigung von Vertragsverhältnissen	19
2.1.4 Vertragsklauseln über allgemeine Einwilligungen und die Entbindung von der ärztlichen Schweigepflicht	20
2.1.5 Einschaltung privater ärztlicher Verrechnungsstellen	21
2.1.6 Bedrängung durch Inkassobüros	23
2.1.7 Datenaustausch zwischen Versicherungen	24
2.1.8 Sperrung von Daten, wenn ihre Richtigkeit bestritten wird	26

	<u>Seite</u>
2.1.9 Veröffentlichung personenbezogener Daten in Mitgliederlisten, beruflichen Verzeichnissen usw.	27
2.1.10 Ausgestaltung von Personalfragebogen	28
2.1.11 Ausforschung der finanziellen Verhältnisse leitender Angestellter	29
2.1.12 Rechtfertigung der Bankauskünfte durch Ergänzung der allgemeinen Geschäftsbedingungen der Kreditwirtschaft	30
2.2 Auswirkungen der Eingaben und Beschwerden	32
2.3 Weitergehende Wünsche und Erwartungen der Betroffenen	33
3. Ergebnisse der Kontrolltätigkeit der Datenschutzaufsichtsbehörde	35
3.1 Organisatorische Gestaltung der Kontrolltätigkeit	35
3.2 Schwerpunkte der Prüfungsmaßnahmen	37
3.2.1 Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung in Service-Rechenzentren	38
3.2.1.1 Produktionsfreigabe für EDV-Verfahren	40
3.2.1.2 Unterstützung durch die Betriebssysteme	42
3.2.1.3 Trennung zwischen Verfahrensentwicklung und Produktion	44
3.2.1.4 Abgrenzung der Kundendatenbestände untereinander	45
3.2.1.5 Realisierung der technischen und organisatorischen Sicherungsmaßnahmen nach § 6 BDSG	46

	<u>Seite</u>
3.2.2 Vertragsgestaltung der Service-Rechenzentren	53
3.2.2.1 Prüfungsansatz der Datenschutzaufsichtsbehörde	53
3.2.2.2 Ergebnis der Überprüfungen	54
3.2.2.3 Konsequenzen aus dem Prüfungsergebnis	56
3.2.3 Informationsgewinnung der Auskunftsteien	57
3.2.3.1 Besondere datenschutzrechtliche Regelungen	57
3.2.3.2 Vorbehalte der Betroffenen	58
3.2.3.3 Einfache und erweiterte Melde-registereinkünfte der Einwohnermeldeämter	59
3.2.3.4 Datenerhebungen bei den Betroffenen selbst und in ihrem Umfeld	60
3.2.4 Die Informationsverarbeitung der Auskunftsteien - Ergebnisse der Einzelprüfungen	62
3.2.4.1 Art der Darstellung der Prüfungsergebnisse	62
3.2.4.2 Arbeitsweise der Auskunftsteien	62
3.2.4.3 Datenschutzrechtliche Beurteilung der Rechtsverhältnisse	64
3.2.4.4 Rechtmäßigkeit der Datenspeicherungen	67
3.2.4.5 Benachrichtigung der Betroffenen, Erteilung von Auskünften über gespeicherte Daten	70
3.2.4.6 Prüfung des berechtigten Interesses der Informationsempfänger	70
3.2.4.7 Berichtigung, Sperrung und Löschung von Daten	71

	<u>Seite</u>
3.3 Zusammenfassende Darstellung der Ergebnisse der bisherigen Prüfungen der Datenschutzaufsichtsbehörde	73
3.4 Zusammenarbeit mit den betrieblichen Datenschutzbeauftragten	74
3.5 Problembereich bei der Durchsetzung datenschutzrechtlicher Ansprüche	76
3.6 Methodische und inhaltliche Auswirkungen der neuen Technologien auf die Prüfungspraxis der Datenschutzaufsichtsbehörde	78
4. Die Akzeptanz des Datenschutzes in der Wirtschaft	81
4.1 Anfängliche Vorbehalte	81
4.2 Abbau der Konfliktsituationen	82
4.3 Mittler-Funktion der Datenschutzaufsichtsbehörde	84
5. Zusammenarbeit zwischen den Datenschutzaufsichtsbehörden der Länder	85
5.1 Entstehung und Funktion des "Düsseldorfer Kreises"	85
5.2 Beispiele für besondere Koordinierungsbemühungen des Düsseldorfer Kreises	86
5.2.1 Verwaltungsvorschriften zum Bundesdatenschutzgesetz	86
5.2.2 Bundeseinheitliche Vereinbarungen mit der SCHUFA-Organisation	87
5.2.3 Klärung datenschutzrechtlicher Fragen mit der Versicherungswirtschaft	89
5.2.4 Einschränkung der Nachbarschaftsbefragungen durch die Auskunftsteien	91
5.3 Weitere Formen der Zusammenarbeit	91

	<u>Seite</u>
6. Möglichkeiten zur Verbesserung des Datenschutzes	92
6.1 Novellierung des Bundesdatenschutzgesetzes	92
6.2 Änderung der Organisationsform der Datenschutzaufsichtsbehörde	96
6.3 Anregungen der Wirtschaft und der Gewerkschaften	97
7. Erkenntnisse über Versuche zur Einführung von Personalinformationssystemen	98
7.1 Datenschutz im Arbeitsverhältnis	98
7.2 Definition der Personalinformationssysteme	100
7.3 Die datenschutzrechtliche Problematik der Personalinformationssysteme	103
8. Individuelle und kollektive Kontrollrechte bei der Einführung und Nutzung von Personalinformationssystemen	108
8.1 Welche Benachrichtigungspflichten obliegen dem Arbeitgeber, welche Einsichtsrechte hat der Arbeitnehmer?	109
8.2 Unter welchen Voraussetzungen kann ein Arbeitnehmer die ihn betreffenden Daten berichtigen, sperren oder löschen lassen?	110
8.3 Welche Mitbestimmungsrechte des Betriebsrates gibt es im Bereich der Verarbeitung von Arbeitnehmerdaten, bei der Einführung von Informationssystemen, bei der Bestellung des betrieblichen Datenschutzbeauftragten?	111

### Vorbemerkungen

Der Schleswig-Holsteinische Landtag hat die Landesregierung mit Beschluß vom 22. November 1983 (Drs.: 10/163) aufgefordert, ihm einen Bericht über die Datenschutzkontrolle in der Wirtschaft vorzulegen und dabei insbesondere auf die in der Beschlußempfehlung des Innen- und Rechtsausschusses vom 8. November 1983 aufgeführten Fragen einzugehen.

Die Landesregierung begrüßt die Möglichkeit, ausführlich und umfassend die Situation des Datenschutzes im nicht-öffentlichen Bereich darstellen zu können. Im Gegensatz zum öffentlichen Bereich, der der jährlichen parlamentarischen Berichterstattung durch den Landesbeauftragten für den Datenschutz unterliegt, erfahren die in der Wirtschaft anfallenden Datenschutzprobleme in der Regel eine geringere Publizität, haben aber gleichwohl erhebliche Auswirkungen für die Bürger und die Unternehmen.

Gegenstand der Berichterstattung ist die Beratungs- und Kontrolltätigkeit der Aufsichtsbehörde für den Datenschutz. Die Behörde hat zum 1. Januar 1978 ihre Tätigkeit aufgenommen. Der Bericht erfaßt ihre Tätigkeit bis Ende 1983.

1. Beurteilung der vom Bundesdatenschutzgesetz festgeschriebenen Form der staatlichen Aufsicht über die personenbezogene Datenverarbeitung in der Wirtschaft

Die Ausgestaltung der staatlichen Aufsicht über die personenbezogene Datenverarbeitung in der Wirtschaft war ein im Verlaufe des Gesetzgebungsverfahrens zum Bundesdatenschutzgesetz (BDSG) ausführlich diskutiertes Thema. Zwar schrieb bereits der Regierungsentwurf die Einrichtung von Aufsichtsbehörden zur Überwachung der Stellen vor, die personenbezogene Daten für fremde Zwecke verarbeiten (Auskunfteien, Markt- und Meinungsforschungsinstitute, Rechenzentren); während der parlamentarischen Beratungen war es aber gleichwohl umstritten, ob neben der Selbstkontrolle der betroffenen Bürger und der Tätigkeit der betrieblichen Datenschutzbeauftragten ganz allgemein noch eine staatliche Aufsicht erforderlich sei. Der Regierungsentwurf sah ein solches Kontrollorgan zumindest für die zahlenmäßig ungleich größere Gruppe der Unternehmen, die Daten für eigene Zwecke verarbeiten (Industrie, Handel, Banken, Versicherungen usw.) nicht vor.

Nicht nur die Wirtschaft stimmte dieser Entscheidung des Regierungsentwurfs zu, da ein Bedürfnis für Aufsichtsbehörden bei der Datenverarbeitung für eigene Zwecke nicht erkennbar sei, sondern auch die Länder machten Bedenken gegen eine Ausweitung der Zuständigkeiten der Aufsichtsbehörden vor allem wegen der Schwierigkeiten und Belastungen geltend, die mit der Einrichtung solcher Behörden verbunden wären, da

qualifiziertes Personal und ausreichende Sachmittel bereitgestellt werden müßten.

Der Gesetzgeber ist dieser Argumentation letztendlich nicht gefolgt. In den Beratungen des Bundestags-Innenausschusses und des Vermittlungsausschusses wurde das Prinzip der "abgestuften Selbstkontrolle" so ausgestaltet, daß einerseits die "Fremdkontrolle" durch staatliche Aufsichtsbehörden wesentlicher Bestandteil des Datenschutzes wurde, daß aber, je nachdem welche Ziele die speichernden Stellen mit der Verarbeitung der personenbezogenen Daten verfolgten, die Aufsicht von Amts wegen bzw. aufgrund begründeter Beschwerden der Betroffenen erfolgte (vgl. hierzu Bundestags-Drucks. 7/1027, 7/5277, 7/5497, 7/5568).

Bereits vor Inkrafttreten des BDSG, als also noch gar keine praktischen Erfahrungen vorlagen, aber auch danach ist diese Regelung heftig kritisiert worden. Je nach dem Standpunkt des Kritikers (Vertreter der speichernden Stellen oder Sachwalter der Interessen der Bürger) wurde entweder von einem "ungerechtfertigten Eingriff in die unternehmerischen Freiheiten", von einem "weiteren Schritt zum Staatsdirigismus" aber auch von einer "faktisch wirkungslosen Feigenblattfunktion" gesprochen.

In den nachfolgenden Ausführungen dieses Berichts (vgl. insbesondere Textziffern 2 und 3) wird dargelegt werden, daß beide Befürchtungen durch die tatsächliche Wirkungsweise der schleswig-holsteinischen Aufsichtsbehörde für den Datenschutz ausgeräumt werden konnten. Seitens

der Landesregierung kann festgestellt werden, daß sich - mit gewissen Einschränkungen im Detail - die staatliche Datenschutzaufsicht gut bewährt hat. Sie befindet sich derzeit in einem gut ausgewogenen Verhältnis zwischen den Belangen der betroffenen Bürger, den finanziellen und organisatorischen Belastungen der speichernden Stellen und dem Personal- und Sachmitteleinsatz in der Datenschutzaufsichtsbehörde.

#### 1.1 Organisation der Datenschutzaufsicht in Schleswig-Holstein

Das BDSG schreibt für die Aufsichtsbehörden für den Datenschutz keine besondere Organisationsform vor. § 30 Abs. 5 i. V. m. § 40 Abs. 2 BDSG legen lediglich fest, daß die Landesregierungen die für die Überwachung der Durchführung des Datenschutzes zuständigen Behörden bestimmen. Die schleswig-holsteinische Landesregierung hat durch Verordnung vom 20. Dezember 1977 den Innenminister als Aufsichtsbehörde benannt. Der Innenminister seinerseits hat durch Bekanntmachung vom 20. Juli 1978 den Landesbeauftragten für den Datenschutz mit der Wahrnehmung dieser Aufgabe betraut.

Vergleichbare Zusammenführungen von staatlicher Datenschutzkontrolle im öffentlichen und privaten Bereich finden sich im Saarland, in Hamburg und Bremen. Für dieses Modell sprechen insbesondere die Möglichkeiten des effektiven und damit kostengünstigen Personal- und Sachmitteleinsatzes (vgl. auch Tz. 6.2).

1.2 Personal- und Sachmitteleinsatz

Das Personal und die Sachmittel, die dem Landesbeauftragten für die Kontrollaufgaben zur Verfügung stehen, werden etwa gleichgewichtig für die Überwachungstätigkeit im privaten und im öffentlichen Bereich eingesetzt.

Personell war die Dienststelle in den Jahren 1978 bis 1983 wie folgt ausgestattet:

Landesbeauftragter	1
Vertreter	1
Sachbearbeitung	3
Vorzimmer	1
Registratur	1

Im Jahr 1984 erfolgt eine Personalerweiterung um einen Referenten und einen Sachbearbeiter.

Die Haushaltsmittel für die aufsichtsbehördliche Tätigkeit werden aus dem Kapitel des Innenministers bestritten. Die dem Datenschutzbeauftragten zur Verfügung stehenden Mittel für Bücher und Zeitschriften, Herausgabe von Informationen, Fortbildung, Sachverständige und Reisekosten in Höhe von z. Z. insgesamt 25 600 DM werden dabei mit herangezogen.

1.3 Bisheriges Überwachungs- und Prüfungsvolumen

Die Tätigkeit der Aufsichtsbehörde läßt sich ihrer Art nach gliedern in:

- Bearbeitung von Eingaben (vgl. Ziffer 2)
- Prüfungstätigkeit (vgl. Ziffer 3)

- Beratungstätigkeit (vgl. Ziffer 4)
- mittelbare Aufgaben, wie z. B. Erfahrungsaustausch (vgl. Ziffer 5).

Gemäß § 40 i. V. m. §§ 31 ff. BDSG übt die Aufsichtsbehörde ihre Kontrolltätigkeit von Amts wegen über Unternehmen aus, die geschäftsmäßig Daten für fremde Zwecke verarbeiten. In diesen Bereich fällt insbesondere die Überwachung der Wirtschafts- und Handelsauskunfteien, der Markt- und Meinungsforschungsinstitute und der Service-Rechenzentren. Die Aufsichtsbehörde hat im Lande ca. 180 derartige Betriebe von Amts wegen zu überprüfen. Über alle liegen bei der Aufsichtsbehörde Informationen vor, da sie gem. § 39 BDSG meldepflichtig sind. Die Aufsichtsbehörde führt ein öffentliches Register, das insbesondere Auskunft gibt über Geschäftszwecke, Form und Inhalt der personenbezogenen Datenverarbeitung. Entsprechend der datenschutzrechtlichen Bedeutung der Datenverarbeitung in diesen Unternehmen für den Betroffenen sind die Prüfungsschwerpunkte gesetzt worden (vgl. Ziffer 3). So hat es sich als erforderlich erwiesen, einige Betriebe einer mehrtägigen Prüfung zu unterziehen. Das gilt insbesondere für Firmen, die mit mehreren Niederlassungen in Schleswig-Holstein vertreten sind, wie z. B. die Handels- und Wirtschaftsauskunfteien. Hier konnte nämlich erwartet werden, daß die Ergebnisse einer ausführlichen Prüfung einer Zweigstelle auch in den anderen Zweigstellen ihren Niederschlag finden würden. Es hat daneben mehrere Prüfungen im schriftlichen Verfahren gegeben. Hier ist bei zufriedenstellenden Auskünften zunächst von weiteren Prüfungsmaßnahmen vor Ort abgesehen worden.

Das bisherige Prüfungsvolumen im Bereich der Kontrolle von Amts wegen stellt sich wie folgt dar:

1980 18 Prüfungen  
1981 3 Prüfungen, davon 1 Großprüfung  
1982 17 Prüfungen, davon 3 Großprüfungen  
1983 1 Großprüfung

Damit sind bis Ende 1983 ca. 20 % der registrierten speichernden Stellen in Prüfungsverfahren der Aufsichtsbehörde einbezogen worden. Stellt man allerdings auf die datenschutzrechtliche Bedeutung der Unternehmen ab, so sind faktisch alle wesentlichen Bereiche durch Prüfungsmaßnahmen erfaßt. Lediglich die in Schleswig-Holstein tätigen Auskunftsstellen der Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA) sind noch nicht einer umfassenden Prüfung unterzogen worden. Eine Betriebsumstellung des Unternehmens auf Datenverarbeitung machte eine zeitliche Verschiebung sinnvoll. Insgesamt ist jedoch die Tätigkeit der SCHUFA nicht ohne Datenschutzaufsicht geblieben (vgl. Ziffer 5).

Im weitaus größten Teil der privatwirtschaftlichen Verarbeitung personenbezogener Daten wird die staatliche Datenschutzaufsicht nur dann tätig, wenn ein Bürger sich mit einer konkreten Beschwerde an die Aufsichtsbehörde wendet. Diese sog. Anlaßaufsicht erstreckt sich gem. § 30 BDSG auf Unternehmen, die Daten für eigene Zwecke verarbeiten (z. B. die Daten ihrer Kunden, Lieferanten und Mitarbeiter). In der Bearbeitung dieser Eingaben liegt ein Schwerpunkt der Tätigkeit der Aufsichtsbehörde. Häufig können die An-

fragen und Beschwerden durch fernmündliche oder schriftliche Kontakte mit den Betrieben und insbesondere deren betrieblichen Datenschutzbeauftragten erledigt werden. Gelegentlich sieht die Aufsichtsbehörde sich aber veranlaßt, den Fall vor Ort zu klären. Es ist nicht möglich, das konkrete Prüfungsvolumen in diesem Bereich zu beziffern.

2. Gegenstand und Zielrichtung von Beschwerden der Bürger

2.1 Schwerpunkte der Eingaben und Beschwerden

Durch die Darstellung einiger exemplarischer Sachverhalte sollen die Schwerpunkte der Bürgerangaben in den letzten Jahren dargestellt werden. Die aufgeführten Fälle repräsentieren ca. 50 % aller an die Datenschutzaufsichtsbehörde gerichteten Anfragen und Beschwerden. Die übrigen Eingaben lassen sich thematisch nicht zu Gruppen zusammenfassen und haben im übrigen auch keine grundsätzlichen datenschutzrechtlichen Wirkungen entfaltet. Ihre Darstellung würde den Umfang des Berichts übersteigen bzw. dessen Zweck nicht gerecht werden.

Die Reihenfolge der Darstellung stellt keine Gewichtung dar, sondern reflektiert die zeitliche Aufeinanderfolge der Schwerpunkte der Eingaben.

2.1.1 Löschungsverlangen gegenüber Auskunftsteilen

Die durch § 34 BDSG vorgeschriebene Benachrichtigung der Betroffenen über die Tatsache der Speicherung von Daten bei den Auskunftsteilen führte in den ersten Monaten nach dem Inkrafttreten des BDSG zu einer Vielzahl von Eingaben. Viele Petenten waren der Annahme, daß die Datenschutzaufsichtsbehörde den Auskunftsteilen gegenüber ein Weisungsrecht habe. So wurde neben den Fragen nach dem Informanten der Auskunftsteil und nach dem Datenempfänger sehr häufig auch der Antrag gestellt, sie möge die Löschung der gespeicherten

Daten veranlassen, weil die Betroffenen "nichts mit einer Auskunft zu tun haben wollten und allein die Tatsache der Speicherung die schutzwürdigen Belange beeinträchtigt".

Die Datenschutzaufsichtsbehörde konnte zwar in einigen begründeten Fällen wegen rechtlicher Mängel bei der Datenerhebung, wegen des Überschreitens der maximalen Speicherdauer von fünf Jahren oder der objektiven Unrichtigkeit der Daten eine Sperrung bzw. Löschung der Daten erwirken. In der überwiegenden Zahl der Fälle bedurfte es aber der Aufklärung der Betroffenen über die tatsächliche Funktion der Datenschutzaufsichtsbehörde und des Hinweises, daß das BDSG einen allgemeinen Lösungsanspruch gegenüber Auskunftgebern nicht geschaffen hat und daß der Handel mit Informationen über Unternehmen und Privatpersonen zwar gewissen Beschränkungen unterworfen, nicht aber grundsätzlich verboten ist.

Nicht selten stießen diese Erläuterungen auf völliges Unverständnis der Bürger, und es wurde die Frage gestellt, wozu der Datenschutz dann geschaffen worden sei, wenn nicht dazu, "Schnüffelei in Privatsachen" zu verhindern. Offenbar als Ergebnis der bundesweiten Aufklärungsarbeit der Aufsichtsbehörden der Länder ist die Anzahl derartiger Eingaben in den letzten Jahren zurückgegangen. Wegen der Problematik der Beschaffung von Informationen durch die Auskunftgeber und der Ergebnisse der diesbezüglichen Prüfungsmaßnahmen der Datenschutzaufsichtsbehörde wird auf Tz. 3.2.3 verwiesen.

2.1.2 Adressenhandel - eine Ursache für die Belästigung durch Werbesendungen

Bereits vor Inkrafttreten des BDSG fühlten sich Bürger durch die Flut der Werbesendungen, die sie täglich in ihren Briefkästen vorfanden, belästigt. Aber erst nach Aufnahme ihrer Tätigkeit fand sich in der Datenschutzaufsichtsbehörde die Stelle, der gegenüber der Betroffene seine Verärgerung und rechtlichen Vorbehalte artikulieren konnte. Vor diesem Hintergrund ist der zweite große Komplex der Bürgereingaben in der Anfangszeit der Datenschutzpraxis zu sehen.

Es mag dahinstehen, ob die unaufgeforderte Zusendung von Angeboten, Waren- und Dienstleistungsanpreisungen usw. ein rechtlich relevanter Eingriff in die Persönlichkeitssphäre des einzelnen ist oder ob nicht das soziale Gemeinschaftsleben als eine wesentliche Grundlage unseres Staatsgefüges auch derartige Formen der Kommunikation impliziert. Das Transparenzgebot des BDSG hat jedenfalls dazu geführt, daß den Bürgern bekannt wurde, daß die Adressen der Werbesendungen "nicht nur willkürlich aus den Telefonbüchern abgeschrieben" worden waren, sondern daß in vielen Fällen ihre Geschäftspartner das Adressenmaterial (teilweise nach ganz konkreten Kriterien aufbereitet) gegen Entgelt anderen Unternehmen zur Verfügung gestellt hatten.

Die Nachprüfungen der Datenschutzaufsichtsbehörde aufgrund der Eingaben hatten sehr unterschiedliche Ergebnisse. Sie reichten von der Aufdeckung, daß Mitarbeiter von Firmen deren Kundenunterlagen ohne Wissen der Firmenleitung

systematisch daraufhin analysieren, ob sie für ein "befreundetes" Unternehmen von Interesse sein könnten, bis hin zu der Feststellung, daß z. B. ein katholischer Kindergarten nur deshalb Kataloge über Artikel für Ehehygiene zugesandt bekam, weil jemand entsprechende Anforderungscoupons aus einer Illustrierten unter Verwendung falscher Namen ausgefüllt hatte. Es zeigte sich aber auch, daß bestimmte Praktiken, die von der Bevölkerung als besonders verwerflich angesehen werden, datenschutzrechtlich nicht faßbar sind: Z. B. war einem Heiratsinstitut, das einer Witwe bereits vier Wochen nach dem Tode des Ehegatten seine Dienste anbot, ein Verstoß gegen das BDSG nicht nachzuweisen, weil es die Anschriften der Betroffenen den Todesanzeigen in der Zeitung entnommen hatte und sie im übrigen nicht in Dateien speicherte.

Die durch Eingaben der Bürger veranlaßten Aktivitäten der Datenschutzaufsichtsbehörde haben aber gerade in diesem Bereich positive Auswirkungen gehabt. So sind z. B. Unternehmen von sich aus an die schleswig-holsteinische Datenschutzaufsichtsbehörde mit der Bitte um Beratung herangetreten. Sie suchten nach einem datenschutzgerechten Weg, auf der einen Seite nicht auf die (in der Preiskalkulation berücksichtigten) Einnahmen aus der Adreßvermietung verzichten zu müssen, auf der anderen Seite jedoch die schutzwürdigen Belange der Betroffenen nicht zu beeinträchtigen. Es konnte ein durchaus praktikabler Weg gefunden werden, indem der Betroffene über die Umstände der Adreßweitergabe aufgeklärt und ihm der Widerspruch gegen eine weitere Verwendung der Anschriften zugestanden wurde.

Von wesentlicher datenschutzrechtlicher Bedeutung erscheint auch das offenbar geänderte Verhältnis der Adressenvermittler zum Datenschutzrecht. Die sogenannte Robinson-Liste ist ein Verzeichnis, in das sich jeder eintragen lassen kann, der keine Werbesendungen zu erhalten wünscht. Dieses Verzeichnis wird von dem Allgemeinen Direktwerbe- und Direktmarketing-Verband in Wiesbaden, einem Zusammenschluß der Adreßvermittler, geführt und maschinell mit den jeweils verwendeten Adreßdatenbeständen verglichen. Es galt früher als "Geheimtip". Heute scheinen die Adreßvermittler durchaus ein Interesse daran zu haben, möglichst viele Anschriften von Bürgern auszusondern, die nicht an einer geschäftlichen Beziehung mit werbenden Unternehmen interessiert sind. Dies hängt offenbar damit zusammen, daß den werbenden Unternehmen eine gewisse Rücklaufquote garantiert wird, die um so eher erreicht wird, je mehr "wertlose" Adressen vorher ausgesteuert worden sind.

### 2.1.3 Löschungsverlangen unmittelbar nach Beendigung von Vertragsverhältnissen

Nicht jedes Vertragsverhältnis, jede Mitgliedschaft in Vereinen usw. wird im gegenseitigen Einvernehmen beendet. Deshalb treten relativ häufig Vertragspartner mit der Bitte an die Datenschutzaufsichtsbehörde heran, dafür zu sorgen, daß ihre Daten "unverzüglich gelöscht würden, weil man mit der betreffenden Firma bzw. Vereinigung nichts mehr zu tun haben wolle". Nicht selten wurde der ganz allgemeine Verdacht geäußert, man traue dem ehemaligen Vertragspartner einen Mißbrauch der Daten zu.

Die Datenschutzaufsichtsbehörde mußte die deshalb oft enttäuschten Bürger darauf verweisen, daß in diesen Fällen zwar unter bestimmten Voraussetzungen ein Sperrungs-, nicht aber ein genereller Lösungsanspruch besteht. Die speichernden Stellen dürfen die Daten noch zu steuerlichen und handelsrechtlichen Nachweiszwecken aufbewahren, eine anderweitige Nutzung ist jedoch untersagt. In vielen Fällen war es der Datenschutzaufsichtsbehörde allerdings nicht möglich, das Mißtrauen abzubauen, das die Betroffenen gegenüber den betreffenden speichernden Stellen hegten, weil die Petenten davon ausgingen, daß Daten, solange sie verfügbar seien, u. U. auch mißbräuchlich genutzt werden (wegen der Problematik der Sperrung vgl. auch Tz. 3.5).

#### 2.1.4 Vertragsklauseln über allgemeine Einwilligungen und die Entbindung von der ärztlichen Schweigepflicht

Ein für die Betroffenen besonders schwierig zu durchschauender Komplex sind die Fragen nach der Form, dem Inhalt, dem Zweck und der Rechtswirksamkeit von Vertragsklauseln über allgemeine Einwilligungen in Versicherungs- und Kreditverträgen und insbesondere die damit verbundene Entbindung der Ärzte von der Schweigepflicht. Mit dieser Materie haben sich zwar die obersten Datenschutzaufsichtsbehörden der Länder im sogenannten Düsseldorfer Kreis eingehend beschäftigt und konstruktiv an der Gestaltung der an sich positiv zu beurteilenden sogenannten SCHUFA- und Versicherungs-Klauseln mitgewirkt (vgl. Tz. 5). Es beklagten sich aber viele Bürger, daß sie faktisch gezwungen wären, derartige Klauseln zu

unterschreiben, da sie andernfalls den gewünschten Kredit bzw. den Versicherungsschutz nicht erhielten. Alle Kreditinstitute und Versicherungsunternehmen hätten diese Klauseln in ihre Verträge aufgenommen und es gäbe somit keine Alternative am Markt.

Die Datenschutzaufsichtsbehörde konnte zwar nicht bewirken, daß in den betreffenden Fällen ein Vertragsverhältnis zustande kam, wenn der Betroffene besagte Vertragsbestandteile gestrichen hatte. Wenn aber schon die von den Kreditinstituten und Versicherungen als notwendig erachtete Risikominimierung (deren Ergebnis sich nach Aussagen der betreffenden Unternehmen für alle Kredit- und Versicherungsnehmer in günstigeren Kreditzinsen und Versicherungsprämien niederschlägt) in dieser Weise nicht zu vermeiden ist, so sollte nach ihrer Auffassung verstärkt darauf geachtet werden, daß die Klauseln inhaltlich so abgefaßt sind, daß sie für den Betroffenen ein Höchstmaß an Transparenz bringen. Die neuere Rechtsprechung und das sich ändernde datenschutzrechtliche Selbstverständnis sind daher der Anlaß, daß die derzeitigen Klauseln im Düsseldorfer Kreis noch einmal kritisch überdacht werden (vgl. zu dieser Problematik auch Tz. 2.1.7 und Tz. 2.1.12).

#### 2.1.5 Einschaltung privater ärztlicher Verrechnungsstellen

Ein Problem, dessen datenschutzrechtliche Dimension erst auf den zweiten Blick erkennbar wird, ist die allgemein übliche Einschaltung privater Verrechnungs- und Inkassostellen, wenn Ärzte

ihre Patienten nicht auf der Grundlage eines Krankenscheins (entsprechend den Bestimmungen der Reichsversicherungsordnung), sondern gegen Rechnung behandeln. Während sich die Zulässigkeit der Übermittlung der Abrechnungsdaten vom behandelnden Arzt an die Ortskrankenkassen oder Ersatzkassen aus der Tatsache ergibt, daß der Patient seinen Krankenschein vorgelegt hat und damit den Arzt beauftragt, die Abrechnung auf der Grundlage der RVO zu vollziehen, geht nicht jeder Privatpatient davon aus, daß seine Daten an ein privatwirtschaftliches Rechenzentrum oder eine privatärztliche Verrechnungsstelle zum Zweck der Abrechnung und des Inkassos weitergegeben werden. Es hat zwar bisher keine Klagen darüber gegeben, daß bei diesen Stellen die Daten mißbräuchlich genutzt wurden, eine Reihe von Bürgern erhoben aber Bedenken dagegen, daß die Datenweitergabe ohne ihr Wissen erfolgte. Die Datenschutzaufsichtsbehörde hat insbesondere im Hinblick auf die Wahrung des Arztgeheimnisses, dessen Durchbrechung gemäß § 203 Strafgesetzbuch strafbewehrt ist, der Ärztekammer empfohlen, ihren Mitgliedern nahezu legen, in den Wartezimmern durch Aushänge o. ä. darauf aufmerksam zu machen, daß Privatpatienten eine Weitergabe bestimmter Daten an eine Verrechnungsstelle erwarten müßten und diesem Verfahren ggf. widersprechen könnten.

Ein grundsätzliches Problem, dem wegen des immer stärkeren Einsatzes der EDV-Technologie in der Medizin in der Zukunft besondere Beachtung gebührt, ist die Frage, unter welchen Voraussetzungen und in welchem Umfang Ärzte die Dienste fremder Dienstleistungsunternehmen (Rechenzen-

tren, externe Labore usw.) in Anspruch nehmen können, ohne das Arztgeheimnis zu durchbrechen. Die Datenschutzaufsichtsbehörde geht davon aus, daß weniger der Begriff des "ärztlichen Hilfspersonals" extensiv ausgelegt werden sollte, sondern daß vielmehr der Weg über die Aufklärung und die Einwilligung des Patienten zu beschreiben ist.

#### 2.1.6 Bedrängung durch Inkassobüros

Viele Gläubiger bedienen sich zur Einbringung fälliger Forderungen der Dienste privater Inkassobüros. Diese Unternehmen arbeiten in der Regel mit erfolgsabhängigen Honoraren bzw. sind aus geschäftspolitischen Gründen an einer hohen Erfolgsquote interessiert. Dementsprechend werden die Schuldner in den Mahnschreiben mehr oder minder drastisch mit den vermeintlichen Folgen des weiteren Zahlungsverzugs konfrontiert. Nicht selten wird dabei auch mit der Registrierung in speziellen "Schuldnerlisten" gedroht. Insbesondere Betroffene, die die Rechtmäßigkeit der dem Beitreibungsverfahren zugrunde liegenden Forderungen bestritten hatten, fühlten sich durch derartige Formulierungen bedrängt.

In einigen Fällen handelte es sich um Inkassobüros, die gleichzeitig auch eine Handelsauskunftei betreiben. Neben der unter Tz. 3.2.4.3 beschriebenen Problematik der Übernahme von Inkassodaten in den Auskunfteibestand ohne Wissen des Auftraggebers besteht hier die datenschutzrechtliche Forderung, daß bestrittene Beträge grundsätzlich nicht zu einer Registrierung im Auskunfteibestand führen dürfen. Dieser Grund-

satz wird von den größeren Auskunftsteiorganisationen beachtet, einige kleinere Unternehmen mußten jedoch auf diese Gegebenheiten nachdrücklich hingewiesen werden.

Bei anderen Unternehmen wurden entgegen den Ausführungen in den Mahnschreiben gar keine Schuldnerlisten geführt. Zwar wurden die Vorgänge eines Schuldners zusammengefaßt, wenn verschiedene Gläubiger das betreffende Inkassobüro mit der Einziehung der Forderungen beauftragt hatten. Auch wurden ältere Vorgänge beigezogen, wenn neue Inkassoaufträge zu der gleichen Person eingingen (Feststellung des Arbeitgebers usw.). Eine systematische dateimäßige Registrierung und vor allem eine Auskunftserteilung fand in diesen Fällen jedoch nicht statt.

Die Datenschutzaufsichtsbehörde hat - soweit es ihr trotz der zum Teil fehlenden Zuständigkeit (keine dateimäßige Verarbeitung) möglich war - versucht, die betreffenden Inkassobüros zu einer weniger "drastischen" Ausdrucksweise in ihren Formschriften zu bewegen. In einer Reihe von Fällen ist ihr dies gelungen, in anderen konnte sie die Petenten nur auf den Rechtsweg verweisen.

#### 2.1.7 Datenaustausch zwischen Versicherungen

Die Versicherungswirtschaft geht davon aus, daß neben den Datenübermittlungen, für die sie durch die Versicherungsnehmer eine besondere Einwilligung erhalten hat (vgl. Tz. 2.1.4), noch weitere, nicht im einzelnen den Betroffenen offenbar werdende Informationsströme insbesondere

innerhalb der Branche notwendig und auch datenschutzrechtlich zulässig sind. Sie leitet dieses Recht aus § 24 BDSG ab. Danach sind Datenübermittlungen u. a. dann gestattet, "soweit es zur Wahrung berechtigter Interessen der übermittelnden Stelle oder eines Dritten oder der Allgemeinheit erforderlich ist und dadurch schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden".

Auf dieser Basis werden z. B.

- den neu versichernden Versicherungsunternehmen Auskünfte erteilt über den Verlauf und die geltend gemachten Schadenshöhen zwischenzeitlich aufgelöster Versicherungsverträge,
- besonders hohe Lebensversicherungsverträge an eine zentrale Registrierstelle gemeldet,
- spezielle Malus-Dateien geführt,
- zur Abwehr von Versicherungsbetrug von den zentralen Registrierstellen der Versicherungswirtschaft Einzelangaben über abgeschlossene Versicherungsverträge undifferenziert an die angeschlossenen Unternehmen weitergegeben, weil das Verfahren der Einzelabrufe im Verdachtsfall zu aufwendig erscheint.

Unabhängig von der Frage, ob die eine oder andere Datenübermittlung durch die vom Versicherungsnehmer unterschriebene Einwilligungsklausel abgedeckt ist, stößt die "Geheimniskrämerei" (so die Einlassung eines Patenten) der Versicherungen bei den Bürgern auf großes Unverständnis.

Die Versicherungswirtschaft beruft sich stets auf ihre berechtigten Interessen. Sie macht unter Hinweis auf die Offenbarungspflichten der Versicherungsnehmer nach dem Versicherungsvertragsgesetz sowie die strafrechtlichen Vorschriften über den Versicherungsbetrug geltend, daß die schutzwürdigen Belange der "ehrlichen Versicherungsnehmer" nicht durch Maßnahmen beeinträchtigt werden könnten, die der Aufdeckung betrügerischer Manipulationen dienen. Letztendlich werde dadurch Schaden von der gesamten Versichertengemeinschaft abgewendet.

Die Datenschutzaufsichtsbehörde hat Zweifel, ob von den Versicherungen in der Vergangenheit wirklich alle Möglichkeiten ausgeschöpft worden sind, den Versicherungsnehmern die Absichten und Verfahrensweisen der Versicherungen transparent zu machen. In Anbetracht der Tatsache, daß z. Z. bundesweit mehrere Gerichtsverfahren zu dieser Thematik anhängig sind, hat sie bis jetzt allerdings darauf verzichtet, konkrete Beanstandungen auszusprechen.

2.1.8 Sperrung von Daten, wenn ihre Richtigkeit bestritten wird

Das BDSG verpflichtet die speichernden Stellen, Daten über eine Person zu sperren, wenn ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt. Diese an sich sehr klare und für den Betroffenen sehr wichtige Bestimmung hat in der Praxis insbesondere im Hinblick auf die Verfahrensweise der Auskunftsteilen zu erheblichen Schwierigkeiten geführt.

In der Literatur besteht zwar Einvernehmen darüber, daß ein bloßes Bestreiten der Richtigkeit der Daten seitens der Betroffenen die speichernden Stellen noch nicht zu einer Sperrung verpflichtet. Es konnte aber der Versuch einiger Auskunftsteilen nicht akzeptiert werden, entsprechenden Anträgen der Bürger dadurch zu begegnen, daß man die Angabe der richtigen Daten forderte, um dann anstelle der Sperrung eine Berichtigung vorzunehmen.

Die Datenschutzaufsichtsbehörde hat die Verfahrensweise der betreffenden Auskunftsteilen beanstandet und sich als Vermittler eingeschaltet. Sie hat sich die gespeicherten und die richtigen Daten von der speichernden Stelle bzw. von den Betroffenen vorlegen lassen und quasi als Schiedsrichter darüber befunden, ob eine Sperrung erforderlich war. In nahezu allen Fällen haben die Beteiligten den Vorschlag der Datenschutzaufsichtsbehörde akzeptiert, wobei nicht immer die speichernde Stelle der "Verlierer" war. In mehreren Fällen war es die offenkundige Absicht der Betroffenen, über den Weg der Sperrung die betreffende Auskunftsteil daran zu hindern, negative, allerdings objektiv richtige Informationen an andere Stellen weiterzugeben.

2.1.9 Veröffentlichung personenbezogener Daten in Mitgliederlisten, berufsständischen Verzeichnissen usw.

Die Tatsache, daß das Datenschutzrecht als Ausfluß der grundgesetzlich garantierten Persönlichkeitsrechte der Bürger sehr stark auf die individuell zu interpretierenden schutzwürdigen

Belange abhebt, wurde in einer Reihe von Eingaben deutlich, die sich gegen die oft bereits seit Jahrzehnten gängige Praxis wandten, Vereinsmitglieder, Mitglieder von Berufsgruppen usw. in Verzeichnissen zusammenzufassen und diese zu veröffentlichen.

Nicht zu Unrecht machten die Betroffenen geltend, daß derartige Veröffentlichungen Ursache für Belästigungen durch Werbesendungen, Vertreterbesuche und telefonische Werbemaßnahmen seien. Inwieweit die Vereinssatzungen bzw. die Beschlüsse der zuständigen Organe der betreffenden Institutionen eine Art Bindungswirkung für die einzelnen Mitglieder entfalteten, mußte von der Datenschutzaufsichtsbehörde in jedem Einzelfall entschieden werden. Dies galt insbesondere dann, wenn die Mehrheit der Mitglieder der Gruppierung die Veröffentlichungen für richtig und zweckmäßig hielten (z. B. Eigenwerbung bestimmter Berufsgruppen).

Die Datenschutzaufsichtsbehörde hat die Probleme allerdings häufig durch einen Kompromiß lösen können. Es wurde in diesen Fällen ein Widerspruchsrecht zwischen den Beteiligten vereinbart.

#### 2.1.10 Ausgestaltung von Personalfragebogen

Im Zeichen eines immer enger werdenden Arbeitsmarktes kommt den Bewerbungsunterlagen eines Arbeitnehmers, der sich um einen neuen Arbeitsplatz bemüht, eine große Bedeutung zu. Obwohl davon auszugehen ist, daß jeder Bewerber um eine offene Stelle vom Grundsatz her bereit ist, um-

fassend über seine Person Auskunft zu geben, um seine Qualifikation deutlich werden zu lassen, scheint gerade in jüngster Zeit der Umfang der Datenerhebung einiger Personalstellen das vertretbare Maß überschritten zu haben. Es erreichten die Datenschutzaufsichtsbehörde immer wieder Anfragen von Bewerbern, ob bestimmte Fragen, die den privaten Bereich betrafen (familiäre Verhältnisse, Krankheiten, persönliche Gewohnheiten usw.) datenschutzrechtlich überhaupt zulässig seien und wozu die Daten benötigt würden.

Die datenschutzrechtliche Problematik der Aufnahme derartiger Informationen in Personalinformationssysteme ist unter Tz. 7 dargestellt. Zu der Frage, wo die rechtlichen Grenzen für eine Erhebung (ohne anschließende Speicherung in Dateien) persönlicher Daten im Rahmen von Arbeitsverhältnissen zu ziehen sind, mußte die Datenschutzaufsichtsbehörde wegen des begrenzten Anwendungsbereichs des BDSG auf das Arbeits- und Tarifrecht verweisen. Sie hat allerdings anlässlich der Kontakte zu Personalleitern, betrieblichen Datenschutzbeauftragten und Personalräten auf die ihr bekanntgewordenen Sorgen der Bewerber hingewiesen und zu einer gewissen kritischen Selbstbeschränkung bzw. zu mehr Transparenz den Bewerbern gegenüber aufgerufen.

#### 2.1.11 Ausforschung der finanziellen Verhältnisse leitender Angestellter

Die unter Tz. 2.1.10 beschriebene Problematik korrespondiert in mehrfacher Hinsicht mit den der Datenschutzaufsichtsbehörde wiederholt vortragenen Hinweisen, daß es in der Wirtschaft

üblich sei, über (zukünftige) leitende Angestellte durch Mithilfe "befreundeter" Banken bzw. deren Mitarbeiter SCHUFA-Auskünfte einzuholen.

Es ist rechtlich zwar nicht zu beanstanden, Referenzen einzuholen. Grundsätzliche datenschutzrechtliche Bedenken sind aber zu erheben, wenn die "Clearing-Stelle" des Kreditgewerbes entgegen ihrer eigentlichen Aufgabenstellung auch für Personalentscheidungen herangezogen wird. Es ist dabei zu beachten, daß die sogenannte SCHUFA-Klausel (vgl. Tz. 5.2.2) nur einen eng begrenzten Verwendungszweck der Daten abdeckt (Absicherung eines kreditorischen Risikos). Die Datenschutzaufsichtsbehörde hat allerdings bisher in keinem Fall, in dem ihr Verdachtsmomente vorgebracht worden sind, ein konkretes Fehlverhalten nachweisen können. Die Frage, ob dies an der von den Betroffenen behaupteten geschickten Verschleierung des Verfahrens liegt oder ob tatsächlich derartige Anfragen nicht gestellt werden, muß offenbleiben.

#### 2.1.12 Rechtfertigung der Bankauskünfte durch Ergänzung der allgemeinen Geschäftsbedingungen der Kreditwirtschaft

Im Jahr 1983 hat die Absicht der Kreditwirtschaft, die sogenannten Bankauskünfte durch Ergänzung der allgemeinen Geschäftsbedingungen auf eine vertragsmäßige Grundlage zu stellen, zu erheblichen Protesten in der Öffentlichkeit geführt. Die Bürger waren sehr verunsichert, als sie durch kurze Hinweise ihrer Kreditinstitute ersucht wurden, sich mit einer Änderung der all-

gemeinen Geschäftsbedingungen einverstanden zu erklären. Erst auf diese Weise erfuhren sie, daß ein ihnen bis dahin unbekannter Informationsaustausch innerhalb der Kreditwirtschaft über die Zahlungsgewohnheiten und das "Kreditgebaren" der Kunden besteht. Es war ihnen insbesondere unverständlich, warum sie in bezug auf den Datenaustausch über die SCHUFA eine besondere Klausel (Einwilligung) zu unterschreiben hatten, während die internen Informationsströme der Kreditwirtschaft "versteckt" in den allgemeinen Geschäftsbedingungen ihre Legitimation finden sollten.

Den öffentlichen Datenschutzbeauftragten und den Datenschutzaufsichtsbehörden der Länder ist es gemeinsam gelungen, die Kreditwirtschaft von der datenschutzrechtlichen Problematik dieser Vorgehensweise zu überzeugen. Es wurden von der Kreditwirtschaft folgende Grundsätze akzeptiert:

- Die Kreditinstitute sind berechtigt, über Geschäftskunden (juristische Personen und Kaufleute) Bankauskünfte zu erteilen, sofern ihnen keine anderslautenden Weisungen der Kunden vorliegen.
- Bankauskünfte über Privatkunden erteilen die Kreditinstitute nur dann, wenn diese allgemein oder im Einzelfall ausdrücklich zugestimmt haben.
- Bankauskünfte umfassen nur allgemein gehaltene Feststellungen und Bewertungen über die wirtschaftlichen Verhältnisse der Kunden, ihre Kreditwürdigkeit und Zahlungsfähigkeit; betragsmäßige Angaben über Kontostände, Spargut-

haben, Depot- oder sonstige dem Kreditinstitut anvertraute Vermögenswerte sowie Kreditansprüche werden nicht gemacht.

- Bankauskünfte erhalten nur eigene Kunden sowie andere Kreditinstitute zu deren eigenen Zwecken und die ihrer Kunden; sie werden nur dann erteilt, wenn der Anfragende ein berechtigtes Interesse an der gewünschten Auskunft glaubhaft darlegt.

Ergänzend hierzu werden die Bankkunden zur besseren Information künftig zusätzlich durch ein Informationsblatt "Kundeninformation Bankauskunftsverfahren" über den Inhalt der vorgenannten Regeln unterrichtet.

## 2.2 Auswirkungen der Eingaben und Beschwerden

Die Bürgereingaben und Beschwerden haben zweifellos Auswirkungen auf die Verfahrensweise der speichernden Stellen bei der personenbezogenen Datenverarbeitung gehabt. Zunächst einmal ging von ihnen durch die entsprechenden Aktivitäten der Datenschutzaufsichtsbehörde eine Signalwirkung aus. Unternehmen, die sich aufgrund der Beschwerden von Betroffenen gegenüber einer staatlichen Stelle rechtfertigen mußten und ggf. auch zugeben mußten, daß im Einzelfall rechtliche oder tatsächliche Mängel bestanden, waren bemüht, Wiederholungsfälle zu vermeiden.

Einige bedenkliche Verfahrensweisen und Praktiken einiger speichernder Stellen sind den Betroffenen nur durch eine Verkettung günstiger Umstände bekanntgeworden (Schreibfehler in An-

schriften, die den Nachweis des Adressenhandels erbrachten usw.). Das Überraschungsmoment, das dadurch entstand, daß die Datenschutzaufsichtsbehörde plötzlich an sich "internen" Vorgängen nachging, führte nicht selten zu Peinlichkeiten, deren zukünftige Vermeidung den betreffenden Unternehmen ein Anliegen sein mußte. Dies um so mehr, als die Betroffenen als Ergebnis der Kontrollmaßnahmen der Datenschutzaufsichtsbehörde von ihr eine Schilderung des tatsächlichen Sachverhalts erhalten.

Nicht zuletzt aber auch die offene Diskussion der datenschutzrechtlichen Fragen mit der "neutralen" Datenschutzaufsichtsbehörde, die in einigen Fällen auch überzogene Forderungen der Betroffenen auf das rechtlich vorgegebene Niveau zurückführen mußte, hat - wie die Beispiele unter Tz. 2.1 zeigen - dazu geführt, daß eine Reihe von Problembereichen für die Zukunft als gelöst angesehen werden kann.

### 2.3 Weitergehende Wünsche und Erwartungen der Betroffenen

Wie sich allerdings aus einigen der unter Tz. 2.1 dargestellten Fälle ergibt, ist den Bürgern in der Praxis häufig nur sehr schwer zu erklären, warum das Datenschutzrecht (und damit die Zuständigkeit der Datenschutzaufsichtsbehörde) so eng an die Verarbeitung von personenbezogenen Daten in Dateien anknüpft. Insbesondere bei gleichgelagerten Sachverhalten, die sich nur dadurch unterscheiden, daß in einem Fall auf der Basis konventioneller Akten und in dem anderen Fall unter Zuhilfenahme einer EDV-Anlage gear-

beitet wird, empfinden die Bürger ihre Rechte als nicht hinreichend geschützt, wenn sie von den speichernden Stellen mit einem Hinweis auf die Rechtslage (keine Datenverarbeitung in Dateien) abgewiesen werden. Dies gilt z. B. für die häufiger kritisierten Detekteien und Inkasobüros, die auch gegenüber der Datenschutzaufsichtsbehörde geltend machen, daß sie mit ihrer aktenmäßigen Informationsverarbeitung nicht den Bestimmungen des BDSG unterworfen sind.

Ähnlich verhält es sich mit den sogenannten internen Dateien im Sinne des § 1 Abs. 2 Satz 2 BDSG. Dabei handelt es sich nicht selten um "schwarze Listen", die zwar dem Gesetz entsprechend gut gesichert sind (§ 6 BDSG), deren Inhalt und Funktion jedoch weder der Betroffene noch die Datenschutzaufsichtsbehörde im einzelnen überprüfen kann. In einem derartigen Fall wurde der Datenschutzaufsichtsbehörde ganz offen dargelegt, daß eine solche Kartei nur deshalb nicht automatisiert geführt werde, um sie den einschlägigen datenschutzrechtlichen Bestimmungen zu entziehen.

In diesem Zusammenhang wären außerdem die Komplexe "Information über Datenquellen und Datenempfänger" und "genereller Lösungsanspruch gegenüber Auskunftsteilen" vgl. Tz. 2.1.1) zu nennen. In Anfragen in derartigen Fällen konnte die Datenschutzaufsichtsbehörde die Betroffenen nur auf die derzeitige Rechtslage und auf die beabsichtigte Novellierung des Bundesdatenschutzgesetzes verweisen.

3. Ergebnisse der Kontrolltätigkeit der Datenschutzaufsichtsbehörde

3.1 Organisatorische Gestaltung der Kontrolltätigkeit

Neben der unter Tz. 2 beschriebenen Bearbeitung von Bürgereingaben stellt die systematische Kontrolle der speichernden Stellen eine der Hauptaufgaben der Datenschutzaufsichtsbehörde dar. Das in den sechs Jahren ihres Bestehens bewältigte Prüfungsvolumen ist unter Tz. 1 beschrieben. Mit der Durchführung der Prüfungsmaßnahmen sind die gleichen Mitarbeiter betraut, die auch im unmittelbaren Zuständigkeitsbereich des Landesbeauftragten für den Datenschutz die Überprüfung der Behörden vornehmen. So ist auch die Methodik und die organisatorische Gestaltung der Prüfungen in beiden Bereichen weitgehend identisch.

In der Regel werden die Unternehmen zunächst schriftlich über den Zeitpunkt und den Prüfungsgegenstand informiert. Ihnen wird dadurch Gelegenheit gegeben, die erforderlichen Unterlagen bereitzuhalten und die zuständigen Mitarbeiter zur Auskunftserteilung freizustellen. Daneben ist es in Einzelfällen erforderlich, eine Nachschau auch ohne Vorankündigung vorzunehmen. Bei einigen Prüfungen waren der betreffenden Geschäftsleitung vorher zwar der Zeitpunkt, nicht aber die zu erörternden datenschutzrechtlichen Fragestellungen bekanntgegeben worden. Die beiden letztgenannten Vorgehensweisen sind angezeigt, wenn sich der Verdacht datenschutzrechtlichen Fehlverhaltens gegen die Geschäftsleitung selbst oder einzelne Mitarbeiter des Unternehmens richtet.

Umfangreichere Prüfungsmaßnahmen enden stets mit einer Schlußbesprechung, an der neben dem Prüfungsbeamten auch der zuständige Referent der Datenschutzaufsichtsbehörde oder sein Vertreter teilnimmt. Außerdem wird stets ein schriftlicher Prüfungsbericht erstellt, der die Rechtsauffassungen der Datenschutzaufsichtsbehörde zu den beanstandeten Sachverhalten darlegt.

Die Prüfungsmaßnahmen selbst stützen sich auf die Rechte, die der Datenschutzaufsichtsbehörde nach § 30 BDSG zustehen. Es sind dies im einzelnen:

- die Befugnis, Grundstücke und Geschäftsräume zu betreten (das Grundrecht der Unverletzlichkeit der Wohnung aus Artikel 13 Grundgesetz ist insoweit eingeschränkt),
- die Möglichkeit zur Besichtigung und Prüfung der örtlichen Gegebenheiten,
- das Recht zur Einsichtnahme in die geschäftlichen Unterlagen, Datenübersichten, gespeicherten Daten und Datenverarbeitungsprogramme,
- das Recht auf mündliche Auskünfte der Inhaber und Mitarbeiter der geprüften Stellen.

Die eingesetzten Beamten benutzen für ihre praktische Arbeit eine Checkliste, die von ihnen im Laufe der Jahre erarbeitet wurde und die aufgrund der zwischenzeitlich gewonnenen Erfahrungen, der neuen Rechtsprechung und der geänderten systemtechnischen Bedingungen regelmäßig vervollständigt wird. Dies gewährleistet eine

gleichmäßige und gleichartige Verfahrensweise und Beurteilung bei allen geprüften Stellen. Es ist seitens der Wirtschaft häufig der Wunsch geäußert worden, daß diese Checklisten veröffentlicht werden, damit die speichernden Stellen Anhaltspunkte für die Ausgestaltung ihrer Datenschutzmaßnahmen gewinnen könnten. Dieses mußte abgelehnt werden, weil die Effizienz einer Überwachungsbehörde auch davon abhängt, daß die Vorgehensweise und der Wissensstand ihrer Beamten "nicht berechenbar" ist.

### 3.2 Schwerpunkte der Prüfungsmaßnahmen

Die Datenschutzaufsichtsbehörde ist nach § 40 BDSG verpflichtet,

- Markt- und Meinungsforschungsinstitute,
- Wirtschafts- und Handelsauskunfteien und
- Service-Rechenzentren

und ähnliche Unternehmen im Hinblick auf die Einhaltung der datenschutzrechtlichen Pflichten "von Amts wegen" zu kontrollieren. Diese Überprüfungspflicht korrespondiert mit einer Meldepflicht der betreffenden Unternehmen nach § 39 BDSG. Die Datenschutzaufsichtsbehörde ist also darüber informiert, wo die zu kontrollierenden Unternehmen ihren Sitz haben, in welcher Form dort personenbezogene Daten verarbeitet werden und wer in den Unternehmen die Verantwortung für die Beachtung der Datenschutzvorschriften trägt. Außerdem ist der Name des betrieblichen Datenschutzbeauftragten bekannt.

Aufgrund einer Analyse der Gesamtheit der vorliegenden Meldungen wurden folgende Schwerpunkte der Kontrolltätigkeit festgelegt:

- Überwachung der Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung in einzelnen Service-Rechenzentren,
- allgemeine Überprüfung der Vertragsgestaltung der Service-Rechenzentren,
- allgemeine Untersuchung der Informationsgewinnung der Auskunftsteilen,
- umfassende Kontrollen bei einzelnen Zweigstellen der Auskunftsteilen.

### 3.2.1 Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung in Service-Rechenzentren

Die Datenschutzgesetze gestatten den Unternehmen der Wirtschaft (ebenso wie den Behörden im öffentlichen Bereich), ihre Geschäftsdaten auch "außer Haus" durch Service-Rechenzentren verarbeiten zu lassen. Dieses Recht bedeutet umgekehrt für die Betroffenen (Kunden, Lieferanten und Mitarbeiter der betreffenden Unternehmen) eine Pflicht zur Duldung, daß ihre Daten unter Umständen sogar ohne ihr Wissen tatsächlich bei einem anderen Unternehmen gespeichert und verarbeitet werden als bei dem, mit dem sie in einem Vertragsverhältnis stehen. Die Zulässigkeit der Auftragsdatenverarbeitung ist deshalb vom Gesetzgeber an zwei Bedingungen geknüpft worden:

- Der Auftraggeber hat den Auftragnehmer (das Rechenzentrum) "unter besonderer Berücksichtigung der Eignung der getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen" (§ 22 Abs. 2 BDSG) und
- dem Auftragnehmer "ist die Verarbeitung der personenbezogenen Daten nur im Rahmen der Weisungen des Auftraggebers gestattet" (§ 37 BDSG).

Darüber hinaus kommt gerade bei Service-Rechenzentren dem betrieblichen Datenschutzbeauftragten eine besondere Bedeutung zu. Er hat nach § 38 i. V. m. § 29 BDSG "die ordnungsgemäße Anwendung der Datenverarbeitungs-Programme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen".

Für die datenschutzrechtlichen Überprüfungen ergeben sich hieraus folgende Grundfragen:

- Ist das Rechenzentrum tatsächlich auch in der Lage, die gegenüber dem Auftraggeber eingegangenen Verpflichtungen zu erfüllen?
- Sind die im Auftrag durchgeführten maschinellen Verarbeitungsvorgänge hinreichend abgesichert?
- Sind die Datenbestände der einzelnen Kunden des Rechenzentrums so gegeneinander abgegrenzt, daß nicht einem Kunden die Daten des anderen Kunden verfügbar werden?
- Bleibt der Auftraggeber trotz der Einschaltung eines Rechenzentrums "Herr seiner Daten"?

- Ist er in der Lage, nachzuvollziehen, was mit seinen Daten außerhalb seiner unmittelbaren Einflußsphäre geschieht?
- Nimmt der Auftraggeber seine Weisungsbefugnisse (im Sinne einer Kontrollverpflichtung) wirklich wahr?
- Ist die Schnittstelle zwischen den Verantwortungsbereichen des Auftraggebers und des Auftragnehmers exakt beschrieben?
- Ist der Betroffene evtl. schlechter gestellt, als bei einer unmittelbaren Verarbeitung seiner Daten beim Auftraggeber?

Im einzelnen hatten die Prüfungsmaßnahmen folgende Ergebnisse:

#### 3.2.1.1 Produktionsfreigabe für EDV-Verfahren

Bevor EDV-Programme erstmals praktisch eingesetzt werden, sind sie einer sehr genauen Testprozedur zu unterziehen, die mit einem Testlauf unter Produktionbedingungen abschließt. Diese Prüfung darf nicht durch den Programmierer erfolgen, sondern muß durch einen Dritten (Anwender, Kunde, Fachabteilung, Geschäftsleitung) geschehen. Dabei kommt es insbesondere darauf an, fehlerhafte Datenausgaben und (noch wichtiger) fehlerhafte Datenspeicherungen zu erkennen und deren Ursachen abzustellen.

Erst danach darf ein Programm "zur Produktion freigegeben" werden. Jede Änderung eines Programmes muß prinzipiell eine Wiederholung der Testprozedur zur Folge haben.

Die vorgenannten, im Schrifttum zur automatisierten Datenverarbeitung allgemein anerkannten Grundsätze werden in der Praxis aus Zeit- und Kostengründen häufig nicht konsequent angewandt. Solange ein Unternehmer in seinem eigenen Betrieb ganz bewußt auf derartige Kontrollen verzichtet, mögen die Risiken überschaubar sein und durch geeignete "flankierende Maßnahmen" aufgefangen werden können. Wenn aber ein Unternehmen sich auf die Richtigkeit der maschinellen Ergebnisse, die von einem Service-Rechenzentrum geliefert werden, verläßt oder wenn das Rechenzentrum den Kunden in dem Glauben läßt, daß die Programme sorgfältig ausgetestet sind, dann können fehlerhafte Programme unübersehbare Folgen haben, die unmittelbar in die schutzwürdigen Belange der betroffenen Bürger eingreifen. Dabei geht es nicht nur um schlechthin falsche Ergebnisse (falscher Kontostand, ungerechtfertigte Mahnungen usw.), sondern insbesondere auch um die Folgen betrügerischer Manipulationen.

Soweit in den Prüfungen Mängel in diesem Bereich festgestellt worden sind, wurden Beanstandungen ausgesprochen. Es war aus rechtlichen Gründen aber nicht möglich, die Kunden der Rechenzentren direkt anzusprechen und sie ggf. zu veranlassen, ihrerseits die von ihnen in Anspruch genommenen Verfahren genauer zu testen, weil diese Unternehmen nur der Anlaßaufsicht nach § 30 BDSG unterliegen.

### 3.2.1.2 Unterstützung durch die Betriebssysteme

Betriebssysteme sind Programmpakete, die von den Herstellern der EDV-Anlagen geliefert werden. Sie stellen eine logische Verknüpfung her zwischen der an sich "toten" Technik (Hardware) und den automatisierten Verfahren des Benutzers (Software). Die Betriebssysteme übernehmen die innere Verwaltung einer EDV-Anlage. Sie steuern die sichere und ordnungsmäßige Durchführung der automatisierten Verfahren. Schwächen im Betriebssystem können durch organisatorische Maßnahmen des Benutzers nur sehr schwer ausgeglichen werden. Enthält ein solches System aber gezielte Kontroll- und Überwachungsprozeduren, so sind diese in der Regel selbst für Systemprogrammierer, Operatoren usw. nicht zu umgehen (innerster Sicherheitsring).

Im Rahmen von Prüfungen gestaltete sich die Schwachstellenanalyse in diesem Bereich sehr schwierig. Es war im allgemeinen nicht einfach, mit den Rechenzentrums-Leitern offen über die objektiv gegebenen Manipulations- und Betrugsmöglichkeiten der einzelnen Mitarbeiter zu sprechen ("Welches ist der größtmögliche Schaden, den ein bestimmter Mitarbeiter unter den gegebenen Voraussetzungen anrichten kann?"). Zum anderen wurde häufig versucht, erkannte Schwachstellen mit der Bemerkung zu entschuldigen: "Das geht bei dem eingesetzten System nicht besser, das ist Stand der Technik". Dieses Argument war oft tatsächlich kaum zu widerlegen, weil die Hersteller ihre Programme in der Vergangenheit mehr nach Leistungs- als nach Sicherheitskriterien ausgelegt haben.

Ein typisches Problem kann anhand eines Beispiels beschrieben werden: In mehreren Rechenzentren wurde festgestellt und beanstandet, daß bestimmte Mitarbeiter Programmänderungen vornehmen konnten, ohne daß dieser Vorgang einer Zwangsdokumentation unterlag. Diese Tatsache eröffnete zumindest theoretisch die Möglichkeit zu weitreichenden betrügerischen Manipulationen, etwa in folgender Weise: Ein Programm wird in Betrugsabsicht geändert, daraufhin erzeugt es unrichtige (fingierte) Datenbestände, anschließend wird das Programm wieder in den ursprünglichen Zustand zurückgeändert, fortan werden die manipulierten Daten als richtig angesehen und als Ausgangswert für alle weiteren Verarbeitungsschritte benutzt. Selbst nach einer Entdeckung des Betruges wären Rekonstruktionen und Rückschlüsse auf den betreffenden Mitarbeiter nicht möglich. Abhilfe hätte allerdings sehr leicht durch eine vom Betriebssystem gesteuerte, nicht zu umgehende Registrierung und Aufzeichnung aller Programmänderungen geschaffen werden können. Die eingesetzten Betriebssysteme sahen eine solche Maßnahme jedoch nicht vor. Die betreffenden Rechenzentren konnten von der Datenschutzaufsichtsbehörde aus Gründen der Verhältnismäßigkeit nicht gezwungen werden, die EDV-Anlagen und die Betriebssysteme durch neuere, finanziell aufwendigere Modelle bzw. Versionen zu ersetzen. So blieb nur der Weg, die Sicherheitslücken durch gezielte organisatorische Maßnahmen so gut wie möglich zu schließen.

Es ist daher das langfristige Ziel der Datenschutzaufsichtsbehörde, das Sicherheitsbewußtsein der EDV-Anwender so zu schärfen, daß sie als Kunden die Herstellerfirmen zu einer entsprechenden Neukonzeption der Betriebssysteme bewegen. Sie selbst führt hierüber seit geraumer Zeit Gespräche mit den betreffenden Unternehmen.

### 3.2.1.3 Trennung zwischen Verfahrensentwicklung und Produktion

Die Tätigkeit von Rechenzentren gliedert sich im allgemeinen in die Bereiche "Entwicklung von Verfahren" und "Produktion". Das bedeutet, daß häufig gleichzeitig auf einem Rechnersystem bereits freigegebene Programme "echte" Daten verarbeiten und Programmierer die in der Entwicklung befindlichen Programme testen. Nicht selten werden für diese Tests Original-Daten benutzt, weil es zu zeitaufwendig erscheint, "künstliche" Datenbestände zu erzeugen.

In mehrfacher Hinsicht sind derartige Verfahrensweisen, die in der Praxis immer wieder angetroffen werden, datenschutzrechtlich bedenklich und daher von der Datenschutzaufsichtsbehörde beanstandet worden.

- Ein Rechenzentrum, das fremde Daten verarbeitet, hat dafür Sorge zu tragen, daß sowenig Personen wie möglich von dem Inhalt der ihm anvertrauten Informationen Kenntnis erhalten. Allein schon dieser Aspekt erfordert eine strikte Trennung von Verfahrensentwicklung und Produktion.

- Wenn zugelassen wurde, Kunden-Daten auch außerhalb eines freigegebenen Verfahrens zu Testzwecken zu verarbeiten, war ein Sicherheitsniveau unterschritten, das nach allen Erfahrungen auch Unbefugten die Möglichkeit eröffnete, Datenbestände einzusehen und zu verändern.
  
- Ein zufällig herausgegriffener Kundendatenbestand enthält in der Regel nicht alle Fallvarianten, die durch das betreffende automatisierte Verfahren insgesamt abgedeckt werden sollen. Von einem wirksamen Test kann also kaum gesprochen werden. Es besteht also das Risiko, daß Programmfehler sich erst im Verlaufe des praktischen Einsatzes herausstellen bzw. deren Konsequenzen für längere Zeit unentdeckt bleiben.

#### 3.2.1.4 Abgrenzung der Kundendatenbestände untereinander

Gerade bei Service-Rechenzentren ist zu fordern, daß eine wirksame "Abschottung" der Kunden-Datenbestände untereinander gewährleistet ist. Von der Datenschutzaufsichtsbehörde wurde z. B. ein Fall beanstandet, in dem ein einzelner Kunde eines Rechenzentrums einen "privilegierten Status" besaß. Dieser Kunde war berechtigt, seine Programme selbst zu entwickeln und auf dem EDV-System zu testen (er nahm also nur die Rechnerleistung in Anspruch). Das Rechenzentrum selbst war nicht im Detail darüber informiert, welche Aktivitäten dieser Kunde auf dem Rechner vollzog. Ohne die von der Datenschutzaufsichtsbehörde geforderten zusätzlichen, sehr spezifischen systemtechnischen Maßnahmen wäre es möglich ge-

wesen, daß der Kunde bzw. dessen Mitarbeiter die Datenbestände der anderen Kunden zur Kenntnis nehmen konnte. In einem anderen Fall betrieben eine Behörde, ein kommunaler Eigenbetrieb und ein Wirtschaftsunternehmen gemeinsam ein Rechenzentrum. Auch hier war eine unbefugte Kenntnisnahme zwar vertraglich, nicht aber technisch ausgeschlossen. Neben technischen und finanziellen Überlegungen haben nicht zuletzt auch die Beanstandungen der Datenschutzaufsichtsbehörde dazu geführt, daß im gegenseitigen Einvernehmen aller Beteiligten das Rechenzentrum in dieser Form aufgelöst wurde.

In der Prüfungspraxis gestalten sich die datenschutzrechtlichen Erörterungen zu dieser Thematik sehr schwierig, weil die Sicherheitsaspekte (vorbeugendes Mißtrauen gegenüber einer potentiellen Vertragsverletzung oder einer kriminellen Tat) in Einklang gebracht werden müssen mit den unternehmenspolitischen und betriebswirtschaftlichen Überlegungen eines Rechenzentrums.

#### 3.2.1.5 Realisierung der technischen und organisatorischen Sicherungsmaßnahmen nach § 6 BDSG

Den Service-Rechenzentren, die aufgrund ihres spezifischen Geschäftszweckes keine eigenen, sondern ausschließlich fremde Daten verarbeiten, muß die Realisierung der technischen und organisatorischen Sicherungsmaßnahmen nach § 6 BDSG ein zentrales Anliegen sein. Im Hinblick darauf hat der Gesetzgeber in der Anlage zu § 6 BDSG einen Anforderungskatalog festgeschrieben, der zehn verschiedene Sicherungsbereiche umfaßt:

- Zugangskontrolle
- Abgangskontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Übermittlungskontrolle
- Eingabekontrolle
- Auftragskontrolle
- Transportkontrolle
- Organisationskontrolle

Es ist daher durch die Datenschutzaufsichtsbehörde zu prüfen, welche

- baulichen Maßnahmen,
- systemtechnischen Maßnahmen,
- programmtechnischen Maßnahmen und
- organisatorischen Maßnahmen

im einzelnen zu treffen sind. Dabei ist zu berücksichtigen, daß Datensicherungsmaßnahmen einerseits einen präventiven Charakter haben (eine Diebstahlssicherung ist auch dann zu installieren, wenn der Betreiber eines EDV-Systems subjektiv davon ausgeht, daß bei ihm nicht gestohlen wird), daß es andererseits aber keine hundertprozentige Sicherheit geben kann (die Risiken können mit vertretbarem Aufwand allenfalls soweit reduziert werden, daß die Wahrscheinlichkeit eines "Datenunfalls" gegen Null tendiert). Auch der Gesetzgeber hat dieses Spannungsfeld zwischen dem Wunsch nach einem Maximum an Sicherheit und dem betriebswirtschaftlich vorgegebenen Zwang zur Kostenminimierung gesehen. Er hat keinem der beiden Aspekte eine Priorität eingeräumt, sondern festgelegt, daß nur solche

Maßnahmen erforderlich sind, deren "Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen". Bei den Prüfungen der Datenschutzaufsichtsbehörde geht es also nicht nur um die Frage, ob die vorgefundenen Sicherungsmaßnahmen ausreichend sind, sondern auch darum, ob sich bessere Sicherungsmaßnahmen mit einem vertretbaren oder nur mit einem zu hohen Kostenaufwand einführen lassen.

Die Prüfungsergebnisse lassen sich in den einzelnen Gruppen wie folgt zusammenfassen:

- Bauliche Maßnahmen

Die räumliche Unterbringung der geprüften Rechenzentren und deren Schutz gegen Einbruch, Diebstahl, Feuer und sonstige Beeinträchtigungen von außen konnten im allgemeinen als ausreichend angesehen werden. Die Beurteilung der hinreichenden Absicherung eines Rechenzentrums gegen äußere Schadenseinflüsse stellt sich bei kleineren und mittleren Unternehmen im allgemeinen als relativ problemlos dar. Aber gerade bei größeren (publizitätsträchtigeren) Installationen ist es in jüngster Zeit bundesweit, aber auch in Schleswig-Holstein, zu gezielten Anschlägen mit kriminellem Hintergrund gekommen. Die Datenschutzaufsichtsbehörde hat daher in den Beratungsgesprächen immer wieder darauf hingewiesen, daß es zwar gegen Sprengstoffanschläge kaum einen wirksamen Schutz gibt, daß aber Rechenzentren, die unmittelbar an einer Straße liegen, die sich im Erdgeschoß eines Gebäudes befinden oder die durch die Anordnung der Fenster von außen einen Einblick ermöglichen (Verlockung zu grobem Unfug und Sach-

beschädigung), besonders gefährdet sind. Auch der Umstand, daß sich das Gefährdungspotential überproportional zur Größe eines Rechenzentrums erhöht, muß in der Wirksamkeit und Intensität der Abwehrmaßnahmen seinen Niederschlag finden. Weil grundlegende räumliche Veränderungen häufig nicht möglich waren, ist in den Prüfungen stets darauf gedrungen worden, daß zumindest eine Einsichtnahme von außen verhindert wurde und ein unkontrollierter Zugang nicht möglich war.

Da die Rechenzentren in der Regel in bereits bestehenden Gebäuden eingerichtet werden, bereitet die räumliche Trennung der einzelnen inneren Sicherheitsbereiche in der Praxis häufig größere Schwierigkeiten. Die Datenschutzaufsichtsbehörde hat dennoch stets mit Nachdruck gefordert, daß Funktionstrennungen, die aus Sicherheitsgründen erforderlich sind (z. B. Trennung zwischen Verfahrensentwicklung und Produktion), auch ihren Niederschlag in der baulichen Gestaltung eines Rechenzentrums finden müssen. In einem Fall wurde beanstandet, daß Anwendungsprogrammierern aus Platzmangel direkt im Systemraum ein Arbeitsplatz zugewiesen worden war. Mehrfach wurde die Situation angetroffen, daß die für nicht sachkundige Personen kaum zu entschlüsselnden elektronischen Datenspeicher (Magnetbänder, Magnetplatten) zwar in einem besonders gesicherten Archiv lagerten, daß aber die für jedermann lesbaren maschinellen Ergebnisse (Rechnungen, Mahnungen usw.) aufgrund der räumlichen Gegebenheiten auf Fluren und dergleichen zwischengelagert wurden.

- Systemtechnische Maßnahmen

Die systemtechnischen Datensicherungsmaßnahmen stehen in einem engen Zusammenhang mit den unter Tz. 3.2.1.2 beschriebenen Funktionen der Betriebssysteme. Die Prüfungen haben ergeben, daß in diesem Bereich noch ein gewisser Nachholbedarf besteht. Während im Bereich der Fertigung das Prinzip "Qualitätskontrolle" und im kaufmännischen Bereich Maßnahmen der "Revision" allgemein anerkannte betriebliche Funktionen sind, hat sich das Instrument der "EDV-Revision" noch nicht überall durchgesetzt. Die Datenschutzaufsichtsbehörde hat ihre diesbezüglichen Beanstandungen mit konstruktiven Vorschlägen zur Anhebung des Sicherheitsniveaus unterbreitet. Eine wesentliche Forderung in diesem Zusammenhang ist die Gewährleistung einer lückenlosen Dokumentation der Systemaktivitäten (Wann ist das System von wem für welche Aufgaben benutzt worden?) und eine zumindest stichprobenweise Überprüfung der Zulässigkeit der einzelnen Aktivitäten. Dazu gehört auch die Dokumentation und Rückverfolgung von abgewehrten Mißbrauchsversuchen. Die präventive Wirkung von Datensicherungsmaßnahmen kommt nach Auffassung der Datenschutzaufsichtsbehörde nur dann zum Tragen, wenn dem potentiellen "Eindringling" bekannt ist, daß verbotenes Tun zumindest zufällig, d. h., mit einer für ihn unkalkulierbaren Wahrscheinlichkeit, aufgedeckt wird.

- Programmtechnische Maßnahmen

Programmtechnische Datensicherungsmaßnahmen in Form sog. Plausibilitäten sind Bestandteile der einzelnen Datenverarbeitungs-Programme und analysieren die Aktivitäten eines System-Benutzers auf deren logische Schlüssigkeit. Zur Verhinderung sachlicher Eingabefehler, die zwangsläufig zu falschen Ergebnissen oder zum Abbruch der Verarbeitung führen, werden Plausibilitäten seit jeher sehr umfassend eingesetzt. Im Bereich der Datensicherung werden die Möglichkeiten nach den Erkenntnissen der Datenschutzaufsichtsbehörde aber noch nicht in dem wünschenswerten Umfang genutzt. Wie die Presseveröffentlichungen über die mangelhafte Absicherung von Datennetzen in den USA zeigen, handelt es sich hierbei nicht um ein spezifisches Problem schleswig-holsteinischer oder bundesdeutscher Rechenzentren. Die Datenschutzaufsichtsbehörde hat in ihren Prüfungen immer wieder darauf gedrungen, den eigenen Mitarbeitern bzw. den Mitarbeitern der Rechenzentrums-Kunden gegenüber ein gesundes Mißtrauen walten zu lassen. Es sollte nicht nur die allgemeine Legitimation zur Nutzung des Systems (z. B. durch ein Pass-Word oder eine Identitäts-Karte) geprüft werden. Auch die "innere Logik" von Datenverarbeitungs-Aktivitäten kann und muß einer Sicherheitsüberprüfung unterzogen werden (wenn entgegen der sonstigen Praxis zum drittenmal in kurzer Zeit eine Gehaltsliste der leitenden Mitarbeiter eines Rechenzentrums-Kunden abgerufen wird, sollte programmgesteuert auch dann eine Warnung erfolgen, wenn jedesmal

das richtige Pass-Word eingegeben wurde). Die Bedeutung derartiger Sicherungsmaßnahmen wird nach Auffassung der Datenschutzaufsichtsbehörde in den nächsten Jahren immer größer werden, weil durch den Einsatz von Bildschirmtext-Verfahren und anderen offenen Datenfernverarbeitungssystemen der Zugriff auf Datenverarbeitungs-Programme einem wesentlich größeren Personenkreis als bisher ermöglicht wird.

- Organisatorische Maßnahmen

Die Wirksamkeit organisatorischer Datensicherungsmaßnahmen (z. B. exakte Beschreibung der Befugnisse und Verantwortungsbereiche der einzelnen Mitarbeiter, Aufenthaltsverbote für bestimmte Mitarbeiter in Sicherheitsbereichen, Verbot der Mitnahme von Unterlagen aus den Sicherheitsbereichen, Registrierung und gesicherte Verwahrung von Datenträgern) hängt entscheidend davon ab, daß die Regelungen hinreichend bestimmt formuliert sind und daß ihre Einhaltung überwacht wird. In den meisten der überprüften Rechenzentren gab es zwar entsprechende Weisungen der Geschäftsleitung, häufig waren sie aber nicht schriftlich fixiert und außerdem fehlten oft auch wirksame Kontrollen. Es war im übrigen festzustellen, daß einige betriebliche Datenschutzbeauftragte ihre Überwachungsaufgaben und -befugnisse in diesem Bereich noch nicht erkannt hatten. In Einzelfällen mußte die Datenschutzaufsichtsbehörde auch die Geschäftsleitung davon überzeugen, daß eine wirksame Datensicherung bereits im organisatorischen Bereich beginnt.

### 3.2.2 Vertragsgestaltung der Service-Rechenzentren

#### 3.2.2.1 Prüfungsansatz der Datenschutzaufsichtsbehörde

Auf die Art und den Inhalt der Vertragsgestaltung zwischen Auftraggeber und Rechenzentrum kann die Datenschutzaufsichtsbehörde unmittelbar keinen Einfluß nehmen. Das BDSG schreibt für das Verfahren der Auswahl des Auftragnehmers und die Ausgestaltung der Weisungen des Auftraggebers keine besondere Form vor. Auch besteht keine Verpflichtung zur schriftlichen Fixierung der Vereinbarungen zwischen Auftraggeber und Auftragnehmer.

Auf der anderen Seite bedeutet die gesetzliche Verpflichtung, Daten nur im Rahmen der Weisungen des Auftraggebers zu verarbeiten (§ 37 BDSG), daß dem Rechenzentrum konkrete Weisungen des Auftraggebers vorliegen müssen. Sie müssen den Umfang und den Inhalt der Verarbeitung bestimmen, doch braucht nicht für jeden technischen Einzelschritt eine ausdrückliche Weisung vorzuliegen. Aus der Weisungsbindung folgt weiter, daß das Rechenzentrum den Weisungen nicht zuwiderhandeln darf. § 37 BDSG verlangt anders als § 665 BGB nicht denkenden, sondern strikten Gehorsam. Auch wenn das Rechenzentrum sich des Einverständnisses des Auftraggebers sicher glaubt, darf es daher nicht eigenmächtig handeln, sondern muß neue Weisungen einholen.

Die Datenschutzaufsichtsbehörde hatte also zu prüfen, ob die in der Praxis vorgefundenen vertraglichen Vereinbarungen geeignet erscheinen, diese gesetzlichen Anforderungen zu gewährleisten.

sten, ob also die in den Verträgen festgelegten Verfahrensweisen als hinreichend konkrete Weisungen an den Auftragnehmer angesehen werden können. Zu diesem Ziel wurden in einem schriftlichen Verfahren eine größere Anzahl von Rechenzentren aufgefordert, Art und Inhalt ihrer Verträge offenzulegen.

#### 3.2.2.2 Ergebnis der Überprüfungen

Die sehr unterschiedlichen Vertragsgestaltungen, mit denen die Datenschutzaufsichtsbehörde konfrontiert wurde, verhinderten einen unmittelbaren Vergleich und machten eine grundsätzliche datenschutzrechtliche Aufarbeitung erforderlich. Im Hinblick auf die Vielschichtigkeit des Gegenstandes der Rechtsverhältnisse, z. B.

- Erledigung von Datenerfassungsarbeiten,
- ausschließliche Bereitstellung von Rechnerleistung,
- Verarbeitung von Daten im Rahmen umfassender Hardware-, Software- und Orgware-Konzepte,
- individuelle Entwicklung und Implementierung komplexer automatisierter Verfahren,

ergaben sich in Einzelfällen Fragestellungen und Forderungen, die unter anderen Voraussetzungen wiederum an Relevanz verloren. Die Datenschutzaufsichtsbehörde hat deshalb unter Zugrundelegung aller vorgelegten Unterlagen eine allgemeingültige Schwachstellenanalyse erstellt und die betreffenden Rechenzentren ersucht, selbst zu prüfen, ob aus Rechtsgründen Verbesserungen in der Vertragsgestaltung erforderlich waren oder aus Gründen der Klarstellung und Transparenz sachdienlich sein konnten.

Den betreffenden Unternehmen wurde z. B. die stärkere Berücksichtigung folgender datenschutzrechtlicher Aspekte nahegelegt (Auszug aus einem mehr als 30 Punkte umfassenden Katalog):

- Exakte Beschreibung des Gegenstandes der Auftragsdatenverarbeitung; Klarstellung, daß ein Auftragsverhältnis vorliegt;
- genaue Beschreibung der Art und des Umfanges der zu erbringenden Leistungen;
- Vereinbarungen über das dem Auftragnehmer ggf. zugestandene Recht, zur Erbringung der Leistungen Dritte heranzuziehen; genaue Bezeichnung des tatsächlichen Speicherungs- und Verarbeitungsortes;
- Regelungen über die ordnungsgemäße Abwicklung im Fall der Beendigung des Vertragsverhältnisses; Beschreibung der Pflichten des Auftragnehmers, die über das Vertragsende hinausreichen;
- Vereinbarungen über die formalen datenschutzrechtlichen Pflichten des Auftragnehmers (Meldungen zum Register nach § 39 BDSG, Bestellung eines Datenschutzbeauftragten, Verpflichtung der Mitarbeiter auf das Datengeheimnis usw.);
- Definition der Kontrollrechte des Auftraggebers;
- Verpflichtung des Auftragnehmers, eine nachvollziehbare Dokumentation der automatisierten Verfahren zu erstellen und Verfahrensänderun-

gen nur mit Genehmigung des Auftraggebers durchzuführen;

- allgemeine und verfahrensspezifische Regelungen bezüglich des Informationsflusses zwischen Auftraggeber und Auftragnehmer;
- Vereinbarungen zur Ausgestaltung der Datensicherungsmaßnahmen beim Auftragnehmer.

### 3.2.2.3 Konsequenzen aus dem Prüfungsergebnis

Nicht alle der geprüften Unternehmen vermochten sich der Auffassung der Datenschutzaufsichtsbehörde anzuschließen, daß ihre bestehenden vertraglichen Vereinbarungen datenschutzrechtlich "verbesserungsfähig" seien. Die Datenschutzaufsichtsbehörde hat diesen Rechenzentren mitgeteilt, daß ihre Bedenken im Hinblick auf die ausschließlich weisungsabhängige Durchführung der Datenverarbeitung nicht ausgeräumt seien und sie zu gegebener Zeit im Rahmen von Einzelprüfungen nach § 40 BDSG die tatsächlichen Verhältnisse untersuchen werde.

Das Ergebnis der Überprüfungen ist in einem Arbeitspapier zusammengefaßt worden, das kostenlos an alle interessierten speichernden Stellen versandt wird. Dies ist in den einschlägigen Fachpublikationen bekanntgegeben worden.

### 3.2.3 Informationsgewinnung der Auskunftsteien

#### 3.2.3.1 Besondere datenschutzrechtliche Regelungen

Zusätzlich zu den allgemeinen Regelungen des BDSG für die personenbezogene Datenverarbeitung in der Wirtschaft gelten für Auskunftsteien besondere Bestimmungen (§§ 32 -35 BDSG). Diese sollen dem Umstand Rechnung tragen, daß es nach geltendem Recht privaten Stellen grundsätzlich nicht untersagt ist, Informationen über Bürger zu sammeln und sie gegen Entgelt an Dritte weiterzugeben.

Den folgenden im BDSG festgelegten Grundsätzen kommt daher eine wesentliche praktische Bedeutung zu:

- Es dürfen nur Daten gespeichert werden, soweit kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange der Betroffenen beeinträchtigt werden.
- Daten dürfen nur an solche Empfänger weitergegeben werden, die der Auskunftstei gegenüber ein berechtigtes Interesse glaubhaft dargelegt haben.
- Spätestens im Zusammenhang mit der erstmaligen Weitergabe von Daten muß der Betroffene über die Tatsache der Speicherung informiert werden.
- Die Daten sind spätestens fünf Jahre nach ihrer Einspeicherung zu sperren.

### 3.2.3.2 Vorbehalte der Betroffenen

Seitdem die Auskunftsteien durch die gesetzlich vorgeschriebenen Benachrichtigungs- und Auskunftsverpflichtungen den Bürgern die Tatsache der Speicherung und den Inhalt der gespeicherten Daten offenbaren müssen, sind gegen die in diesem Bereich gebräuchlichen Methoden der Informationsgewinnung immer wieder Bedenken erhoben worden. Die Vorbehalte der Betroffenen resultieren nach den Erfahrungen der Datenschutzaufsichtsbehörde nicht zuletzt auch daraus, daß der Gesetzgeber die Auskunftspflicht nur auf die tatsächlich in Dateien gespeicherten Daten begrenzt hat und den Bürgern somit die Informationsquellen und die Auftraggeber der Handelsauskunftsteien unbekannt bleiben. Die Betroffenen sind insoweit auf Mutmaßungen angewiesen. Wenn nun aber aus dem gespeicherten Datenbestand Rückschlüsse auf einen bestimmten Informanten (z. B. Nachbar, Vermieter oder Arbeitgeber) gezogen werden, ergibt sich häufig der Verdacht, daß weit mehr als die gespeicherten und für eine Auskunft vorgesehenen Daten (nämlich alle Informationen, von denen der Betroffene meint, daß der Informant sie kennt) preisgegeben worden sind, daß also die betreffende Auskunftstei nicht alle ihr bekannten Informationen mitgeteilt hat.

Dieses Mißtrauen den Auskunftsteien gegenüber drückte sich in einer Vielzahl mündlicher und schriftlicher Beratungersuchen und konkreten Beanstandungen der Bürger aus. Sie waren für die Datenschutzaufsichtsbehörde Anlaß, die Informationsgewinnung der Auskunftsteien bei öffentlichen Stellen (im wesentlichen bei den Einwohnermeldeämtern der Gemeinden und Städte) und bei privaten Quellen (in der Hauptsache Nachbarn und Vermietern) zu untersuchen.

### 3.2.3.3 Einfache und erweiterte Melderegisterauskünfte der Einwohnermeldeämter

Das Melderecht unterscheidet zwischen einfachen und erweiterten Melderegisterauskünften. Erstere umfassen lediglich den Namen und die Anschriften eines Einwohners und werden jedermann ohne Nachweis eines besonderen berechtigten Interesses erteilt. Die erweiterte Auskunft umfaßt außerdem Angaben über die Geburtsdaten, frühere Namen, Familienstand usw., sie darf nur erteilt werden, wenn von dem Auskunftersuchenden ein berechtigtes Interesse nachgewiesen wurde.

In Rechtsprechung und Literatur ist unbestritten, daß Handels- und Kreditauskunfteien nicht schon allein deshalb ein berechtigtes Interesse geltend machen können, weil sie geschäftsmäßig Daten über Bürger sammeln und weitergeben. Trotzdem mußte die Datenschutzaufsichtsbehörde im Rahmen einer Überprüfung der Vordrucke, mit denen Auskünfte bei den Meldeämtern eingeholt wurden, feststellen, daß viele Formblätter auch Fragen enthielten, die nur Gegenstand einer erweiterten Auskunft hätten sein können (Geburtsdatum, Beruf, Familienstand usw.).

Unabhängig davon, ob und in welchem Umfang von den Einwohnermeldeämtern tatsächlich entsprechende Auskünfte erteilt worden waren, hat die Datenschutzaufsichtsbehörde die betreffenden Vordrucke beanstandet und die Auskunfteien ersucht, in Zukunft von derartigen Fragen Abstand zu nehmen. Den Auskunfteien dürfte nämlich bereits im Zeitpunkt der Anfrage bewußt gewesen sein, daß eine evtl. Beantwortung der betreffen-

den Fragen durch die Meldebehörde melderechtlich unzulässig wäre. Es besteht damit ein Grund zu der Annahme, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden. Dies führt zu einer datenschutzrechtlichen Unzulässigkeit der Speicherung ("unrechtmäßig gewonnene Informationen können nicht rechtmäßigerweise gespeichert werden"). Auf dieses Kernproblem der Informationsgewinnung und -speicherung der Auskunftsteien wird auch unter den Tz. 3.2.4 eingegangen.

#### 3.2.3.4 Datenerhebungen bei den Betroffenen selbst und in ihrem Umfeld

Unmittelbar nach dem Inkrafttreten des Bundesdatenschutzgesetzes versuchten einige Auskunftsteien, die ihnen auferlegte Pflicht zur Information der Betroffenen über die Datenspeicherung im Zusammenhang mit der erstmaligen Übermittlung von Daten als Instrument zur Datengewinnung zu benutzen. Sie kombinierten das Benachrichtigungsschreiben mit einem Formblatt, in dem der Betroffene um eine Selbstauskunft gebeten wurde. Dieses führte bundesweit zu Protesten von Bürgern. Sie fühlten sich aufgrund der gewählten Formulierungen und der Gesamtgestaltung der Vordrucke falsch informiert, weil man annehmen konnte, das Datenschutzgesetz verpflichte sie zu einer Selbstauskunft bzw. gewähre den Auskunftsteien neue, weitergehende Rechte als bisher.

In Zusammenarbeit mit dem "Düsseldorfer Kreis" und den Spitzenorganisationen der Auskunftsteien sowie durch Einzelmaßnahmen auf Landesebene konnte erreicht werden, daß von den Auskunftsteien auf diese Art der Kombination der Benachrichtigung mit einer Aufforderung zur Selbstauskunft nunmehr verzichtet wird.

Datenschutzrechtliche Probleme ergaben sich auch aus der Vorgehensweise einzelner Auskunftsteien bei der Befragung von Nachbarn, Arbeitgebern, Vermietern, Hausverwaltern usw. Speziell zu der Nachbarschaftsbefragung haben die obersten Datenschutzaufsichtsbehörden mit den Auskunftsteien eine bundeseinheitliche Regelung getroffen, die unter Tz. 5.2.4 dargestellt ist.

Die Überprüfung von Vordrucken, die für die Befragung anderer Personen und Institutionen benutzt wurden, hat ebenfalls zu Beanstandungen geführt. In der Hauptsache hat die Datenschutzaufsichtsbehörde gefordert, daß zu allgemein gehaltene Fragen nach dem Privatleben der Betroffenen ("was gibt es sonst noch über die Person zu berichten") gestrichen wurden. Konkrete Fragen nach der Art der beruflichen Tätigkeit, der Dauer des Arbeitsverhältnisses, der Größe der Wohnung usw. konnten nicht kritisiert werden. Der Maßstab für eine datenschutzrechtliche Beurteilung ist auch hier nur die Frage, ob durch die Speicherung der auf diese Art gewonnenen Daten die Annahme gerechtfertigt ist, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden. Dies kann nur angenommen werden, wenn die Fragestellung darauf ausgerichtet ist, Gerüchte, rein subjektive Beurteilungen und "Klatsch" anstelle von nachprüfbaren Fakten zu erfahren.

Als Grenzfall ist insoweit die häufiger gebräuchliche Praxis anzusehen, die Schreiben mit Zusätzen wie "vertraulich", "Diskretion wird zugesichert und erbeten" oder "Weitergabe an Dritte untersagt" zu versehen. Diese Hinweise

sollen offenbar den Informanten veranlassen, doch detailliertere Auskünfte zu erteilen, als normalerweise vertretbar (Auskunft im Schutz der Anonymität). Die Datenschutzaufsichtsbehörde hat in den ihr bekanntgewordenen Fällen im Wege der Beratung versucht, die betreffenden Unternehmen davon zu überzeugen, daß derartige Formulierungen - auch wenn sie nicht generell zu beanstanden sind - im Einzelfall zu bedenklichen Datenspeicherungen führen können, der Nutzen also geringer sein dürfte als die möglichen negativen Folgen. Nicht alle Unternehmen haben sich dieser Auffassung anschließen können.

#### 3.2.4 Die Informationsverarbeitung der Auskunfteien - Ergebnisse der Einzelprüfungen -

##### 3.2.4.1 Art der Darstellung der Prüfungsergebnisse

Wegen der begrenzten Anzahl der geprüften Unternehmen sind die beispielhaft aufgeführten Sachverhaltsdarstellungen soweit verallgemeinert worden, daß Rückschlüsse auf die Gegebenheiten und Praktiken einzelner Auskunfteien nicht möglich sein dürften. Auf diese Weise soll vermieden werden, daß durch diesen Bericht Mitbewerbern am Markt und anderen Dritten Betriebsinterna einzelner speichernder Stellen bekanntwerden.

##### 3.2.4.2 Arbeitsweise der Auskunfteien

Auskunfteien werten zunächst systematisch alle verfügbaren allgemein zugänglichen Quellen (Telefonbücher, Adreßbücher, Handelsregister, öffentliche Verzeichnisse, Zeitungen, Schuldner-

verzeichnisse usw.) aus. Außerdem beschäftigen sie festangestellte und freiberufliche Rechercheure.

Kernstück einer jeden Auskunftsteil ist das sogenannte Archiv, das, wie immer es organisatorisch aufgebaut ist (konventionell oder computerunterstützt), die datenschutzrechtliche Dateiqualfikation erfüllt. Deshalb unterliegen Auskunftsteilen dem BDSG, während typische Detekteien (die im Grunde in gleicher Weise recherchieren) nicht der Kontrolle der Datenschutzaufsichtsbehörde unterworfen sind, weil sie nur im Einzelfall Informationen sammeln und diese nicht dateimäßig ablegen.

Die größeren Unternehmen sind in der Regel bundesweit organisiert. Sie unterhalten regional tätige "unselbständige Zweigstellen" im Sinne des § 39 BDSG. Zwischen den Auskunftsbüros der einzelnen Unternehmen findet ein umfangreicher Informationsaustausch statt. In vielen Fällen sind den Auskunftsteilen sogenannte Inkassobüros angegliedert.

Von der unmittelbar datenschutzrelevanten Recherche- und Auskunftstätigkeit zu trennen ist die sogenannte Akquisition dieser Unternehmen. Sie besteht darin, daß den Kunden sogenannte Anfragegutscheine veräußert werden. Die Gutscheine berechtigen (da die Auskunftsgebühr durch den Erwerb bereits gezahlt ist) unmittelbar zur Einholung einer Auskunft. Bei den bundesweit operierenden Auskunftsteilen können die Gutscheine in jedem Auskunftsbüro "eingelöst" werden.

### 3.2.4.3 Datenschutzrechtliche Beurteilung der Rechtsverhältnisse

#### - Vereinbarungen der einzelnen Auskunftsteilen mit ihren "Muttergesellschaften"

Bei den von der Datenschutzaufsichtsbehörde geprüften Stellen handelte es sich um Unternehmen (Organisationen), die sich über viele Jahrzehnte hinweg zu ihrer heutigen Form entwickelt haben. Hieraus resultieren unterschiedliche und zum Teil sehr komplexe vertragliche Konstruktionen. Charakteristisch ist in diesem Zusammenhang die Zwischenschaltung von Tochtergesellschaften, Betriebsgesellschaften, eingetragenen Vereinen und dergleichen. Den aus betriebswirtschaftlichen und unternehmenspolitischen Überlegungen heraus entstandenen Gebilden mangelt es nicht selten an Transparenz. So war es in einigen Fällen selbst den Unternehmen nicht ohne weiteres möglich, der Datenschutzaufsichtsbehörde darzulegen, wer für die Datenspeicherungen und Beauskunftungen die datenschutzrechtliche Verantwortung trägt. Erst nach eingehenden Analysen konnte in Zusammenarbeit mit der Datenschutzaufsichtsbehörde ermittelt werden, welche der beteiligten Gesellschaften als speichernde Stelle im datenschutzrechtlichen Sinne zu betrachten war.

Für den betroffenen Bürger sind derartig komplizierte Konstruktionen kaum zu durchschauen. Er läuft deshalb Gefahr, nicht den richtigen Adressaten für seine Ansprüche zu finden. Aus diesem Grunde hat die Datenschutzaufsichtsbe-

hörde darauf gedrungen, daß die betreffenden Unternehmen entweder ihre Rechtsbeziehungen neu ordnen oder aber die Betroffenen detailliert über die Gegebenheiten aufklären.

- Vereinbarungen der Auskunftsteien mit ihren Kunden

Grundlage für die vertraglichen Beziehungen zwischen den Auskunftsteien und ihren Kunden sind stets sogenannte "allgemeine Vertragsbedingungen". Gegen einige dieser Vereinbarungen mußte die Datenschutzaufsichtsbehörde Bedenken anmelden. So war teilweise festgelegt, daß die erteilten Auskünfte (die Schriftstücke, die den Kunden zugehen) Eigentum der betreffenden Auskunfttei bleiben und ersatzlos oder im Rahmen des Austausches gegen eine neue Auskunft zurückgefordert werden können, und zwar unabhängig davon, ob und in welcher Form der Kunde bereits Konsequenzen aus der ursprünglichen Auskunft gezogen hat. Als Grund für diese Regelung wurde der Wunsch der Auskunftsteien genannt, evtl. fehlerhafte Auskünfte "so aus der Welt zu schaffen, daß jeder Mißbrauch unmöglich ist".

Die Datenschutzaufsichtsbehörde sieht hier nicht nur handels- und zivilrechtliche Fragen der Aufbewahrungspflicht von Geschäftsunterlagen berührt. Sie geht auch davon aus, daß jede datenschutzrechtlich relevante Datenübermittlung - gerade wenn sie sich auf sehr sensitive Daten Dritter bezieht - nicht im nachhinein ungeschehen gemacht werden kann. Sie muß aufgrund ihrer Prüfungspflicht nach §§ 30 und 40

BDSG kontrollieren können, aufgrund welcher Anfrage welche Auskunft erteilt worden ist und wie diese Auskunft beim Empfänger verwertet wurde. Ähnliches gilt für das häufig vereinbarte Recht der Auskunftsteien, unter bestimmten Voraussetzungen nur mündliche statt schriftliche Auskünfte zu erteilen (vgl. Tz. 3.2.4.6).

In einigen allgemeinen Geschäftsbedingungen finden sich Bestimmungen, die durch ihre nicht eindeutigen Formulierungen bei den Kunden der Auskunftstei den Eindruck erwecken können, sie seien verpflichtet, quasi als Gegenleistung für die empfangene Auskunft (und zusätzlich zum gezahlten Entgelt) selbst auch Auskünfte über andere ihnen bekannte Personen zu erteilen. Ein solcher "Informationsaustausch auf Gegenseitigkeit" findet seine datenschutzrechtlichen Grenzen in den vertraglichen Beziehungen zwischen den Kaufleuten (z. B. in einer vereinbarten Verschwiegenheit) und in § 24 BDSG, der eine Datenübermittlung an Dritte außerhalb konkreter vertraglicher Vereinbarungen davon abhängig macht, daß schutzwürdige Belange nicht beeinträchtigt werden. Dies hat der Kunde der Auskunftstei im Einzelfall zu prüfen. Er darf nicht veranlaßt werden, pauschal Auskünfte zu erteilen.

Ein ähnliches Problem ergibt sich aus der Kombination einer Auskunftstei mit einem Inkassobüro. Es ist in diesen Fällen allgemein üblich, daß die Daten, die im Inkassobereich anfallen, in das Auskunftstei-Archiv übernommen werden. Dies geschieht bisher ohne ausdrückliche Einwilligung des Inkasso-Auftraggebers

und kann dessen Intentionen durchaus zuwiderlaufen (z. B. bei einer vereinbarten Verschwiegenheit mit dem säumigen Kunden). Die Datenschutzaufsichtsbehörde hat aus den o. g. Gründen gefordert, daß eine Übernahme der Daten nur noch dann erfolgt, wenn im Einzelfall eine entsprechende Vereinbarung mit dem Gläubiger getroffen wurde, dieser die Rechtmäßigkeit der Datenweitergabe also geprüft hat.

#### 3.2.4.4 Rechtmäßigkeit der Datenspeicherungen

Der Gesetzgeber hat die Zulässigkeit der Speicherung personenbezogener Informationen durch Auskunftsteilen davon abhängig gemacht, daß kein Grund zu der Annahme besteht, daß durch die Speicherung schutzwürdige Belange der Betroffenen beeinträchtigt werden (§ 32 BDSG). In der Literatur zum BDSG ist anerkannt, daß diese Bestimmung "zu den am wenigsten präzisen Generalklauseln des Bundesdatenschutzgesetzes" gehört. Wie bereits unter Tz. 3.2.3 dargestellt, ist für die Datenschutzaufsichtsbehörde bei der Festlegung von Beurteilungsmaßstäben die Art und Weise der Informationsgewinnung von besonderer Bedeutung. Die Speicherung einer sehr persönlichen Information, die der Betroffene in freier Entscheidung selbst preisgibt, braucht nicht zu der Annahme zu führen, daß schutzwürdige Belange beeinträchtigt werden, während die Speicherung der gleichen Information unzulässig wäre, wenn sie nur "vom Hörensagen" von einem Dritten stammt. Die Datenschutzaufsichtsbehörde hat daher bei allen Prüfungen die Archive der Auskunftsteilen stichprobenweise daraufhin überprüft, ob in ihnen Daten gespeichert waren, deren Inhalt und

deren mutmaßliche Herkunft zu Bedenken Anlaß gaben. Als Ergebnis ist festzustellen, daß in über 90 % der geprüften Vorgänge in dieser Hinsicht (vgl. jedoch Tz. 3.2.4.7 hinsichtlich der Speicherdauer) keine Gründe zu Beanstandungen vorlagen.

Hierbei ist allerdings zu berücksichtigen, daß die Auskunftsteile überwiegend nur Daten über Handelsunternehmen speichern, die teilweise ein eigenes Interesse an einer (möglichst positiven) Registrierung haben. Dies geht so weit, daß den Auskunftsteilen unaufgefordert Geschäftsberichte usw. zur Verfügung gestellt werden.

Gleichwohl gibt eine Beanstandungsquote zwischen 5 und 10 % zur Sorge Anlaß. Es kann nicht übersehen werden, daß sich die Auskunftsteile zumindest in der Vergangenheit auch solcher Quellen bedient haben, bei denen von vornherein feststand, daß sie die Auskünfte unter Verstoß gegen gesetzliche Bestimmungen oder vertragliche Vereinbarungen erteilten. Es ist der Datenschutzaufsichtsbehörde aus Rechtsgründen nicht möglich (vgl. Tz. 3.2.4.1), die aufgedeckten Quellen und Methoden sowie die Namen der betr. speichernden Stellen im einzelnen in diesem Bericht zu nennen. Als Beispiel sei jedoch der Fall genannt, in dem einem Kunden mitgeteilt wurde, bestimmte Daten könnten nur geschätzt werden, weil die betreffenden Datenbestände aufgrund gesetzlicher Bestimmungen durch die Auskunftsteile nicht eingesehen werden könnten. Tatsächlich lagen der Auskunftsteile jedoch die (rechtswidrigerweise gewonnenen) Originaldaten vor. Die angeblich geschätzten Daten entsprachen den Originaldaten bis ins Detail.

Ein anderer Komplex, der im Rahmen der Prüfungen zu datenschutzrechtlichen Bedenken Anlaß gegeben hat, ist die Überwachung der Rechercheure und die kritische Würdigung ihrer Rechercheergebnisse. Diese freien oder angestellten Mitarbeiter geben der Auskunftsteil in der Regel ihre Informanten nicht preis. Das gilt insbesondere für freie Mitarbeiter, die ausschließlich auf Honorarbasis arbeiten. Die Auskunftsteilen haben zwar ein geschäftliches Interesse daran, "gute" Informationen zu erhalten. Die Art und Weise, wie die Daten beschafft werden, wird aber offenbar nicht so genau überwacht. In den Archiven ist im allgemeinen nur vermerkt, welcher Rechercheur die Daten erhoben hat. Woher er sie bekommen hat und in welcher Weise er deren Richtigkeit verifiziert hat, ist nicht dokumentiert.

Die Datenschutzaufsichtsbehörde hat bei ihren Überprüfungen zwar in einer Reihe von Einzelfällen Zweifel an der Richtigkeit der gespeicherten Daten angemeldet, es war ihr aber aufgrund der fehlenden Dokumentation ebensowenig möglich, den Nachweis einer Manipulation des Rechercheurs zu erbringen, wie es den Auskunftsteilen möglich war, die Richtigkeit und Rechtmäßigkeit der Datenspeicherung nachzuweisen. Aus diesem Grund hat die Datenschutzaufsichtsbehörde die Auskunftsteilen ersucht, in Zukunft die Datenquellen so aufzuzeichnen, daß die Beurteilung der Rechtmäßigkeit der Datenspeicherung möglich ist. Die Auskunftsteilen haben diese Forderung zur Kenntnis genommen, jedoch Zweifel an der rechtlichen Durchsetzbarkeit der Auffassung der Datenschutzaufsichtsbehörde angemeldet. Eine endgültige Klärung wird u. U. erst durch die Gerichte oder im Rahmen der Novellierung des BDSG erfolgen.

#### 3.2.4.5 Benachrichtigung der Betroffenen, Erteilung von Auskünften über gespeicherte Daten

Nachdem die unter Tz. 3.2.3.4 beschriebenen Probleme der unzulässigen Kombination der Benachrichtigungsschreiben nach § 34 BDSG mit der Bitte um eine Selbstauskunft bereinigt werden konnten, haben sich im Rahmen der Prüfungen insoweit keine Gründe für Beanstandungen ergeben.

Das gleiche gilt für die Erteilung von Auskünften über die gespeicherten Daten. Den Betroffenen wird von den Auskunftsteilen in der Regel nicht einmal das gesetzlich vorgesehene Entgelt für derartige Auskünfte berechnet. Die Bürger sind dennoch häufig mit dem Inhalt der Auskünfte unzufrieden, weil ihnen zwei Fragen nicht beantwortet werden: "Woher stammen die Informationen?" und "An wen sind sie weitergegeben worden?" Diese Daten (Informanten und Auftraggeber) sind in der Regel nicht im Auskunftsbestand abgespeichert und unterliegen damit nicht der gesetzlichen Auskunftspflicht.

#### 3.2.4.6 Prüfung des berechtigten Interesses der Informationsempfänger

Die Übermittlung von personenbezogenen Daten durch Auskunftsteilen ist zulässig, wenn der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat. Die Gründe für das Vorliegen eines berechtigten Interesses und die Mittel für ihre glaubhafte Darlegung sind von der Auskunftsteil aufzuzeichnen (§ 32 Abs. 2 BDSG). Diese Bestimmung zwingt die Auskunftsteilen dazu, unter Umständen einem Kunden Informationen

vorzuenthalten (und auf die entsprechenden Honorare zu verzichten), weil Zweifel an dem berechtigten Interesse des Empfängers bestehen. Daß dieses in der Praxis zu Interessenkonflikten führt, wurde durch die Prüfungen bestätigt. Die Handelsauskunfteien haben sich zwar bereit erklärt, sich das berechnete Interesse durch das Ankreuzen von vorgedruckten Möglichkeiten (Darlehensgewährung, Warenverkauf auf Ziel, Geschäftsanbahnung u. ä.) nachweisen zu lassen. Sie haben auch die Absicht bekundet, bei ihren Kunden die Richtigkeit dieser Angaben stichprobenweise anhand der Geschäftsunterlagen zu überprüfen, und kommen ihren Dokumentationspflichten nach. Als ein wirkungsvolles Instrument zur Abwehr mißbräuchlicher Anfragen kann dieses Verfahren nach den Feststellungen der Datenschutzaufsichtsbehörde aber dennoch nicht gewertet werden. Zum einen sind derartige Kontrollen bei mündlichen und telefonischen Auskünften nahezu wirkungslos, zum anderen bleiben Täuschungen durch Kunden der Auskunfteien ohne Sanktionen, da das "Erschleichen" von Informationen nach den Bestimmungen des BDSG weder strafbewehrt ist noch eine Ordnungswidrigkeit darstellt.

#### 3.2.4.7 Berichtigung, Sperrung und Löschung von Daten

Wenn Betroffene von den Auskunfteien berechtigterweise die Berichtigung, Sperrung oder Löschung ihrer Daten verlangen, so können sie davon ausgehen, daß ihren Anträgen entsprochen wird. Stichprobenweise Kontrollen der Datenschutzaufsichtsbehörde haben insoweit keine Anhaltspunkte für Unregelmäßigkeiten ergeben.

Dennoch haben sich bei den Prüfungen eine Reihe von Problemen grundsätzlicher Art bezüglich der Sperrung und Löschung von Daten ergeben. § 35 BDSG schreibt den Auskunftsteilen vor, Daten, die älter als fünf Jahre sind, zu sperren. Gesperrte Daten sind mit einem entsprechenden Vermerk zu versehen. Sie dürfen "nicht mehr verarbeitet, insbesondere übermittelt oder sonst genutzt werden, es sei denn, daß die Nutzung zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerlässlich ist oder der Betroffene in die Nutzung eingewilligt hat". Die Realisierung dieses Nutzungsverbot es erfordert weitreichende organisatorische Maßnahmen, die auch mit einem personellen Aufwand verbunden sind. Wenn die Daten nicht unmittelbar gelöscht werden, müssen sie aus dem aktuellen Archivbestand entfernt und in ein Alt-Archiv überführt werden. Dieser Arbeit versuchten sich einige der geprüften Stellen zu entziehen. So wurden von der Datenschutzaufsichtsbehörde Vorgänge beanstandet, die bis zu 16 Jahre alt waren. 8 bis 10 Jahre alte Belege waren häufiger zu finden. Dabei handelte es sich nicht nur um Unterlagen mit statischem Charakter (z. B. Handelsregisterauszüge). Die betreffenden Auskunftsteile rechtfertigten die Zeitüberschreitung mit einem ihrer Meinung nach unzumutbaren Aufwand für eine jährliche systematische Durchsicht des Archivs. Diesem Argument konnte die Datenschutzaufsichtsbehörde nicht folgen, weil auch die Mitteilungen aus dem Schuldnerverzeichnis nach § 915 Zivilprozeßordnung (eidesstattliche Versicherungen usw.) nach Zeitablauf (3 Jahre) ausge-

sondert werden müssen. Deren Aussonderung wurde im übrigen besser befolgt, offenbar, weil die Auskunftsteilen anderenfalls vom Bezug dieser Mitteilungen ausgeschlossen werden können. Die Datenschutzaufsichtsbehörde hat den betreffenden Auskunftsteilen eine angemessene Frist eingeräumt, um die erforderlichen Aussonderungen nachzuholen. Das gilt auch für die Löschung derjenigen Archivunterlagen, deren Speicherung die Datenschutzaufsichtsbehörde aus den unter Tz. 3.2.4.4 genannten Gründen (rechtswidrige Informationsgewinnung) für unzulässig hält. Ob diese Forderungen in der Praxis erfüllt werden, müssen die künftigen Prüfungen zeigen.

### 3.3 Zusammenfassende Darstellung der Ergebnisse der bisherigen Prüfungen der Datenschutzaufsichtsbehörde

Die unter Tz. 3.2 dargestellten Prüfungsergebnisse zeigen, daß der Datenschutzaufsichtsbehörde weder in den Rechenzentren noch im Bereich der Auskunftsteilen Fälle betrügerischer Manipulationen oder bewußten Datenmißbrauchs bekanntgeworden sind.

Als weiteres positives Ergebnis der bisherigen Prüfungen kann festgestellt werden, daß es durch das BDSG zu einem Umdenken bei den speichernden Stellen gekommen ist. Die Rechte der Betroffenen haben einen höheren Stellenwert erhalten, die Datenverarbeitung ist transparenter geworden. Die staatliche Datenschutzaufsicht hat zweifellos zu einem sehr viel sorgfältigeren Umgang mit personenbezogenen Daten als in der Vergangenheit geführt.

Auch wenn die Komplexe

- Sicherheit und Ordnungsmäßigkeit der automatisierten Datenverarbeitung,
- rechtliche und tatsächliche Ausgestaltung der Auftragsdatenverarbeitung,
- Methoden der Informationsgewinnung der Auskunftsteilen,
- Offenbarung von Datenquellen gegenüber der Datenschutzaufsichtsbehörde

von den speichernden Stellen und der Datenschutzaufsichtsbehörde noch nicht in allen Einzelheiten gleich beurteilt werden, so haben die Prüfungen zumindestens die Sachverhalte klargestellt, Mißverständnisse abgebaut und zu Überlegungen zur Verbesserung des Datenschutzes geführt.

#### 3.4 Zusammenarbeit mit den betrieblichen Datenschutzbeauftragten

Die Zusammenarbeit zwischen den betrieblichen Datenschutzbeauftragten und der Datenschutzaufsichtsbehörde vollzieht sich in unterschiedlicher Form. Zunächst zählen die betrieblichen Datenschutzbeauftragten neben der Geschäftsleitung und den Leitern der Datenverarbeitungsstellen bei Prüfungsmaßnahmen zu den unmittelbaren Gesprächspartnern der Datenschutzaufsichtsbehörde. Die Funktion der betrieblichen Datenschutzbeauftragten hat sich dabei gut bewährt, weil sie als "betriebliche Datenschutz-Sachverständ-

dige" eine Mittlerfunktion einnehmen können zwischen den mehr "unternehmerisch" orientierten Standpunkten der speichernden Stellen und der primär dem Gesetzeswortlaut verpflichteten Datenschutzaufsichtsbehörde.

Nicht alle betrieblichen Datenschutzbeauftragten haben diese Aufgabe richtig erkannt. Einigen von ihnen war von der Geschäftsleitung offenbar die Funktion eines "Datenschutz-Abwehr-Beauftragten" übertragen worden. Die Datenschutzaufsichtsbehörde hat in diesen Fällen klargestellt, daß das vom Gesetzgeber vorgegebene Prinzip der "qualifizierten Selbstkontrolle" (die Durchführung des Datenschutzes wird zunächst von der speichernden Stelle selbst realisiert und überwacht, die Datenschutzaufsichtsbehörde schreitet nur in Konfliktfällen bzw. kontrollierend ein) auch zukünftig nur dann Bestand haben kann, wenn die betrieblichen Datenschutzbeauftragten ihre Aufgaben auch tatsächlich erfüllen.

Einige betriebliche Datenschutzbeauftragte mußten daran erinnert werden, daß sie selbst Normadressat des Gesetzes sind. Die Führung und Auswertung der Datenübersicht, die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme sowie die Auswahl und datenschutzrechtliche Ausbildung der Mitarbeiter in der Datenverarbeitung sind wichtige Funktionen, die nicht mit der Bemerkung, daß "man den EDV-Leuten sowieso nicht auf die Schliche komme, wenn diese wirklich manipulieren wollten", abgetan werden können.

Im übrigen hat sich die Zusammenarbeit mit den betrieblichen Datenschutzbeauftragten nach Anfangsschwierigkeiten positiv entwickelt. Es konnte ein Vertrauensverhältnis aufgebaut werden, das eine offene Diskussion auch sehr komplexer und kontroverser Themen (z. B. Personalinformationssysteme, schwarze Listen über Kunden und Geschäftspartner, Adressenhandel) zuläßt. Das gilt auch für Unternehmen, die dem dritten Abschnitt des Bundesdatenschutzgesetzes unterliegen; hier ist die Behandlung "heikler Fragen" aus der Sicht der Unternehmen offenbar deshalb relativ unproblematisch, weil die Datenschutzaufsichtsbehörde (wegen der Begrenzung ihrer Kontrollbefugnis auf die ihr von den Betroffenen vorgetragenen Beschwerden) zwar beratend, nicht aber beanstandend tätig werden kann. Dies dokumentiert sich auch in der steigenden Zahl von Ersuchen, sie möge im Rahmen von Vorträgen oder Diskussionsveranstaltungen zu aktuellen datenschutzrechtlichen Problemen Stellung nehmen.

### 3.5 Problembereiche bei der Durchsetzung datenschutzrechtlicher Ansprüche

Der Bereich, in dem in erster Linie von Schwierigkeiten bei der Durchsetzung konkreter Bestimmungen des BDSG gesprochen werden kann, ist der Komplex der Sperrung und Löschung von Daten. Die Erkenntnisse der Datenschutzaufsichtsbehörde beziehen sich zwar primär auf die Gegebenheiten bei Auskunftsteilen (Sperrung der Daten am Ende des fünften Kalenderjahres nach ihrer Einspeicherung gemäß § 35 Abs. 2 BDSG), aber auch bei den Prüfungen von Rechenzentren wurde deutlich, daß der Gesetzesbefehl, "Daten zu sperren, wenn ihre

Kenntnis für die Erfüllung des Zweckes ihrer Speicherung nicht mehr erforderlich ist" (§ 27 Abs. 2 BDSG) von Handelsunternehmen nur eingeschränkt befolgt wird.

In der Regel werden die Daten nicht zunächst gesperrt, sondern gelöscht, wenn dies nach Ablauf gesetzlicher Aufbewahrungsfristen oder aus Speicherplatzgründen opportun erscheint. Das neue datenschutzrechtliche Instrument eines differenzierten Nutzungsverbotes entfaltet somit kaum eine praktische Wirkung. Dies resultiert im wesentlichen aus der nach wie vor ungelösten Frage, ob Daten, die aus handelsrechtlichen oder steuerrechtlichen Gründen (z. B. Anspruchsverjährung nach 30 Jahren) aufbewahrt werden müssen, noch zur "Erfüllung des Zwecks der Speicherung erforderlich sind" oder nicht. Die Unternehmen der Wirtschaft bejahen im allgemeinen diese Frage und weisen außerdem darauf hin, daß dem Betroffenen keine Nachteile aus dem Umstand entstehen, daß die Formvorschriften des § 14 Abs. 2 Satz 3 BDSG (Kennzeichnung der gesperrten Daten) nicht erfüllt werden.

Ein weiterer Komplex, bei dem Zweifel angebracht sind, ob die datenschutzrechtlichen Ansprüche der Bürger hinreichend beachtet werden, ist die Wahrung der Verschwiegenheit des Vertragspartners (Handelsunternehmen, Bank, Versicherung usw.) gegenüber anderen Unternehmen. Die branchenüblichen mündlichen oder schriftlichen Informationsdienste über vermeintlich "schwarze Schafe" begründen in der Regel Datenübermittlungen im Sinne des § 24 BDSG. Wie die öffentliche Diskussion um die Bankauskünfte gezeigt

hat, wird seitens der Wirtschaft in diesen Fällen dem gesetzlichen Tatbestand "berechtigte Interessen der Datenempfänger" ein wesentlich höheres Gewicht beigemessen als dem gesetzlichen Auftrag, die schutzwürdigen Belange der Betroffenen zu wahren.

Ein dritter Bereich, der in diesem Zusammenhang zu erwähnen ist, umfaßt die formalen Pflichten der speichernden Stellen. In Publikationen wird immer wieder darauf hingewiesen, daß gerade in kleinen und mittleren Unternehmen betriebliche Datenschutzbeauftragte nicht bestellt werden. Davon ausgehend, daß die Datenschutzaufsichtsbehörden ohnehin nur in konkreten Einzelfällen und auch dann nur soweit, wie die jeweilige Beschwerde reicht, prüfen können, werde das Datenschutzrecht insgesamt weitgehend ignoriert. Die Datenschutzaufsichtsbehörde hat zwar keine konkreten Anhaltspunkte, die derartige Aussagen bestätigen, eine teilweise durchaus nachlässige Befolgung der gesetzlich vorgeschriebenen Pflichten der speichernden Stellen in diesem Bereich ist aber nicht zu übersehen.

### 3.6 Methodische und inhaltliche Auswirkungen der neuen Technologien auf die Prüfungspraxis der Datenschutzaufsichtsbehörde

Als neue datenschutzrelevante Technologien sind alle technischen Systeme und Verfahren anzusehen, die "Computer-Intelligenz" dezentralisieren und damit Möglichkeiten eröffnen, individuelle Entscheidungen, Verhaltensweisen und Bedürfnisse der Benutzer unter Umständen sogar ohne ihr Wissen zu registrieren, aufzubereiten und zweckge-

richtet zu verwerten. Unter Sicherheitsaspekten unterliegen zusätzlich auch die zur Zeit entstehenden großen Computer-Netzwerke und die Informationpools als neue "Organisations-Technologien" der besonderen Aufmerksamkeit der Datenschutzaufsichtsbehörde. Es handelt sich hierbei z. B. um folgende Projekte:

- Bildschirmtext,
- Pay-TV,
- Fernmeß- und Fernwirksysteme,
- private Breitbandkommunikationen,
- offene Datenübertragungsnetze,
- offene Informationsdatenbanken,
- automatisierte Bürokommunikation,
- elektronische Sicherungs-, Personenidentifizierungs- und Zugangskontrollsysteme.

Die Datenschutzaufsichtsbehörde wird bereits jetzt mit einigen speziellen Technologien (z. B. externe BTX-Rechenzentren oder Online-Abfragen bei Auskunftsteilen) im Rahmen der Überprüfungen von Rechenzentren und Auskunftsteilen unmittelbar befaßt. Sie wird im Rahmen ihrer Beratungsfunktion gegenüber den Unternehmen aber in absehbarer Zeit auch mit der ganzen Bandbreite der datenschutzrechtlichen Fragestellungen im Zusammenhang mit den neuen Technologien konfrontiert werden.

Wenn außerdem, wie in den Entwürfen zur BDSG-Novelle geplant, die sogenannte Anlaßaufsicht (§ 30 BDSG) in eine qualifizierte Aufsicht von Amts wegen umgewandelt werden soll und ggf. bestimmte Maßnahmen zur Gewährleistung des Datenschutzes von der Datenschutzaufsichtsbehörde mit Hilfe von Verwaltungsakten durchzusetzen sein

werden, dann wird dies erhebliche methodische, inhaltliche und kapazitätsmäßige Auswirkungen auf die Prüfungspraxis der Datenschutzaufsichtsbehörde haben.

Auch wenn man davon ausgeht, daß die besondere wirtschaftliche und geographische Struktur des Landes Schleswig-Holstein zu einer gewissen Zeitversetzung bei der Realisierung derartig komplexer Systeme führen wird, so kann sich die Datenschutzaufsichtsbehörde nicht der Diskussion der Grundsatzfragen in den zuständigen Gremien des Bundes und der Länder (Düsseldorfer Kreis) und der Wirtschaft (Arbeitskreise der betrieblichen Datenschutzbeauftragten) entziehen. Anders als in der Vergangenheit (die heute gängigen EDV-Systeme und -Verfahren bestanden bereits, bevor das Datenschutzrecht in Kraft trat) werden in der Zukunft die nachvollziehenden Prüfungen der Datenschutzaufsichtsbehörde zunehmend ersetzt werden durch Prüfungen, die die Planungs- bzw. Realisierungsphase flankieren. Die betreffenden Unternehmen werden nicht das Risiko eingehen, Verfahren einzuführen, die sich im nachhinein als datenschutzrechtlich bedenklich erweisen; sie werden vielmehr bemüht sein, vorab ein Testat zu erhalten, das die rechtliche Unbedenklichkeit bestätigt.

4. Die Akzeptanz des Datenschutzes in der  
Wirtschaft

4.1 Anfängliche Vorbehalte

Gegen die Überlegungen des Datenschutzgesetzgebers gab es zunächst erhebliche Vorbehalte. Die Gründe hierfür waren mehrschichtig. Insbesondere wurden unübersehbare Kostenfolgen ins Feld geführt. Diese Reaktion war insofern überraschend, als Wirtschaft und Verwaltung seit Beginn der 70er Jahre immer wieder gesetzgeberische Maßnahmen auf dem Gebiete der Verarbeitung personenbezogener Daten gefordert hatten. So war z. B. eine entsprechende Resolution auf dem Internationalen Kongreß für Datenverarbeitung 1974 in Berlin getragen von dem Wunsch der Datenverarbeiter, ihnen die Last abzunehmen, möglicherweise im rechtsfreien Raum personenbezogene Daten verarbeiten zu müssen. Dennoch mußten die obersten Datenschutzaufsichtsbehörden insbesondere in den Bereichen Kreditwirtschaft, Versicherungswirtschaft und allgemeine Personalverwaltung mit den Interessenvertretern der Wirtschaft eingehende Verhandlungen führen. Es ging dabei z. B. um die Probleme der Speicherung von Daten der Bankkunden bei der Schutzgemeinschaft für das Kreditgewerbe, der Weitergabe der Daten von Versicherungsgesellschaften an Rückversicherer und Außendienstmitarbeiter sowie um den Aufbau von sog. Personalinformationssystemen.

Zwischenzeitlich kann jedoch festgestellt werden, daß in der Privatwirtschaft überwiegend eine sachgerechte Einstellung zum Datenschutz vorzufinden ist.

#### 4.2 Abbau der Konfliktsituationen

Viele Unternehmen haben erkannt, daß die Forderungen des Datenschutzgesetzgebers positive betriebswirtschaftliche Nebeneffekte haben. Bereits die Realisierung einzelner Maßnahmen zum Datenschutz führt häufig zu einer besseren Steuerung der Arbeitsabläufe. Mehr- und Doppelarbeiten können vermieden werden, die Transparenz der Arbeitsabläufe führt zur Überschaubarkeit und wirksameren Kontrolle, Arbeitsabläufe lassen sich vereinfachen und beschleunigen. Eine sorgfältige Programm- und Verfahrensprüfung mit vorgeschaltetem Testverfahren hilft kostenintensive Wiederholungsläufe zu vermeiden und Haftungsrisiken zu mindern. Die Dokumentation, die sinnvolle Zusammenfassung aller Unterlagen, die bei der Erstellung eines Programms entstanden sind, ermöglicht eine schnelle Einarbeitung bei Programmänderungen, vergleichbare Vorhaben lassen sich schneller lösen, neues Personal kann besser eingearbeitet werden. Das Ausscheiden eines Programmierers stellt keine "betriebliche Katastrophe" dar, wenn die Dokumentation der Verfahren verhindert, daß er womöglich "sein Wissen mit ins Grab nimmt".

Insbesondere auch die Verpflichtung, technische und organisatorische Sicherheitsmaßnahmen zu treffen, hat erhebliche Nebeneffekte, die sich letztendlich als betriebswirtschaftlicher Nutzen quantifizieren lassen.

Ursächlich für eine Hinwendung zum Datenschutzgedanken ist offenbar auch die bisherige Arbeitsweise der Datenschutzaufsichtsbehörde

selbst gewesen. Sie hat versucht, eine emotionsfreie Atmosphäre zu schaffen, die es der datenverarbeitenden Wirtschaft erlaubt, von sich aus an der Verwirklichung des Datenschutzes mitzuarbeiten. In diesem Sinne hat die Datenschutzaufsichtsbehörde einen großen Teil ihrer Kapazität darauf verwandt, im Vorfeld beratend und unterstützend tätig zu werden. Sie hat sich auch als Service-Unternehmen und nicht nur als Kontrollinstitution verstanden. Einige Beispiele mögen dies verdeutlichen:

- Wann immer die Datenschutzaufsichtsbehörde bei ihren Prüfungen festgestellt hat, daß bestimmte datenschutzrechtliche Schwachstellen sich als symptomatisch für einen größeren Bereich erwiesen, hat sie versucht, durch gezielte Informationen andere Betriebe hierauf aufmerksam zu machen. Als z. B. bei der Prüfung der Vertragsbeziehungen zwischen Auftraggeber und Service-Rechenzentrum Regelungsdefizite bei fast jeder Einzelprüfung sichtbar wurden, hat die Datenschutzaufsichtsbehörde eine entsprechende Checkliste für die Vertragsgestaltung erstellt und sie veröffentlicht.
  
- Sie hat ferner besonderen Wert auf die Information und Unterrichtung der Wirtschaft in allen Datenschutzfragen gelegt, zahlreiche Vortragsveranstaltungen durchgeführt und zu allgemeinen und speziellen Datenschutzfragen bis hin zu branchenspezifischen Problemstellungen Stellung genommen. Die wichtigsten Beschlüßergebnisse der obersten Aufsichtsbehörden für den Datenschutz hat sie veröffentlicht.

- Besondere Aufmerksamkeit wurde der allgemeinen und speziellen Beratung der betrieblichen Datenschutzbeauftragten gewidmet. So ist die Datenschutzaufsichtsbehörde u. a. regelmäßig den Einladungen des für Schleswig-Holstein zuständigen Erfahrungsaustauschkreises der Gesellschaft für Datenschutz und Datensicherung gefolgt. Hier hat sie betriebliche Datenschutzbeauftragte beraten und informiert.

Dies bedeutet aber nicht, daß sich die Datenschutzaufsichtsbehörde im Einzelfall nicht sehr entschieden für die Durchsetzung der Rechte der betroffenen Bürger eingesetzt und ihre Kontrollen von Amts wegen umfassend durchgeführt hat.

#### 4.3 Mittler-Funktion der Datenschutzaufsichtsbehörde

Die oben geschilderte Vorgehensweise hat es der Datenschutzaufsichtsbehörde ermöglicht, zunehmend die Mittlerrolle zwischen Bürger und Wirtschaft zu übernehmen. Anerkennung aufgrund fachlicher Kompetenz, Vertrauen aufgrund positiver Erfahrungen und kurze Wege in die Betriebe hinein durch vielfältige Kontakte sind hierbei die entscheidenden Faktoren. Daß diese Funktion erforderlich ist, beweisen viele Einzelfälle. Mißverständnisse, durch schroffen Schriftwechsel verhärtete Fronten, aber auch die Inanspruchnahme von Datenschutzrechten als bloßer Vorwand zur Verdeckung anderer Absichten fordern immer wieder das ausgleichende Vermitteln der Datenschutzaufsichtsbehörde .

5. Zusammenarbeit zwischen den Datenschutzaufsichtsbehörden der Länder

5.1 Entstehung und Funktion des "Düsseldorfer Kreises"

Unmittelbar nach dem Inkrafttreten des BDSG hat die Innenministerkonferenz (durch Beschlüsse vom 22. Juni 1977 und 15. Oktober 1977) vereinbart, durch regelmäßige Abstimmungsgespräche der Datenschutzreferenten eine möglichst einheitliche Anwendung des Datenschutzrechts zu erreichen. Dies sollte insbesondere für "Datenschutzprobleme von überregionaler Bedeutung" gelten. Das Land Nordrhein-Westfalen hatte sich bereit erklärt, die Federführung für den Gesprächskreis zu übernehmen, so daß wegen des regelmäßigen Tagungsortes am Sitz des nordrhein-westfälischen Innenministeriums sich im Laufe der Zeit die Bezeichnung "Düsseldorfer Kreis" herausgebildet hat.

Der Düsseldorfer Kreis hat in der Zwischenzeit zu mehr als 200 datenschutzrechtlichen Problemen Stellung genommen. Die Beschlußfassung des Gremiums unterliegt keinen formalen Zwängen, es gibt weder ein Vetorecht noch sind die Teilnehmer gezwungen, sich Mehrheitsentscheidungen zu unterwerfen. In der nunmehr sechsjährigen Tätigkeit des Düsseldorfer Kreises war es aber stets möglich, auch bei zunächst unterschiedlichen Rechtsauffassungen zu bestimmten Problemen jeweils für alle Seiten tragbare Kompromisse zu finden. Dies ist im Hinblick auf die sehr kritische und insbesondere auch vergleichende Beobachtung der Datenschutzaufsichtsbehörden durch überregional operierende speichernde Stellen der einzelnen Länder sehr wichtig.

Daneben steht der Düsseldorfer Kreis den Wirtschaftsverbänden als Ansprechpartner für die Diskussion spezieller datenschutzrechtlicher Fragen zur Verfügung. Zu diesem Zweck werden von Fall zu Fall kleine Arbeitsgruppen gebildet, in denen die Probleme zusammen mit den Vertretern der Wirtschaft aufbereitet und eine abschließende Stellungnahme der Datenschutzreferenten der Länder vorbereitet wird.

Nicht zuletzt dient der Düsseldorfer Kreis auch dem Erfahrungsaustausch der Datenschutzaufsichtsbehörden der Länder untereinander.

## 5.2 Beispiele für besondere Koordinierungsbemühungen des Düsseldorfer Kreises

Nachstehend sind aus der Vielzahl der datenschutzrechtlichen Themen, zu denen der Düsseldorfer Kreis allgemein anerkannte Rechtsauffassungen erarbeitet bzw. Übereinstimmungen mit den Interessenvertretungen der betreffenden speichernden Stellen erzielt hat, einige ausgewählt, die wegen ihrer weitreichenden Auswirkungen eine besondere Aufmerksamkeit in der Öffentlichkeit gefunden haben.

### 5.2.1 Verwaltungsvorschriften zum Bundesdatenschutzgesetz

Eines der wichtigsten Ergebnisse der gemeinsamen Bemühungen der Datenschutzaufsichtsbehörden der Länder um eine möglichst einheitliche Anwendung des Datenschutzrechts sind die sogenannten "vorläufigen Verwaltungsvorschriften zum BDSG". In den Ländern, in denen die Datenschutzaufsicht

auf der Ebene der Regierungspräsidenten (in Bayern der Regierungen) wahrgenommen wird, sind sie von den jeweiligen Innenministerien in Form einer die Verwaltung bindenden Richtlinie erlassen und veröffentlicht worden. In Schleswig-Holstein werden die Verwaltungsvorschriften zwar inhaltlich angewandt, ein formelles Inkraftsetzen und eine Veröffentlichung erübrigten sich aber, weil die Datenschutzaufsicht direkt vom Innenminister wahrgenommen wird.

Vertreter der Wirtschaft, die Vereinigungen der betrieblichen Datenschutbeauftragten, die Gewerkschaften, die EDV-Hersteller und nicht zuletzt auch die Interessenvertreter der Betroffenen sind bereits während der Erarbeitung der Vorschriften gehört und teilweise aktiv an ihrer Gestaltung beteiligt worden.

#### 5.2.2 Bundeseinheitliche Vereinbarungen mit der SCHUFA-Organisation

Die Organisation der "Schutzgemeinschaft für allgemeine Kreditsicherung" (SCHUFA) stellt sich den Datenschutzaufsichtsbehörden als eine auf Gegenseitigkeit beruhende Gemeinschaftseinrichtung kreditgebender Stellen dar, die mit Banken, Sparkassen, Einzel- und Versandhandelsunternehmen und sonstigen durch Vertrag berechtigten Firmen zusammenarbeitet. Die dreizehn regionalen SCHUFA-Gesellschaften erhalten ihre Informationen direkt von der kreditgebenden Wirtschaft. Ihre Vertragspartner übermitteln der SCHUFA die Daten über die gewährten Konsumentenkredite und deren Abwicklungsmerkmale. Als Gegenleistung sind sie berechtigt, bei der SCHUFA Auskünfte aus den dort gespeicherten Informationen zu erhalten.

Die Dateien der SCHUFA-Organisation dürften zu den größten und von ihrem Inhalt und ihrer Zweckbestimmung her sensitivsten privaten Datenbeständen mit personenbebezogenen Informationen in der Bundesrepublik zählen. Aus diesem Grunde waren umfangreiche und intensive Verhandlungen mit den Vertretern der SCHUFA-Organisation erforderlich, um festzulegen, in welcher Form die neuen datenschutzrechtlichen Gegebenheiten insbesondere im Hinblick auf die Art der Auskünfte, die Sicherung gegen Mißbrauch und die Benachrichtigung der Betroffenen in der Praxis ihren Niederschlag zu finden hatten.

Für jedermann sichtbar wurden die diesbezüglichen Bemühungen des Düsseldorfer Kreises im Zusammenhang mit der sogenannten "SCHUFA-Klausel". Hierbei handelt es sich um die schriftliche Einwilligung der Betroffenen den Kreditinstituten gegenüber zur Übermittlung von Kreditdaten an die SCHUFA. Der mit dem Düsseldorfer Kreis abgestimmte Text dieser SCHUFA-Klausel lautet: "Das Kreditinstitut ist berechtigt, der Schutzgemeinschaft für allgemeine Kreditsicherung Daten des Kreditnehmers und etwaiger Mitschuldner über die Aufnahme (Kreditbetrag, Laufzeit, Ratenbeginn) und die Abwicklung dieses Kredites zur Speicherung zu übermitteln". Dem Kreditnehmer wird außerdem die Anschrift der betreffenden SCHUFA-Gesellschaft genannt. Vergleichbare Klauseln bestehen auch für Kontoeröffnungsverträge und Bürgschaftserklärungen.

Die Datenschutzaufsichtsbehörden der Länder gehen davon aus, daß in dieser Formulierung ein Kompromiß zwischen den Interessen des Kreditge-

werbes an einer größtmöglichen Absicherung gegen Kreditausfälle und den individuellen Rechten der Kunden auf Geheimhaltung ihrer finanziellen Verhältnisse gefunden ist.

Unabhängig von diesen Absprachen zwischen dem Düsseldorfer Kreis und der SCHUFA-Organisation unterliegen die einzelnen SCHUFA-Gesellschaften mit ihren Zweigstellen der Kontrolle durch die zuständigen Datenschutzaufsichtsbehörden.

### 5.2.3 Klärung datenschutzrechtlicher Fragen mit der Versicherungswirtschaft

Die Abschätzung des Risikos ist in der Versicherungswirtschaft ein wesentliches Element der Tarifikalkulation und der einzelfallbezogenen Vertragsgestaltung. Da Versicherungsverträge zu einem großen Teil mit oder zugunsten natürlicher Personen abgeschlossen werden, bedingt diese Risikoabschätzung grundsätzlich das Sammeln und Analysieren personenbezogener Daten. Die Voraussetzungen und die Grenzen solcher Datenerhebungen und die rechtlichen Voraussetzungen für die Bildung von Informationspools waren und sind noch immer Gegenstand von Verhandlungen des Düsseldorfer Kreises mit dem Gesamtverband der Versicherungswirtschaft.

Obwohl bereits vor mehreren Jahren eine Einigung über die sogenannte "Versicherungs-Klausel" und damit im Zusammenhang stehende Aufklärungspflichten erzielt werden konnte, wird sich der Düsseldorfer Kreis auch in Zukunft schwerpunktmäßig mit dieser schwierigen datenschutzrechtlichen Materie zu befassen haben.

Der Text dieser Klausel ist je nach Art des Versicherungsvertrages unterschiedlich, in bezug auf Lebens-, Kranken- und Unfallversicherungen hat er folgenden Wortlaut: "Alle Ärzte, die mich bisher behandelt haben und in Zukunft behandeln werden, entbinde ich hiermit der Gesellschaft gegenüber von ihrer Schweigepflicht, auch über meinen Tod hinaus. Außerdem ermächtige ich andere Versicherungsgesellschaften, Versicherungsträger und Behörden, der Gesellschaft die erforderlichen Auskünfte zu erteilen. Ich willige ein, daß der Versicherer im erforderlichen Umfang Daten, die sich aus den Antragsunterlagen oder der Vertragsdurchführung (Beiträge, Versicherungsfälle, Risiko-/Vertragsänderungen) ergeben, an Rückversicherer zur Beurteilung des Risikos und zur Abwicklung der Rückversicherung sowie an den HUK-Verband und andere Versicherer zur Beurteilung des Risikos und der Ansprüche übermittelt. Ich willige ferner ein, daß die Versicherer der ... Gruppe, soweit dies der ordnungsgemäßen Durchführung meiner Versicherungsangelegenheit dient, allgemeine Vertrags-, Abrechnungs- und Leistungsdaten in gemeinsamen Datensammlungen führen und an ihre Vertreter weitergeben. Gesundheitsdaten dürfen nur an Personen- und Rückversicherer übermittelt werden; an Vertreter dürfen sie nur weitergegeben werden, soweit es zur Vertragsgestaltung erforderlich ist. Auf Wunsch werden mir zusätzliche Informationen zur Datenübermittlung zugesandt."

#### 5.2.4 Einschränkung der Nachbarschaftsbefragungen durch die Auskunfteien

Die Praxis der Auskunfteien bei Nachbarschaftsbefragungen ist in der Öffentlichkeit heftig kritisiert worden. Das hat den Düsseldorfer Kreis veranlaßt, auf eine restriktive Anwendung dieser Methode der Datenerhebung hinzuwirken. Es konnten Absprachen darüber getroffen werden, daß Nachbarschaftsbefragungen in Fällen, in denen nicht auf sie verzichtet werden kann, auf folgende Angaben beschränkt werden: Wohnort, Aufenthaltsdauer, Größenordnung des Einkommens, Arbeitgeber, wirtschaftliche Verhältnisse.

Weiterhin wurde dem Düsseldorfer Kreis von den Auskunfteien zugesichert, daß Fragen nach einer persönlichen Beurteilung nicht gestellt würden und daß sich die betreffenden Rechercheure dem Befragten gegenüber auszuweisen sowie den Grund der Befragung zu offenbaren hätten.

#### 5.3 Weitere Formen der Zusammenarbeit

Neben den bundesweiten Abstimmungsgesprächen im Düsseldorfer Kreis bestehen von Fall zu Fall auch noch enge Kontakte zwischen den einzelnen Datenschutzaufsichtsbehörden der Länder. Diese enge Zusammenarbeit ist insbesondere erforderlich in bezug auf speichernde Stellen, die in mehreren Bundesländern tätig sind. Enge Kontakte sind aber auch notwendig, um Informationsströme, die die Ländergrenzen überschreiten, zurückverfolgen zu können (Woher kommen die Daten? Wohin gehen sie?). Auch diese Zusammenarbeit ist konstruktiv und erfolgreich.

6. Möglichkeiten zur Verbesserung des Datenschutzes

6.1 Novellierung des Bundesdatenschutzgesetzes

Nach fast 10jährigen Vorarbeiten wurde der Entwurf des BDSG im Jahre 1972 dem Deutschen Bundestag zur Beratung vorgelegt (Bundestags-Drs. VI/ 3826). Es bedurfte weiterer 5 Jahre, bis das Gesetz am 27. Januar 1977 verkündet werden konnte. Dazwischen lagen intensive Beratungen über Grundsatz- und Detailfragen in den zuständigen Ausschüssen des Bundestages. Außerdem war der Gesetzentwurf Gegenstand von zwei Anhörungen der Interessenvertreter von Wirtschaft, Verwaltung und der Betroffenen und machte die Anrufung des Vermittlungsausschusses erforderlich, um bezüglich der dennoch bestehenden unterschiedlichen Auffassungen in einigen Fragen (insbesondere der Ausgestaltung der staatlichen Datenschutzaufsicht für den Bereich der Wirtschaft) zu einem mehrheitsfähigen Kompromiß zu kommen.

Im Gesetzgebungsverfahren waren sich alle Beteiligten darüber im klaren, daß mit dem BDSG in vielfacher Hinsicht rechtliches Neuland betreten wurde. Die Praktikabilität des Gesetzes und seine unmittelbaren und mittelbaren Auswirkungen konnten insbesondere für den Bereich der Wirtschaft nicht vorhergesehen werden. Trotz der zunächst vorherrschenden Skepsis und Unsicherheit brachte die Anwendung des Gesetzes sowohl bei den Datenschutzaufsichtsbehörden als auch bei den speichernden Stellen keine wesentlichen Probleme. Es war insbesondere festzustellen, daß in der Praxis keine Sachverhalte von grundsätzlicher Bedeutung erkennbar wurden, die nicht be-

reits im Gesetzgebungsverfahren erörtert worden waren und - in welcher Form auch immer - ihren Niederschlag im Gesetz gefunden hatten.

Aus der relativ problemlosen Realisierung der staatlichen Datenschutzaufsicht erwuchs sehr schnell der Wunsch nach einer weiteren Verbesserung des Datenschutzrechts. Unter Verbesserung verstand man im wesentlichen eine Konkretisierung der im Gesetz enthaltenen Generalklauseln und eine Stärkung der Stellung der betroffenen Bürger (abgesehen von den speziell den öffentlichen Bereich betreffenden Änderungsvorschlägen). So legten die CDU/CSU-Bundestags-Fraktion im Januar und die SPD/F.D.P.-Fraktion im Februar 1980 Entwürfe zu einer BDSG-Novelle vor. Beide Entwürfe wurden in der 8. Legislaturperiode des Bundestages nicht mehr behandelt. Ihnen folgte im Jahr 1981 ein Regierungsentwurf, der in ca. 25 bis 30 Punkten eine Änderung des BDSG vorsah. Es ging dabei im wesentlichen um

- die Erweiterung des Dateibegriffs,
- die Einführung eines verschuldensunabhängigen Schadenersatzanspruchs,
- die Neugestaltung des Auskunftsrechts,
- die Erweiterung der Befugnisse der Datenschutzaufsichtsbehörden und
- die Stärkung der Position der betrieblichen Datenschutzbeauftragten.

Die Landesregierung stand und steht einer Fortschreibung des Datenschutzrechts grundsätzlich positiv gegenüber. Auch nach ihrer Auffassung müssen die vorgenannten Schwerpunkte eingehend diskutiert werden. Allerdings sollten im Novellierungsverfahren Anwendungspraxis und Erfah-

rungen der Datenschutzaufsichtsbehörden ausreichend gewürdigt werden. Das war 1982 nach Auffassung der Landesregierung nicht der Fall. Es war außerdem zu befürchten, daß die in der öffentlichen Diskussion aufgebauten sehr hohen Erwartungen der Bürger unter der damaligen Prämisse "keine grundlegende Änderung der Konzeption und Systematik des Gesetzes" nicht erfüllt werden würden. Von besonderer Bedeutung erschien der Landesregierung schließlich die Tatsache, daß in absehbarer Zeit eine weitere Novellierung des BDSG nicht vertretbar sein würde. Dies gebot ihr, einen besonders kritischen Maßstab an den damaligen Entwurf anzulegen.

Durch die weitere Entwicklung der Novellierungsbemühungen, die Vorlage neuer Entwürfe der Bundesregierung und der Opposition, die Ergebnisse der öffentlichen Anhörungen und die Reaktion in der Fachliteratur fühlt sich die Landesregierung in ihrer Auffassung bestätigt. Sie ist nach wie vor der Meinung, daß eine Änderung des BDSG nicht punktuell und unter einschränkenden Prämissen erfolgen sollte. Ihr ist aber bewußt, daß jede für den Bürger spürbare Erweiterung des Datenschutzes auch ein Mehr an staatlichem Eingriff in Abläufe der Wirtschaft bedeutet. Nur wenn dieser Aspekt in die Diskussion einbezogen wird, kann ihres Erachtens erreicht werden, daß die vermeintlichen und tatsächlichen Schwachstellen des Datenschutzrechts im Konsens mit allen Beteiligten ausgeräumt werden. Es erscheint ihr z. B. fraglich, ob die Bürger einen spezifischen Kündigungsschutz für betriebliche Datenschutzbeauftragte als erstrebenswerte Neuerung ansehen würden, wenn andererseits die Behauptung

unwidersprochen im Raum steht, daß das BDSG nicht verhindern kann, daß in vielen Betrieben gar keine betrieblichen Datenschutzbeauftragten bestellt werden bzw. sie ihre Aufgaben praktisch gar nicht wahrnehmen. Vor der Schaffung neuer Rechtsnormen sollte daher auch geprüft werden, durch welche Maßnahmen die Wirksamkeit der bereits bestehenden Regelungen im Interesse der Betroffenen nachhaltig verbessert werden kann.

Die Landesregierung wird, da anders als für den öffentlichen Bereich (vgl. Landesdatenschutzgesetz) hier die Gesetzgebungskompetenz beim Bund liegt, dessen Bemühungen um eine tatsächliche Verbesserung des Datenschutzes konstruktiv unterstützen. Sie beabsichtigt, sich besonders dafür einzusetzen, daß

- die Dokumentationspflichten bei einem Datenaustausch zwischen speichernden Stellen verschärft werden,
- im Bereich der Auftragsdatenverarbeitung die Vertragspartner zu einer genaueren Abgrenzung der Verantwortlichkeiten angehalten werden und daß
- die Zulässigkeit der Verarbeitung personenbezogener Daten außerhalb bestehender Vertragsverhältnisse konkreter geregelt wird.

Sie ist im übrigen der Auffassung, daß vor einer Kodifizierung neuer Tatbestände im BDSG stets geprüft werden sollte, ob nicht die Möglichkeit besteht, diese in bereichsspezifischen Regelungen mit zu erfassen. Sie verweist hier insbesondere auf den Medienbereich, wo durch den Bildschirmtext-Staatsvertrag medienpezifische Ergänzungen des allgemeinen Datenschutzrechts im privaten

Bereich geschaffen worden sind. In den Entwurf des Landesrundfunkgesetzes sind ebenfalls spezielle Datenschutzregelungen eingefügt worden. Auch in Sachbereichen, die in die Gesetzgebungskompetenz des Bundes fallen, wie z. B. das Versicherungs- und Kreditwesen und das Arbeitsrecht, sollte geprüft werden, ob der gebotene Datenschutz in den dort zur Verfügung stehenden bereichsspezifischen gesetzlichen Regelungen nicht mit erfaßt werden sollte.

## 6.2 Änderung der Organisationsform der Datenschutzaufsichtsbehörde

Zu der Frage nach einer Änderungsnotwendigkeit der bisherigen Organisationsform der Aufsichtsbehörde, insbesondere zu ihrer Zusammenführung mit der Dienststelle des Landesbeauftragten für den Datenschutz, hat die Landesregierung bereits im Zusammenhang mit der Beratung des 6. Tätigkeitsberichts des Landesbeauftragten für den Datenschutz Stellung genommen. Sie sieht insoweit keine Möglichkeiten zu konkreten Verbesserungen der Datenschutzaufsicht. Die Praxis hat gezeigt, daß eine Vielzahl spezieller Datenschutzfragen sowohl für den öffentlichen als auch den privatwirtschaftlichen Bereich von Bedeutung sind. Neben der Verringerung des Verwaltungsaufwandes dürfte eine solche Konzentration vor allem der Rechtssicherheit dienen.

Es hat sich ferner herausgestellt, daß Sachverhalte häufig gleichzeitig den öffentlichen und den privaten Bereich berühren. Dies ist insbesondere der Fall bei Datenübermittlungen zwischen öffentlichen und nichtöffentlichen Stel-

len. So sind beispielsweise unabhängig voneinander mehrere Behörden an den Landesbeauftragten für den Datenschutz herangetreten und haben um Mitteilung gebeten, ob sie dem Verlangen von Wirtschaftsauskunfteien entsprechen dürfen, durch Ausfüllen von Formblättern Auskünfte über persönliche Verhältnisse von Einwohnern zu geben. Hier konnte der Landesbeauftragte sowohl seiner Beratungspflicht gegenüber den öffentlichen Stellen nachkommen als auch als Aufsichtsbehörde sich unmittelbar um das Geschäftsgebahren der Auskunfteien kümmern (vgl. 3. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz, S. 43).

### 6.3 Anregungen der Wirtschaft und der Gewerkschaften

Die Bestrebungen des Bundes zur Novellierung des BDSG und die damit im Zusammenhang stehenden Fragen zur Verbesserung der Datenschutzaufsicht haben den Innenminister veranlaßt, Anfang des Jahres 1984 Interessenverbände der Wirtschaft, Industrie- und Handelskammern und Gewerkschaften im Lande anzuschreiben und um entsprechende Meinungsäußerungen zu bitten. Seitens der schleswig-holsteinischen Wirtschaft und der Gewerkschaften wurden keine konkreten Änderungswünsche geäußert, die über das hinausgehen, was in den Anhörungen auf Bundesebene vorgetragen worden ist.

7. Erkenntnisse über Versuche zur Einführung von  
Personalinformationssystemen

7.1 Datenschutz im Arbeitsverhältnis

Arbeitnehmer reagieren sehr datenschutzbewußt, wenn es um das Ob und Wie der Nutzung ihrer Personal- und Leistungsdaten im Arbeitsverhältnis geht, wie sich aus einer Vielzahl sehr engagiert vorgetragener Eingaben ergibt. Beispielhaft wird auf folgende typischen Sachverhalte verwiesen:

- Erheben und Speichern von Personaldaten im Zusammenhang mit sogenannten Einstellungsfragebögen (insbesondere Fragen nach bisherigen Krankheiten und familiären Verhältnissen),
- Weitergabe der Daten an Verlage, um den Mitarbeitern eine bestimmte Zeitschrift zukommen zu lassen (Angst vor verbandspolitischer Indoktrination),
- Übermittlung von Daten an Arbeitgeberverbände,
- Übermittlung von Daten an Versicherungsvermittler und Versicherungsgesellschaften, z. B. im Zusammenhang mit Gruppenversicherungsverträgen,
- Übermittlung von Daten an öffentliche Stellen, z. B. Träger von Sozialleistungen,
- Beantwortung von Anfragen von Auskunftsteilen,
- Weitergabe von Informationen an den neuen Arbeitgeber (auch im Rahmen branchenüblicher, zentraler Auskunftsdienste),

- Datenübermittlungen an Gewerkschaften, z. B. im Zusammenhang mit der Berechnung und Einziehung von Gewerkschaftsbeiträgen,
- Aufzeichnung privat geführter Telefongespräche,
- Nutzung der aus der Gleitzeiterfassung gewonnenen Daten,
- Bekanntgabe betriebsärztlicher Untersuchungsergebnisse,
- Bekanntgabe bestimmter Leistungsdaten, z. B. durch Führen sogenannter Rennlisten,
- Bekanntgabe der Gehaltsdaten eines Arbeitnehmers an den Betriebsrat; Personalakteneinsicht durch den Betriebsrat.

Die Aufsichtsbehörde hatte also zahlreiche Rechtsfragen im Zusammenhang mit der Nutzung von Personaldaten zu klären. In keinem einzigen Fall bezog sich die Eingabe eines Arbeitnehmers aber auf ein Personalinformationssystem als solches. Da die privaten Stellen, bei denen hier im Lande Personalinformationssysteme zum Einsatz kommen, fast ausschließlich der Anlaßaufsicht unterliegen, war es der Aufsichtsbehörde bisher aus rechtlichen Gründen verwehrt, die im Einsatz befindlichen Personalinformationssysteme unmittelbar zu prüfen.

Gleichwohl hat sie Erkenntnisse über die Art, die Leistungsfähigkeit, den Entwicklungsstand und den Verbreitungsgrad von Personalinforma-

tionssystemen aus Kontakten, Diskussionen, Vortragsveranstaltungen, Beratungsgesprächen mit Betrieben, betrieblichen Datenschutzbeauftragten, Verbänden, Gewerkschaften und Arbeitnehmern gewonnen. Ferner ist ihr aus Literatur und Rechtsprechung bekannt, welche rechtlichen, insbesondere datenschutzrechtlichen Fragen sich ergeben.

## 7.2 Definition der Personalinformationssysteme

Weder Gesetz und Rechtsprechung noch Literatur lassen einen allgemeingültigen Begriff für Personalinformationssysteme erkennen. Insbesondere kann eine Abgrenzung zur konventionellen Personalverwaltung nicht über den Einsatz technischer Hilfsmittel (Umfang der ADV-Unterstützung) oder über bestimmte Eignungskriterien des Systems, wie z. B. die Kontrollmöglichkeit, gefunden werden. Es erscheint daher sinnvoll, jedes System der teilweisen oder vollständigen geordneten Erfassung, Speicherung und Auswertung von Informationen über persönliche oder sachliche Verhältnisse der Arbeitnehmer, ungeachtet der dabei angewandten Verfahren, als Personalinformationssystem zu bezeichnen. Als Personalinformationssystem im engeren Sinne werden in der Literatur allerdings nur Systeme bezeichnet, die die für Zwecke der Personalführung, -steuerung und -planung erforderlichen Arbeitnehmerdaten vorhalten. Dazu gehören aber auch die in den unterschiedlichen Funktionsbereichen der Unternehmen bestehenden Teilinformationssysteme (z. B. für Produktion, Vertrieb, Verwaltung), die miteinander verkoppelt werden können. In der entsprechenden DV-Realisierungsstufe können auch sie ein umfas-

sendes Verwaltungs- und Planungsinstrument des Unternehmens bilden.

Da der schleswig-holsteinischen Datenschutzaufsichtsbehörde nicht bekannt war, ob Untersuchungen darüber bestehen, in welchem Umfang Daten über Arbeitnehmer im Informationssystem gespeichert werden, hat sie sich an Verbände, Gewerkschaften und Industrie- und Handelskammern gewandt und um entsprechende Informationen gebeten. Die Antworten lassen erkennen, daß die eingesetzten, sehr unterschiedlichen Systeme im allgemeinen folgende Funktionen abdecken:

- Personalverwaltung (Einstellung, Einstufung, Kündigung, Versetzung, Beförderung)
- Lohn- und Gehaltsabrechnung, Überstunden- und Spesenabrechnung
- Personaleinsatz
- Aus- und Fortbildung
- Personalbedarfsplanung
- Personalentwicklungsplanung
- Personalbeschaffungsplanung
- Zugangskontrolle
- Gleitzeiterfassung
- Anwesenheitskontrolle
- Telefondatenerfassung
- Kantinendatenerfassung
- Projektüberwachung/Budgetkontrolle
- Erfassung von Leistungsdaten für Fakturierung

Die bisher umfangreichste, bundesweite Erhebung über den Einsatz von Personalinformationssystemen in Großbetrieben hat allein für die Bereiche Personalverwaltung und -planung aufgezeigt, daß

durch die im Markt befindlichen Programmpakete bis zu 45 Einzelfunktionen erledigt werden können und daß die Unternehmen diese Einzelaufgaben im Rahmen ihrer Personalinformationssysteme weitgehend realisiert haben. So wickeln fast alle Betriebe die Lohn- und Gehaltsabrechnung, die Altersversorgung und die Führung der wichtigsten Personalstatistiken mit Hilfe der ADV ab (vgl. Wolfgang Kilian, Personalinformationssysteme in deutschen Großunternehmen, Ausbaustand und Rechtsprobleme, 1982, S. 41 ff.). Diese Gesamtsituation entspricht auch den Verhältnissen im Lande, wie die Befragung der Personalleiter von 24 Groß- und Mittelbetrieben (Unternehmensgrößen von ca. 200 bis 4000 Mitarbeiter) anlässlich einer Zusammenkunft im Arbeitskreis Personalwesen des Rationalisierungs-Kuratoriums der deutschen Wirtschaft ergeben hat. Nahezu alle Betriebe lösen ihre lohn- und gehaltstechnischen Fragen mit Hilfe der automatisierten Datenverarbeitung. Darüber hinaus hat jeder Betrieb, individuellen Bedürfnissen und Prioritäten angepaßt, weitere Personaldaten für Verwaltungs-, Planungs- und Kontrollaufgaben gespeichert. Lediglich in einem der befragten Betriebe geschah dies auf der Basis einer Betriebsvereinbarung im Rahmen eines in sich geschlossenen Personal-, Abrechnungs- und Verwaltungsinformationssystems. In den übrigen Betrieben hat man die für die Gehaltsabrechnung vorhandenen Verfahren punktuell um Aufgaben der Personalverwaltung, -planung und -kontrolle erweitert.

Die Entwicklung komplexer Personalinformationssysteme steckt also noch in den Anfängen. Die Betriebe haben an den unterschiedlichsten Stel-

len mit der Automatisierung begonnen, so daß der erreichte Stand noch sogenannten Insellösungen entspricht. Umfassende Systeme werden von verschiedenen Herstellerfirmen zwar angeboten, sind aber in Schleswig-Holstein kaum im Einsatz.

### 7.3 Die datenschutzrechtliche Problematik der Personalinformationssysteme

Die Personalinformationssysteme werden, je nach Standpunkt des Betrachters, als Herrschaftssysteme und als Verletzung der Waffengleichheit im Arbeitsverhältnis oder als unverzichtbare Planungs- und Verwaltungswerkzeuge bezeichnet.

Ihr Nutzen liegt auf der Hand. Er besteht in der Möglichkeit, bessere, wirtschaftlichere und auch für den Arbeitnehmer sachgerechtere Entscheidungen zu treffen. Von besonderer Bedeutung sind hierbei die mit den Systemen zu erzielenden Rationalisierungsgewinne. So sind z. B. die Arbeitgeber allein aufgrund gesetzlicher Auflagen verpflichtet, bis zu 214 Einzelangaben zur Person des Arbeitnehmers aufgrund von 126 Gesetzen und Verordnungen zu führen und bis zu 239 unterschiedliche Datenübermittlungen an 75 öffentliche Stellen aufgrund von 232 Rechtsvorschriften zu ermöglichen (vgl. Hentschel, Datenschutzberater 11/83, S. 9 ff.). In Anbetracht der Termine und Fristen und insbesondere der gesetzgeberischen Änderungsnotwendigkeiten kommt der Unternehmer allein in diesem Bereich kaum noch ohne DV-Einsatz aus.

Dem stehen die Befürchtungen vieler Arbeitnehmer gegenüber, daß sie durch die Nutzung der in die-

sen Systemen anfallenden Informationen Nachteile erleiden können. So sieht man bei einem umfassenden DV-Einsatz ein Übermaß an Kontrolle im betrieblichen und sogar außerbetrieblichen Bereich auf sich zukommen. Man befürchtet, daß Daten, die im Hinblick auf einen bestimmten Verwendungszweck offenbart werden, aufgrund ihrer multifunktionalen Eigenschaft losgelöst von ihrem ursprünglichen Verwendungszweck genutzt werden. Man sorgt sich darüber, daß einem das in der Kantine zum Mittagessen genossene Glas Bier, das im automatisierten Abrechnungsverfahren registriert wurde, bei nächster Gelegenheit vom Vorgesetzten vorgehalten wird. Die Einführung einzelner bzw. umfassender Informationssysteme wird oft als faktischer Zwang zur Datenentäußerung empfunden.

Wenn der Arbeitnehmer im Betrieb seine wie auch immer geartete Tätigkeit über einen Bildschirm bzw. mit Unterstützung eines Bildschirms abwickelt, sitzen die Ängste noch tiefer. Vom Redakteur einer Zeitung, über den online-arbeitenden Programmierer bis hin zur datenerfassenden Kraft werden die Befürchtungen geäußert, daß ihr Verhalten am Bildschirmarbeitsplatz zum Zweck einer offenen oder verdeckten Leistungsmessung im Detail analysiert werden kann. Durch die Möglichkeit, Verhaltensweisen in Leistungskurven zu erfassen oder Reaktionen auf bestimmte Ereignisse in Psychogramme zu verwandeln, fühlen sie sich in einem Bereich überwacht, der bei der bisherigen Produktion geistiger Leistungen in der Regel einer Einsichtsmöglichkeit von außen verborgen war.

Ob und inwieweit die geschilderten Ängste begründet sind, kann nach heutigem Erkenntnisstand nicht abschließend beantwortet werden. Die Möglichkeit, die Informationssysteme mißbräuchlich zu Lasten des Arbeitnehmers zu nutzen, sind allerdings theoretisch gegeben.

Der dem Arbeitnehmer durch bereichsspezifisches Recht und das BDSG gewährte Rechtsanspruch auf Schutz vor Beeinträchtigung seiner Belange im Zusammenhang mit jeglicher personenbezogener Informationsverarbeitung wird z. B. tangiert,

- wenn der Arbeitnehmer betrieblichen oder sogar außerbetrieblichen Kontrollmechanismen ausgesetzt wird, die nicht durch vertragliche oder gesetzliche Grundlagen abgedeckt sind,
- wenn Arbeitnehmerdaten ohne Rücksicht auf betriebliche Erfordernisse den verschiedensten Stellen zugänglich sind und ein an den Grundsätzen der Zweckbestimmung und Erforderlichkeit orientiertes Abschottungssystem nicht existiert oder
- wenn bewußte oder unbewußte Datenentäußerungen des Arbeitnehmers zu sachfremden Entscheidungen genutzt werden.

Der Arbeitnehmer steht jedoch nach heutigem Recht diesen Mißbrauchsmöglichkeiten nicht schutzlos gegenüber, wie auch unter Ziffer 8 des Berichts dargetan wird.

Den Zeitpunkt für eine abschließende Antwort auf die Frage, ob und inwieweit die heutigen Rechts-

grundlagen ausreichen, um die Datenschutzproblematik komplexer Informationssysteme im Arbeitsverhältnis zu erfassen, hält die Landesregierung aber noch nicht für gegeben. Zunächst sollten die Ergebnisse folgender Arbeiten abgewartet werden:

- Im Auftrage des Bundesministers für Arbeit und Sozialordnung ist von dem hessischen Datenschutzbeauftragten und Arbeitsrechtswissenschaftler Professor Dr. S. Simitis ein Gutachten erstellt worden zum Thema "Schutz von Arbeitnehmerdaten, Regelungsdefizite - Lösungsvorschläge". Dieses Gutachten ist 1979 im Hinblick auf eine mögliche Gesetzgebungsinitiative in Auftrag gegeben worden. Hintergrund war die Überlegung, daß das Bundesdatenschutzgesetz als Auffanggesetz bereichsspezifische Regelungserfordernisse im Arbeitsrecht nur unzureichend abdecken kann. Simitis kommt zu dem Ergebnis, daß eine besondere arbeitsrechtliche Regelung erforderlich ist. Eine Äußerung des Auftraggebers, ob er dieser Rechtsauffassung folgt und insbesondere ob eine entsprechende Regelung im Bereich des kollektiven Arbeitsrechts oder im allgemeinen Datenschutzrecht anzusiedeln sei, steht noch aus.
  
- Die im Auftrag des Deutschen Bundestages eingesetzte Enquete-Kommission "Neue Informations- und Kommunikationstechniken" wirft in ihrem Zwischenbericht vom März 1983 (Bundestags-Drs. 9/2442) die Frage nach der Notwendigkeit spezieller gesetzlicher Regelungen für den Aufbau und den Einsatz von Personal- oder sonstigen Informationssystemen auf. Hier fin-

det sich im Ergebnis die Tendenz, die gestiegene Schutzbedürftigkeit des Arbeitnehmers nicht über das Datenschutzrecht gewährleisten zu wollen. Das Datenschutzrecht sei nicht darauf ausgerichtet, auf die durch den Aufbau weitreichender innerbetrieblicher Informationssysteme geschaffene Machtverschiebung im Betrieb zu reagieren. Es sei primär Individualschutzrecht (Persönlichkeitsschutzrecht) und daher nicht ein Instrument zur Reaktion auf soziale Machtverschiebungen in einem Sozialbereich wie dem Betrieb.

- Letztere Überlegung gewinnt insbesondere Bedeutung vor dem Hintergrund des Urteils des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz. Nach Ansicht der Landesregierung wäre durch den Bundesgesetzgeber zu prüfen, ob und inwieweit die dortigen Ausführungen zum informationellen Selbstbestimmungsrecht - insbesondere zu den Grundsätzen der Erforderlichkeit und Zweckbindung - auch im Bereich der betrieblichen Informationssysteme ihre Wirkungen entfalten, insbesondere den Gesetzgeber verpflichten.

8. Individuelle und kollektive Kontrollrechte bei der Einführung und Nutzung von Personalinformationssystemen

Die Fragestellungen in bezug auf

- die lückenlose Information des Arbeitnehmers über seine im Betrieb gespeicherten Daten;
- die Möglichkeit für den Arbeitnehmer, jederzeit Einsicht in sein Datenregister nehmen zu können;
- die Zusicherung, daß falsche Daten gelöscht werden;
- die Sperrung von Daten, wenn deren Richtigkeit vom Arbeitnehmer bestritten wird und der Nachweis durch den Arbeitgeber nicht erbracht werden kann;
- die Mitbestimmung des Betriebsrates bei der Einführung des Personalinformationssystems;
- die Mitbestimmung des Betriebsrates bei der Bestellung des betrieblichen Datenschutzbeauftragten, um von vornherein ein Vertrauensklima zu gewährleisten,

lassen sich zusammengefaßt wie folgt beantworten:

8.1 Welche Benachrichtigungspflichten obliegen dem Arbeitgeber, welche Einsichtsrechte hat der Arbeitnehmer?

Grundsätzlich gelten auch für Personalinformationssysteme die datenschutz- und arbeitsrechtlichen Bestimmungen zum Schutz personenbezogener Daten im Arbeitsverhältnis.

Der Arbeitnehmer hat nach § 26 Abs. 1 BDSG ein Recht darauf, im Falle erstmaliger Datenspeicherung entsprechend informiert zu werden. Dieses Recht wird nicht durch das Betriebsverfassungsgesetz, z. B. durch das Akteneinsichtsrecht gemäß § 83 Abs. 1 BetrVG, ausgeschlossen. Die Benachrichtigungspflicht des Arbeitgebers entfällt allerdings (vgl. § 26 Abs. 1 BDSG), wenn der Arbeitnehmer auf andere Weise Kenntnis von der Datenspeicherung erlangt hat. Ob ein Arbeitnehmer von der Speicherung seiner Daten rechtlich wirksam "auf andere Weise" Kenntnis erhalten hat, kann nur im Einzelfall entschieden werden. Allgemein läßt sich die Feststellung treffen, daß z. B. bei denjenigen Daten, die der Arbeitnehmer im Personaleinstellungsfragebogen selbst geliefert hat oder bei den Lohn-, Gehaltsdaten und sonstigen Abrechnungsdaten, über die der Arbeitnehmer durch entsprechende EDV-Belege informiert wird, eine solche Kenntnisnahme unterstellt werden kann.

Ein allgemeines und umfassendes Einsichtsrecht in Personalakten folgt für die Arbeitnehmer bereits aus § 83 BetrVG und weiteren Bestimmungen. Es bezieht sich auch auf Personaldaten, die sich auf elektronischen Speichermedien in Personal-

informationssystemen finden. "Einsichtsrecht" bedeutet in diesem Zusammenhang, daß die gespeicherten Daten lesbar und dem Arbeitnehmer zugänglich zu machen sind. Das Auskunftsrecht nach § 26 Abs. 2 BDSG ist noch weitergehend, da der Arbeitnehmer auf diese Weise bei automatisierten Datenübermittlungen auch die regelmäßigen Empfänger der Daten erfährt.

8.2 Unter welchen Voraussetzungen kann ein Arbeitnehmer die ihn betreffenden Daten berichtigen, sperren oder löschen lassen?

Grundsätzlich gelten die in § 27 BDSG gewährten Rechte auf Berichtigung, Sperrung und Löschung der personenbezogenen Daten unter den dort genannten Voraussetzungen auch gegenüber den Betreibern betrieblicher Informationssysteme. Sie werden im Bereich der elektronischen Personaldatenverarbeitung nicht durch die Bestimmung des § 83 Abs. 2 BetrVG ausgeschlossen, wonach der Arbeitnehmer nur das Recht hat, Erklärungen dem Inhalt der Personalakte beifügen zu lassen. Allerdings ist nach herrschender Auffassung in der Literatur das Recht auf Sperrung von Daten nach § 27 Abs. 2 Satz 1 BDSG ausgeschlossen durch die spezialgesetzliche Regelung im Betriebsverfassungsgesetz. Das Recht, die Personalakte durch die Abgabe eigener Erklärungen ergänzen zu können, deckt den Sachverhalt ab, daß der Arbeitnehmer die Richtigkeit bestimmter Daten bestreitet, daß aber weder er noch der Arbeitgeber die Richtigkeit bzw. die Unrichtigkeit feststellen können.

8.3 Welche Mitbestimmungsrechte des Betriebsrates gibt es im Bereich der Verarbeitung von Arbeitnehmerdaten, bei der Einführung von Informationssystemen, bei der Bestellung des betrieblichen Datenschutzbeauftragten?

Die Frage nach dem Umfang und der Ausgestaltung der betrieblichen Mitbestimmung berührt die eigentlichen Datenschutzprobleme der Personalinformationssysteme nur noch mittelbar. Datenschutz ist in erster Linie Individualrechtsschutz und nicht als Instrument gedacht, die Probleme kollektiver betrieblicher Anhörungs- und Mitwirkungsrechte zu lösen. Es soll in diesem Bericht lediglich referierend die Mitbestimmungsproblematik in ihren wichtigsten Grundzügen unter Berücksichtigung der hierzu ergangenen Rechtsprechung dargestellt werden.

Im Betriebsverfassungsgesetz sind keine ausdrücklichen Mitbestimmungsrechte in datenschutzrechtlichen Fragen vorgesehen. Das gilt auch für die Planung, Ausgestaltung, Einführung und Weiterentwicklung betrieblicher Personalinformationssysteme. Gleichwohl mehren sich in Rechtsprechung und Literatur Stimmen, die ein Mitbestimmungsrecht des Betriebsrates beim Einsatz sogenannter Personalinformationssysteme bejahen (vgl. NJW 83, 920).

In diesem Zusammenhang wird u. a. auf folgende Rechtsprechung verwiesen:

- "Dem Antragsgegner (Gesamtbetriebsrat) steht bei der Einführung und Anwendung des Personalabrechnungs- und Informationssystems PAISY

ein Mitbestimmungsrecht gemäß § 87 Abs. 1 Ziff. 6 BetrVG zu." (Arbeitsgericht Karlsruhe, Beschluß vom 27.01.1983 in Betrieb 1983, 1211)."

- "Mitbestimmungsrecht des Betriebsrats bei Einführung und Anwendung von Personalinformationssystemen (PAISY)" (Landesarbeitsgericht Frankfurt/ M., Beschluß vom 01.09.1983, Datenschutz und Datensicherung 2/84, S. 144 ff.)."
  
- "Diese Rechtsprechung ist nunmehr durch zwei richtungsweisende Entscheidungen des Bundesarbeitsgerichts zur Frage des Mitbestimmungsrechts des Betriebsrates gemäß § 87 Abs. 1 Nr. 6 BetrVerfG bestätigt worden. In der Entscheidung vom 6. Dezember 1983 (AZ 1 ABR 43/81) hatte das BAG entschieden, daß bereits das Erheben von Daten durch technische Einrichtungen über das Verhalten oder die Leistung von Arbeitnehmern den Mitbestimmungstatbestand ausfüllt; nunmehr wurde das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVerfG durch die Entscheidung des BAG vom 14. September 1984 (AZ 1 ABR 23/82) auch für das technische Verarbeiten von Daten über das Verhalten oder die Leistung von Arbeitnehmern bejaht. Somit ist beim Einsatz technischer Einrichtungen im Hinblick auf eine objektiv größere Gefährdung für das Persönlichkeitsrecht des Arbeitnehmers der Mitbestimmungstatbestand bereits erfüllt, ohne daß es auf die subjektive Absicht des Arbeitgebers ankommt, diese Daten auch für einen Leistungsvergleich zu erheben oder zu nutzen. Im einzelnen gilt folgendes:

- Das Vorliegen technischer Überwachung im Sinne von § 87 Abs. 1 Nr. 6 BetrVerfG hat das Bundesarbeitsgericht immer angenommen, wenn durch die technische Einrichtung Daten über das Verhalten oder Leistung der Arbeitnehmer erhoben werden. Auf eine Absicht des Arbeitgebers, diese Daten zur Überwachung zu erheben oder zu nutzen, kommt es nicht an.
  
- Ob Verhaltens- oder Leistungsdaten erhoben werden, bestimmt sich nach dem im System zur Anwendung gelangenden Programm. Nur die Verwendung eines Programmes vermag zu begründen, daß eine Einrichtung dazu bestimmt ist, das Verhalten oder die Leistung von Arbeitnehmern zu überwachen.
  
- Eine technische Überwachung liegt auch vor, wenn bereits vorhandene - auch in herkömmlicher Weise - erhobene Verhaltens- oder Leistungsdaten mittels einer technischen Einrichtung zu Aussagen über das Verhalten oder die Leistung von Arbeitnehmern verarbeitet werden. Ob dies der Fall ist, bestimmt sich wiederum nach dem zur Anwendung gelangenden Programm. Daß das so erstellte Verhaltens- oder Leistungsbild von der technischen Einrichtung auch beurteilt, d. h. mit einer vorgegebenen Sollnorm verglichen wird, ist nicht erforderlich.

Indem das Bundesarbeitsgericht in datenschutzfreundlicher Auslegung des § 87 Abs. 1 Ziff. 6 BetrVerfG den Mitbestimmungstatbestand bei technischen Einrichtungen bereits an den Erhebungs- oder Verarbeitungsvorgang anknüpft - ohne auf

einen konkreten Leistungsvergleich durch den Arbeitgeber abzustellen - hat es in der Überwachung von Arbeitnehmerverhalten im Zusammenhang mit technischen Einrichtungen eine größere Gefährdung für das Persönlichkeitsrecht der Arbeitnehmer gesehen als bei einer Überwachung mit bloßen herkömmlichen Mitteln. Für die weitere Entwicklung, Einführung und den Betrieb von Personalinformationssystemen ist daher die BAG-Entscheidung vom 14. September 1984 von gravierender Bedeutung.

Nach herrschender Meinung unterliegt die Bestellung des betrieblichen Datenschutzbeauftragten nicht der Mitbestimmung des Betriebsrates. Insbesondere im Zusammenhang mit der Diskussion um die Novellierung des Bundesdatenschutzgesetzes sind Stimmen laut geworden, dem Betriebsrat ein Mitbestimmungsrecht bei der Auswahl und Abberufung des betrieblichen Datenschutzbeauftragten einzuräumen. Der schleswig-holsteinischen Aufsichtsbehörde für den Datenschutz sind aus der Prüfungspraxis und den sonstigen Kontakten heraus keine Fälle bekanntgeworden, in denen es aufgrund fehlender Mitbestimmung des Betriebsrates nicht zu einer vertrauensvollen Zusammenarbeit zwischen Betriebsrat und betrieblichen Datenschutzbeauftragten gekommen ist. Dennoch wird nicht verkannt, daß die Stellung des betrieblichen Datenschutzbeauftragten deshalb besonders schwierig ist, weil er sowohl die Unternehmensleitung bei der Erfüllung der datenschutzrechtlichen Verpflichtungen zu unterstützen hat, als auch die Interessen eines Arbeitnehmers z. B. im Bereich der Personaldatenver-

arbeitung gegenüber der Geschäftsleitung zu vertreten hat. Ihm eine möglichst unabhängige Stellung im Betrieb zu verschaffen, war und ist die Absicht des Datenschutzgesetzgebers. Es wird daher im Rahmen der Novellierungsüberlegungen zum BDSG erwogen, zusätzlich zu dem bereits gesetzlich verankerten Gebot der Weisungsfreiheit und dem Benachteiligungsverbot eine zusätzliche dritte Absicherung des betrieblichen Datenschutzbeauftragten einzuführen. Die Bestellung zum Datenschutzbeauftragten soll danach nur in entsprechender Anwendung von § 626 BGB (fristlose Kündigung aus wichtigem Grund) widerrufen werden können.