13. Wahlperiode

Drucksache **13/2650**

HESSISCHER LANDTAG

19. 08. 92

28 Seiten

Vorlage der Landesregierung

betreffend den Fünften Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden

Vorgelegt mit der Stellungnahme zum Zwanzigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten – Drucks. 13/1756 – nach § 30 Abs. 2 des Hessischen Datenschutzgesetzes vom 11. November 1986.

Eingegangen am 19. August 1992 · Ausgegeben am 10. September 1992

Herstellung: Johannes Weisbecker, 6000 Frankfurt am Main · Auslieferung: Kanzlei des Hessischen Landtags · Postf. 3240 · 6200 Wiesbaden 1

Inhaltsverzeichnis

		Seite
1.	Bearbeitung von Beschwerden gegen Stellen, die personenbezogene Daten nach § 28 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) für die Erfüllung eigener Geschäftszwecke verarbeiten	5
2.	Bearbeitung von Beschwerden gegen Stellen, die nach § 32 Abs. 1 Nr. 1–3 BDSG geschäftsmäßig personenbezogene Daten verarbeiten oder nutzen	5
3.	Bearbeitung von Anfragen zu Problemen des Datenschutzes	5
4.	Von Amts wegen durchgeführte Überprüfungen von Stellen, die nach § 32 Abs. 1 Nr. 1–3 BDSG geschäftsmäßig personenbezogene Daten verarbeiten oder nutzen	6
4.1	Meldepflicht nach § 32 BDSG	6
4.2	Register	6
4.3	Prüfungsbericht	6
5.	Kreditkartenunternehmen	7
6.	Wirtschaftsauskunfteien	9
6.1	Allgemeines und Entwicklung der Branche	9
6.2	Darlegung und Dokumentation des berechtigten Interesses nach § 29 Abs. 2 Ziffer 1a BDSG	10
6.3	Dokumentation der Eingaben und Datenquellen	11
6.4	Rechte der Betroffenen, insbesondere das Recht auf Auskunft	11
6.5	Speicherung geschätzter personenbezogener Daten	13
6.6	Wechselprotestlisten	13
6.7	SCHUFA	14
7.	Werbewirtschaft	15
8.	Versand- und Einzelhandel	15
8.1	Versandhandel	15
8.2	Einzelhandel	16
9.	Aktienrecht	17
10.	Versicherungen	17
11.	Banken	17
12.	Vereine	18
13.	Auslandsdatenverarbeitung	18
14.	Arbeitnehmerdatenschutz	20
15.	Datenverarbeitung im medizinischen Bereich	21
15.1	Rechtsgrundlagen	21
15.2	Datenübermittlung an ärztliche Verrechnungsstellen	21
15.3	Diagnoseangabe auf Rechnungen	21
15.4	Behandlung von Patientendaten bei der Praxisaufgabe und beim Austausch zwischen Ärzten	22
15.5	Datenschutz im Krankenhaus	23
16.	Betrieblicher Datenschutzbeauftragter	23
17.	Datensicherung	25

17.1 Zugangskontrolle 25
17.2 Zugriffskontrolle 25
17.3 Eingabekontrolle 26
17.4 Datenträgerkontrolle 26
17.5 Auftragskontrolle 27
17.6 Organisationskontrolle 27
18. Ordnungswidrigkeitenverfahren 28

1. Bearbeitung von Beschwerden gegen Stellen, die personenbezogene Daten nach § 28 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) für die Erfüllung eigener Geschäftszwecke verarbeiten

Die Anzahl von Beschwerden gegen Stellen, die Datenverarbeitung für die Erfüllung eigener Geschäftszwecke betreiben, ist im Berichtsjahr gegenüber den Vorjahren angestiegen:

Bei den Aufsichtsbehörden gingen 94 Beschwerden ein.

Die Beschwerden betrafen

- Versicherungen in 11 Fällen,
- Kreditinstitute in 12 Fällen,
- das Gesundheitswesen (Ärzte- und Krankenhäuser) in 9 Fällen,
- den Einzelhandel in 7 Fällen,
- Kreditkartenunternehmen in 6 Fällen,
- den Versandhandel in 6 Fällen,
- Inkassounternehmen in 5 Fällen,
- Verlage in 3 Fällen,
- Rechtsanwälte in 2 Fällen,
- sonstige Unternehmen in 33 Fällen.

In 20 Fällen waren die Beschwerden begründet, davon in 4 Fällen gegen den Einzelhandel, in je 3 Fällen gegen Inkassounternehmen und im Gesundheitsbereich, in je 2 Fällen gegen Kreditinstitute und Versicherungen sowie in 6 Fällen gegen sonstige Unternehmen. Bei 4 Beschwerden konnte nicht mehr abschließend festgestellt werden, ob die Datenverarbeitung in zulässiger oder in unzulässiger Art und Weise erfolgt ist. In 19 Fällen sind die Ermittlungen der Aufsichtsbehörde noch nicht abgeschlossen. Bei weiteren 6 noch aus dem Vorjahr übernommenen Beschwerdefällen waren 2 Beschwerden – gegen ein Kreditkartenunternehmen und eine Vermögensberatungsgesellschaft – begründet, 4 Beschwerden stellten sich als unbegründet heraus.

2. Bearbeitung von Beschwerden gegen Stellen, die nach § 32 Abs. 1 Nr. 1 – 3 BDSG geschäftsmäßig personenbezogene Daten verarbeiten oder nutzen

Im Berichtsjahr sind die Beschwerden gegen Stellen, die personenbezogene Daten geschäftsmäßig verarbeiten, im Verhältnis zu den Vorjahren auf 49 Beschwerden stark angestiegen. Alle Beschwerden führten zu einer Überprüfung durch die Aufsichtsbehörde.

Die Beschwerden betrafen

- Kreditinformationsdienste (Wirtschaftsauskunfteien und SCHUFA) in 46 Fällen
- Adreßhändler in 3 Fällen.

17 Beschwerden gegen Kreditinformationsdienste waren begründet. Bei 5 Beschwerden gegen Kreditinformationsdienste und einer Beschwerde gegen einen Adreßhändler sind die Ermittlungen der Aufsichtsbehörde noch nicht abgeschlossen.

3. Bearbeitung von Anfragen zu Problemen des Datenschutzes

Im Berichtsjahr wurden von den Aufsichtsbehörden zahlreiche schriftliche und mündliche Anfragen betroffener Bürger, Betriebsräte, Datenschutzbeauftragter und Unternehmen zu Fragen des Datenschutzes bei den verschiedensten datenverarbeitenden Stellen beantwortet. Häufig wurden die Aufsichtsbehörden von datenverarbeitenden Stellen um die Begutachtung geplanter Verfahren gebeten. Dadurch sollte sichergestellt werden, daß die Verfahren den Datenschutzbestimmungen entsprechen und kostspielige Fehlinvestitionen vermieden werden. Oft konnten die Aufsichtsbehörden dabei Möglichkeiten aufgezeigen, durch die datenschutzrechtlich kritische Verarbeitungen oder Nutzungen von personenbezogenen Daten verhindert werden konnten. Häufig bestand der Rat darin, die gar nicht erst in Betracht gezogene Einwilligung des Betroffenen zu erbitten, um die sonst unzulässige Datenverarbeitung doch noch zu ermöglichen. So fragte der Herausgeber eines Gästemagazins, welches

regelmäßig an den Kiosken und im Buchhandel einer Kurstadt verkauft wird, bei der Aufsichtsbehörde an, ob die regelmäßige Veröffentlichung von Namen, Wohnort und Adresse, Tag der Anreise sowie Unterkunft – Hotel oder Klinik – zulässig sei. Er hatte beabsichtigt, diese Daten von der Kurverwaltung zu übernehmen. Die Aufsichtsbehörde konnte in diesem Fall die datenschutzrechtlichen Bedenken der Kurverwaltung nur bestätigen.

Zumindest einem Teil der Kurgäste dürfte es nicht angenehm sein, als Patient einer Kur- oder Rehabilitationsklinik öffentlich bekannt gemacht zu werden. Außerdem könnte die Veröffentlichung der Heimatadresse zu Einbrüchen in die unbeaufsichtigte Wohnung anregen. Da bei einer einheitlichen Veröffentlichung aller Kurgäste nicht feststellbar ist, in welchem Einzelfall ein überwiegendes Interesse am Unterlassen der Veröffentlichung besteht, ist die Einwilligung aller Gäste erforderlich.

Schließlich ist noch bemerkenswert, daß bei der beratenden Tätigkeit der Aufsichtsbehörden die Auslandsdatenverarbeitung eine wachsende Rolle spielte.

4. Von Amts wegen durchgeführte Überprüfungen von Stellen, die gemäß § 32 Abs. 1 Nr. 1–3 BDSG geschäftsmäßig personenbezogene Daten verarbeiten oder nutzen

4.1 Meldepflicht nach § 32 BDSG

Nach § 32 Abs. 1 BDSG haben die Stellen, die personenbezogene Daten geschäftsmäßig zum Zwecke der personenbezogenen oder der anonymisierten Übermittlung speichern oder sie im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen, sowie ihre Zweigniederlassungen und unselbständigen Zweigstellen die Aufnahme und Beendigung ihrer Tätigkeit der zuständigen Aufsichtsbehörde innerhalb eines Monats mitzuteilen. Wie bereits im Vorjahresbericht festgestellt, besteht insbesondere im Bereich der verbundenen Unternehmen und der Konzerne nicht immer Klarheit über die Meldepflicht, wenn auch der Informationsstand spürbar gestiegen ist. Eine Erleichterung sowohl für die Unternehmen als auch für die Aufsichtsbehörden ist durch die Novellierung des Bundesdatenschutzgesetzes insoweit eingetreten, als zum einen nicht mehr sämtliche Angaben in das von jedermann einsehbare Register der Aufsichtsbehörden aufgenommen werden, zum anderen die zuständige Aufsichtsbehörde im Einzelfall den Umfang bestimmter Angaben festlegen kann. Damit soll unnötiger Verwaltungsaufwand auf beiden Seiten reduziert werden.

In Einzelfällen wurde von dieser Regelungsmöglichkeit bereits Gebrauch gemacht, so zum Beispiel bei Stellen, die Daten an eine Vielzahl regelmäßiger Empfänger herausgeben und ständig in größerem Umfang neue regelmäßige Datenempfänger hinzugewinnen. Hier konnte die Meldehäufigkeit durch Feststellung bestimmter Meldestichtage, zum Beispiel zum Quartalsende, reduziert werden und in den Fällen, in denen der Empfängerkreis ohnehin von Anfang an offen ist, auf die Nennung einzelner Empfängerdaten verzichtet werden. Der Registrieraufwand wurde damit erheblich verringert. Vereinfachende Festlegungen dieser Art können allerdings nur solange gewährt werden, als die Aufsichtsbehörde bei ihren regelmäßigen oder fallweisen Überprüfungen eine ordnungsgemäße Dokumentation, insbesondere auch im Bereich der Onlineübermittlungen feststellen kann.

4.2 Register

Zur Zeit sind zu dem nach § 38 Abs. 2 BDSG geführten Register 544 Unternehmen gemeldet.

4.3 Prüfungsübersicht

Im Berichtsjahr 1991 wurden 86 Prüfungen nach § 38 BDSG, bzw. vor dem 1. Juni nach § 40 BDSG a.F. durchgeführt. Davon betrafen Datenverarbeiter nach § 38 Abs. 2 Satz 1 Ziffer 3 BDSG insgesamt 53, nämlich

- Servicerechenzentren 28, davon allein für Konzernunternehmen 5
- Datenerfasser 10
- Telemarketingunternehmen 5
- Mikroverfilmer 4

– Datenträgervernichter 4
– Schreibbüros 2.

Des weiteren wurden 7 Kreditinformationsdienste und 10 Adreßverlage sowie 8 Unternehmen aus dem Bereich der Markt- und Meinungsforscher und 8 sonstige geprüft.

Diese Prüfungen brachten folgendes Ergebnis:

– Beanstandungen 52
– Empfehlungen 22
– ohne wesentliche Beanstandungen 8.

In 4 Fällen wurde während der Prüfung festgestellt, daß das Unternehmen keine meldepflichtige Tätigkeit ausübt.

Folgende wesentliche Mängel wurden am häufigsten festgestellt:

1. Keine bzw. verspätete oder unvollständige Registermeldung nach § 32 BDSG
2. Keine bzw. unwirksame Bestellung des betrieblichen Datenschutzbeauftragten
3. Keine Aus- und Fortbildung des betrieblichen Datenschutzbeauftragten
4. Keine ausreichende Wahrnehmung der Aufgaben durch den betrieblichen Datenschutzbeauftragten, d.h. keine oder mangelhafte Schulung/Unterrichtung der Mitarbeiter, keine oder mangelhafte Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme
5. Keine bzw. unzureichende Verpflichtung nach § 5 BDSG (Datengeheimnis)
6. Unzureichende Zugangskontrolle (Raum- und Objektsicherung)
7. Unzureichende Datenträgerverwaltung
8. Unzureichende Auftragskontrolle (keine schriftlichen Verträge)
9. Unzureichende Eingabe und Zugriffskontrolle (Passwort)
10. Unzureichende Dokumentation

In diesem Berichtszeitraum haben die Aufsichtsbehörden erstmalig Unternehmen, bei denen aufgrund einer Datenschutzüberprüfung die Beseitigung von Mängeln gefordert worden war, unangemeldet zur Nachkontrolle aufgesucht.

Das Ergebnis war überwiegend negativ. Trotz ausführlicher Aufklärung der Unternehmen sind die bestehenden Mängel nicht beseitigt worden. Als Grund wurde Arbeitsüberlastung angegeben. In einem Fall bestand nach wie vor die Möglichkeit, Computerauswertungen unbemerkt aus dem Rechenzentrum zu entfernen. Unangemeldete Nachkontrollen soll es zukünftig in erhöhtem Maße geben. Erforderlichenfalls wird hier von der Möglichkeit Gebrauch gemacht werden, Maßnahmen bindend anzuordnen.

5. Kreditkartenunternehmen

Im Vergleich zu den Vorjahren hat die Anzahl der Beschwerden gegen Kreditkartenunternehmen im Berichtsjahr stark abgenommen.

Die weitere Verbreitung von Kreditkarten hatte jedoch eine erhebliche Ausweitung der Kriminalität im Zusammenhang mit Kreditkarten zur Folge. Um das Schadensrisiko einzudämmen, wurden von einem großen Kreditkartenunternehmen die vertraglichen Beziehungen zu den kontenführenden Kreditinstituten in der Weise abgeändert, daß zukünftig nicht mehr das Kreditkartenunternehmen, sondern das Kreditinstitut für alle, auch betrügerisch veranlaßten Kreditkartenumsätze, z.B. bei Verlust oder Diebstahl der Kreditkarte, eintreten muß. Der gutgläubige Kreditkartenkunde selbst haftet wie bisher lediglich für einen Betrag bis zu 100 DM. Diese Risikoverlagerung ging von dem Gedanken aus, daß das kontoführende Kreditinstitut, also regelmäßig die Bank des Kartenkunden, näher am Kunden sei, von daher auch dessen Bonität besser einschätzen könne und besser in der Lage sei, Risikofälle rechtzeitig zu erkennen.

Wo früher das Kartenunternehmen aufgrund der Einwilligungserklärung im Kartenantrag selbst eine Schufaauskunft über den Betroffenen Kar-

tenantragsteller sowie eine bankübliche Auskunft bei dessen Kreditinstitut einholte, bevor es die Karte ausgab, verschafft sich jetzt das Kreditinstitut selbst aufgrund der ihm bereits im Kontoführungsvertrag in aller Regel eingeräumten Erlaubnis des Bankkunden Einblick in die bei der Schufa geführten Daten über den Kartenbewerber. Diese Informationen zusammen mit den Kenntnissen des Kreditinstituts aufgrund der Bankverbindung zum Kunden bilden nun die Grundlage für das Kreditinstitut, dem Kreditkartenunternehmen die Ausstellung einer Kreditkarte unter gleichzeitiger Angabe eines vorläufigen Bonitätsrahmens für diesen Kunden zu empfehlen. Das Kreditkartenunternehmen seinerseits ist verpflichtet, das Kreditinstitut des Kunden von drohenden Überschreitungen des Bonitätsrahmens innerhalb eines Abrechnungsintervalls in Kenntnis zu setzen, insbesondere wenn, was erfahrungsgemäß kritisch zu bewerten ist, erhebliche Bargeldumsätze per Karte getätigt wurden.

Die zuständige Datenschutzaufsichtsbehörde wurde bei dieser Neugestaltung der Haftungsverhältnisse und damit auch der Datenaustauschbeziehungen hinzugezogen und um ihre Stellungnahme gebeten. Datenschutzrechtlich bestanden gegen diese Änderung keine grundsätzlichen Bedenken. Das betroffene Kreditkartenunternehmen bzw. seine Servicegesellschaft wird nunmehr – wie dies bereits bei anderen großen Kartenherausgebern der Fall ist – bei der Verwaltung und Verarbeitung der Kreditkartendaten auch im Auftrag der kontenführenden Banken tätig. Datenübermittlungen, die nach dem Bundesdatenschutzgesetz begrifflich nur zwischen der speichernden Stelle und einem Dritten stattfinden können, liegen damit nicht vor. Die gleichwohl hier anzunehmende Nutzung von personenbezogenen Daten, die den gleichen Regeln unterliegt wie die Übermittlung, wird sowohl auf dem Weg zwischen Bank und Kartenunternehmen als auch in umgekehrter Richtung durch berechtigte Interessen der Beteiligten legitimiert. Demgegenüber sind schutzwürdige Interessen des Betroffenen, also des Kreditkartenkunden, an dem Ausschluß dieser Nutzung kaum denkbar. Dies gilt um so mehr, als der Anlaß für die Meldung von Kartenumsätzen durch das Kreditkartenunternehmen an die Bank auf mögliche Überschreitungen des Bonitätsrahmens beschränkt ist und auch in diesem Fall nicht Einzelumsätze, sondern nur die jeweilige Gesamtsumme von Barumsatz bzw. Händlerumsatz genannt wird. Die Summe dieser Umsätze erfährt das Kreditinstitut ohnehin auch jetzt schon zum Zeitpunkt der Monatsabrechnung mit der Lastschrift des Kreditkartenunternehmens.

Es erwies sich jedoch als schwierig, diese rechtlichen Zusammenhänge dem Kartenkunden verständlich zu machen. An den zahlreichen Anfragen, die bei der Aufsichtsbehörde eingingen, wurde vielmehr deutlich, daß nur wenige Kartenkunden die Bedeutung der Einwilligungsklauseln aus dem Kartenantrag, die den Datenaustausch zwischen Kartenunternehmen, Schufa und Banken regeln, richtig verstanden haben.

Das Mißtrauen von Kartenkunden hinsichtlich eines großzügigen Austausches von Daten zeigte sich in einem weiteren Beschwerdefall. Ein Betroffener beklagte sich darüber, daß seine gesamten Reisebuchungsdaten einschließlich der Daten einer Mitreisenden durch das in Anspruch genommene Reisebüro und über dessen Reservierungssystem an das Kreditkartenunternehmen übermittelt worden waren.

Derartige Übermittlungen können zweckmäßig sein, wenn ein Unternehmen über eine Firmenkarte für seine Mitarbeiter Geschäftsreisen bucht und die Daten für Abrechnungszwecke sofort in die Unternehmensbuchhaltung übernommen werden sollen. Bei der Nutzung privater Kreditkarten ist allerdings zu fragen, ob das Kreditkartenunternehmen tatsächlich wissen muß, daß der Karteninhaber X mit Frau Y zum Beispiel eine Reise in die USA mit Anschlußflug nach Hawai gebucht hat. Für die Monatsabrechnung des Privatkunden hätte es durchaus ausgereicht, wenn das Buchungsdatum, das Reisebüro und der Reisepreis vermerkt worden wären. Umfangreiche Speicherungen bzw. Übermittlungen sind lediglich für die Reisevertragspartner zur Abwicklung der Reiseleistungen erforderlich, nicht jedoch für das Kreditkartenunternehmen.

Änderungen dieses Verfahrens sind jedoch schwer durchzusetzen, da die Abläufe international zwischen den beteiligten Unternehmen standardisiert sind. Es zeigte sich jedoch gerade an diesem Fall, daß oft bedenkenlos ein weit größerer Umfang an Daten erhoben und verarbeitet wird, als für die eigentlich zu erbringenden Leistungen erforderlich wäre.

In einem weiteren Fall hatte ein Betroffener einer anderen Person eine Zweitkreditkarte ausstellen lassen. Bei der Zweitkreditkarte, die oft für Ehepartner oder andere Verwandte ausgestellt wird, erfolgt die Abrechnung der Kartenumsätze allein über die Bankverbindung des Hauptkarteninhabers. Dieser haftet nach den Vertragsbedingungen als Gesamtschuldner für alle Umsätze sowohl der Hauptkarte als auch der Zweitkarte. Im Beschwerdefall hatte der Zweitkarteninhaber erhebliche Kartenumsätze getätigt, für die der Hauptkarteninhaber nicht eintreten wollte. Mahnungen des Kreditkartenunternehmens, das überzogene Kreditkartenkonto unverzüglich auszugleichen, leitete er daher an den Zweitkarteninhaber weiter. Auch auf einen gerichtlichen Mahnbescheid hin reagierte er nicht. Das Kreditkartenunternehmen kündigte daraufhin sowohl die Haupt- als auch die Zweitkarte und meldete diese Kündigung der Schufa. Der Betroffene war der Ansicht, daß die Eintragung der Kreditkartenkündigung unter seinem Namen zu Unrecht erfolgt war.

Aufgrund der gesamtschuldnerischen Haftung, die der Betroffene auch für die Zweitkarte übernommen hatte, war jedoch sowohl die Kreditkartenkündigung als auch die darauffolgende Meldung an die Schufa rechtens. Die Aufsichtsbehörde nahm den Fall allerdings zum Anlaß, das Kreditkartenunternehmen auf die Notwendigkeit einer besseren Aufklärung des Hauptkarteninhabers über die mit der Übernahme der gesamtschuldnerischen Haftung für die Zweitkarte auf sich genommenen Risiken hinzuweisen. Allein aufgrund der knappen Ausführungen in den Kartenanträgen wird nicht jedem Hauptkarteninhaber klar sein, daß er in solchen Fällen sogar das Risiko eingeht, Negativeintragungen in seinem Schufadatenbestand zu erhalten.

6. Wirtschaftsauskunfteien

6.1 Allgemeines und Entwicklung der Branche

Im Berichtsjahr hat sich die Anzahl der Beschwerden gegen Wirtschaftsauskunfteien und Kreditinformationsdienste stark erhöht.

Eine Vielzahl dieser Beschwerden betraf allerdings eine einzige Auskunftei, die aufgrund der Aufforderung durch die Aufsichtsbehörde bisher versäumte Benachrichtigungen von Betroffenen über die Tatsache der Speicherung ihrer Daten bei der Auskunftei nachholen mußte (siehe Ziffer 6.1 des 4. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Landtagsdrucksache 13/584). Aus dem Inhalt dieser Beschwerden und dem Presseecho, das dieser Angelegenheit folgte, kann nur geschlossen werden, daß in weiten Teilen der Bevölkerung kaum Kenntnisse über die Arbeitsweise und die rechtlichen Grundlagen der Auskunfteien vorhanden sind. Immer wieder wurde die Frage gestellt, ob es denn rechtlich zulässig sei, daß eine Auskunftei ohne Einwilligung des Betroffenen Daten speichern und weitergeben dürfe. Anlaß zur Einschaltung der Aufsichtsbehörde gab allerdings oft auch die durch die eingeholte Selbstauskunft bestätigte Speicherung und Übermittlung völlig unzutreffender Daten (hierzu weiter unten).

Der Anstieg der Fallzahlen liegt allerdings auch daran, daß Auskunfteien und Wirtschaftsinformationsdienste ihre Angebote mehr und mehr vervielfältigen und spezialisieren. So verfolgen einige dieser Unternehmen zur Zeit die Zielsetzung, neue Gruppen von Anschlußpartnern zu gewinnen, die früher in diesem Umfang üblicherweise keine Auskünfte über ihre Kunden eingeholt haben, wie Wohnungs- und andere Vermieter, Inkassounternehmen, Ärzte sowie Dienstleistungsunternehmen aus den verschiedensten Bereichen.

So beabsichtigt ein im Rhein-Main-Gebiet ansässiges Unternehmen, eine zentrale Negativdatei aufzubauen, der sich alle Firmen und Personen bedienen können sollen, die im Gegenzug bereit sind, eigene negative Erfahrungen über ihre Kunden bekannt zu geben. Zu einem späteren Zeitpunkt sollen auch die in den unterschiedlichen Wirtschafszweigen angelegten zentralen Warndateien zu Auskunftszwecken an Anfrager aus den jeweiligen Wirtschaftszweigen genutzt werden. Dabei sollen in erheblichem Umfang auch "weiche" Daten gespeichert und übermittelt werden, d.h. Daten, die, wie die Angabe "Forderung angemahnt", weder objektiv nachprüfbar, geschweige denn in ihrer Berechtigung durch gerichtliche Verfahren bestätigt sein müssen. Dennoch darf nicht über-

sehen werden, daß solche Angaben den wirtschaftlichen Ruf eines Betroffenen und damit seine Persönlichkeitsrechte schwer und nachhaltig beeinträchtigen können. Die Aufsichtsbehörde hat daher die vorgesehene Speicherung mehrerer Datenarten beanstandet.

Ein anderer Informationsdienst, gegen den im Berichtsjahr zahlreiche Beschwerden eingingen, beabsichtigte, in einer Datenbank speziell wettbewerbswidrige Tatbestände von Unternehmen aus verschiedenen Branchen zu speichern und solchen Stellen zu übermitteln, die diese Verstöße abmahnen wollen. Das Unternehmen gab sein Vorhaben jedoch nach Beratung mit der Aufsichtsbehörde auf.

6.2 Darlegung und Dokumentation des berechtigten Interesses nach § 29 Abs. 2 Ziffer 1a BDSG

Wie bereits im Vorjahresbericht dargelegt, ist die bisherige Praxis der Darlegung des die Anfrage begründenden berechtigten Interesses durch den Anfrager und die Dokumentation dieser Angaben durch die Auskunfteien weiter als problematisch zu betrachten. Das berechtigte Interesse nach § 29 Abs. 2 Ziffer 1a BDSG wird von den Anfragern bei den Auskunfteien pauschal mit festgelegten Stichworten – z.B. Bonitätsprüfung, Forderung usw. – dargelegt. Bei der gebräuchlichen Verwendung von Formularanfragen muß so der Anfrager lediglich ein Kästchen für das zutreffende Stichwort ankreuzen. Es wurde bei Überprüfungen auch festgestellt, daß es eine Rubrik "Sonstiges" gab, bei deren Ankreuzen gänzlich unklar bleibt, ob ein berechtigtes Interesse beim Anfrager vorliegt. Ebenso unannehmbar ist die Praxis, als berechtigtes Interesse automatisch eine Kreditentscheidung anzunehmen, wenn der Anfrager keine Rubrik ankreuzt. Das Bundesdatenschutzgesetz selbst geht davon aus, daß der Anfrager ein berechtigtes Interesse "glaubhaft darlegt"; dies ist eine der Voraussetzungen für die Zulässigkeit der Übermittlung. Mit der gegenwärtig häufig anzutreffenden Praxis wird allerdings die Forderung des Gesetzes zu einer reinen Formalität reduziert. Die betroffene Auskunftei wurde daher aufgefordert, ihre Anfrageformulare dergestalt zu ändern, daß in jedem Fall ein Anfragegrund angegeben werden muß. Wird versehentlich ein Anfragegrund nicht genannt, ist die Auskunftei verpflichtet, den tatsächlichen Anfragegrund vor Auskunftserteilung zu ermitteln.

Sowohl die vorgebrachten Gründe für das Vorliegen eines berechtigten Interesses als auch die Mittel für ihre glaubhafte Darlegung sind nach § 29 Abs. 2 Satz 3 BDSG von der Auskunftei aufzuzeichnen. Dadurch soll die nachträgliche Überprüfung von Übermittlungsvorgängen durch die Aufsichtsbehörde ermöglicht werden. Die Auskunfteien sind allerdings auch verpflichtet, in einem Promille der Auskunftsfälle selbst das Vorliegen des angegebenen berechtigten Interesses nachzuprüfen. Auf Mängel dieses Selbstkontrollverfahrens wurde bereits im Vorjahresbericht aufmerksam gemacht. Diese Feststellungen wurden auch im Berichtsjahr bestätigt. Bei einer Auskunftei konnten solche Überprüfungen jedoch überhaupt nicht nachgewiesen werden. Als Grund wurde angegeben, daß gerade in diesen Überprüfungsfällen der Schriftverkehr nach Abschluß der Prüfung vernichtet würde. Eine weitere Kontrolle durch die Aufsichtsbehörde ist damit unmöglich gemacht. In einem anderen Fall wurden gerade bei telefonischen Anfragen keinerlei Überprüfungen durch die Auskunftei selbst durchgeführt. Telefonische Anfragen und Auskünfte hinterlassen jedoch geringe Spuren und sind deswegen tendenziell mit einem größeren Mißbrauchsrisiko belastet, so daß gerade bei den telefonischen Anfragen stichprobenweise Überprüfungen erforderlich sind.

Außerdem wurde von der Aufsichtsbehörde beanstandet, wenn im Rahmen der Selbstkontrolle Rückfragen an den Anfrager persönlich gerichtet wurden, statt an die Geschäftsleitung oder den Datenschutzbeauftragten des anfragenden Unternehmens. Bei solchem Vorgehen wird man wohl kaum erwarten können, daß mißbräuchliche Anfragen aufgedeckt werden. Immer wieder wurde auch festgestellt, daß die Kontrollanfragen wenig ausführlich oder überhaupt nicht beantwortet wurden.

Diese Probleme und Schwierigkeiten hatten zur Folge, daß die Aufsichtsbehörden in zweifelhaften Fällen nicht nur eine Prüfung bei der betroffenen Auskunftei, sondern auch bei dem Anfrager durchführten.

6.3 Dokumentation der Eingaben und Datenquellen

Das Bundesdatenschutzgesetz legt in seiner Anlage zu § 9 Satz 1 fest, daß bei automatisierter Verarbeitung Maßnahmen zu treffen sind, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle, Ziffer 7). Dadurch betroffen ist nicht nur die ursprüngliche Eingabe, sondern auch jede Veränderung von bereits gespeicherten Daten. Wie Überprüfungen der Aufsichtsbehörden ergeben haben, ist im Datenverarbeitungssystem in der Regel lediglich das Datum der letzten Änderung und das Zeichen der Sachbearbeiterin bzw. des Sachbearbeiters eindeutig dokumentiert. Welche Daten im Einzelnen geändert wurden, läßt sich oft bestenfalls aus den Quellenangaben und vorhandenen schriftlichen Unterlagen – teilweise – ermitteln. Werden diese schriftlichen Unterlagen (Recherchebögen) nach einer bestimmten Aufbewahrungsdauer vernichtet, dann ist die oben geschilderte Eingabekontrolle nicht mehr gewährleistet.

Auch die Heranziehung schriftlich erteilter Auskünfte ist nur zum Teil geeignet, den zu einem bestimmten Zeitpunkt gespeicherten Datenstand nachträglich festzustellen. Zur Aufklärung im Einzelfall, wer zu welchem Zeitpunkt welche Falschinformationen erhalten hat, ist in jedem Fall eine deutliche Verbesserung der Maßnahmen zur Eingabekontrolle notwendig. Auf Betreiben der Aufsichtsbehörde werden deshalb inzwischen die schriftlichen Änderungsunterlagen so lange aufbewahrt, bis es eine vollständige automatisierte Dokumentation der Dateneingaben gibt. Problematisch ist auch die durchweg mangelhafte Dokumentation der Datenquellen.

Nach § 34 Abs. 2 BDSG kann der Betroffene von Auskunfteien Auskunft über seine personenbezogenen Daten, sowie unter bestimmten Voraussetzungen Auskunft über Herkunft und Empfänger dieser Daten verlangen. Eine ausdrückliche rechtliche Verpflichtung der Auskunfteien zur Dokumentation insbesondere der Herkunft von Daten gibt es allerdings nicht. Die Verordnung über die Buchführungs- und Auskunftspflicht von Auskunfteien und Detekteien (Auskunftei- und Detekteiverordnung vom 18. Januar 1965 (Gesetz- und Verordnungsblatt für das Land Hessen, Teil I, 1965 Seite 25) als Spezialregelung kennt nur Aufzeichnungspflichten über andere Fakten. Daher haben in der Regel Auskunfteien in der Vergangenheit die Herkunft der Daten nicht dokumentiert und sind in Beschwerdefällen häufig nicht in der Lage nachzuvollziehen, wie sie an die Daten gelangt sind. Aus datenschutzrechtlicher Sicht setzt allerdings der Auskunftsanspruch die Dokumentation der Quellen voraus. Die Aufsichtsbehörde hat daher die Auskunfteien und Wirtschaftsinformationsdienste im Rahmen ihrer Überprüfungen aufgefordert, dafür Sorge zu tragen, daß zukünftig auch die Herkunft der Daten dokumentiert wird, da andernfalls der gesetzliche Auskunftsanspruch der Betroffenen ins Leere geht. Eine entsprechende Änderung der Auskunftei- und Detekteiverordnung ist darüber hinaus wünschenswert und steht zu erwarten.

6.4 Rechte der Betroffenen, insbesondere das Recht auf Auskunft

Im Bereich der Verarbeitung und Nutzung personenbezogener Daten durch Wirtschaftsauskunfteien und andere Stellen, die personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung speichern, hat das novellierte Bundesdatenschutzgesetz die Rechte der Betroffenen erweitert.

So ist der Betroffene, der über die erstmalige Übermittlung seiner personenbezogenen Daten zu benachrichtigen ist, jetzt gleichzeitig auch darüber in Kenntnis zu setzen, welche Art von Daten – zum Beispiel Geburtsdatum, Beruf, Grundbesitz – zu seiner Person gespeichert werden. Dies ist besonders im Hinblick darauf wichtig, daß betroffene Privatpersonen, die keine Kenntnis über den Umfang der Tätigkeit von Auskunfteien haben, sich durch diese Information einen Überblick über den Umfang der Datenspeicherung verschaffen können.

So speichern beispielsweise Auskunfteien, die nur für den Versandhandel tätig werden, in der Regel keine über Namen, Anschrift, Geburtsdatum, Beruf, Grundbesitz und eine knappe Beurteilung der finanziellen Verhältnisse hinausgehenden Daten zur Person des Betroffenen. Wie oben

ausgeführt, hat es jedoch im Berichtsjahr aufgrund nachgeholter Benachrichtigungen zahlreiche Anfragen und Beschwerden bei den Aufsichtsbehörden gegeben.

Das Bundesdatenschutzgesetz gibt den Betroffenen daneben ein Auskunftsrecht über die konkreten zu seiner Person gespeicherten Daten. Darüber hinaus kann der Betroffene über Herkunft und Empfänger der Daten Auskunft verlangen, wenn er begründete Zweifel an der Richtigkeit der Daten geltend macht (§ 34 Abs. 2 BDSG). In diesem Fall ist die Auskunft über Herkunft und Empfänger auch dann zu erteilen, wenn diese Angaben nicht in der Datei gespeichert sind, sondern sich lediglich aus Akten ergeben.

Die Erfahrungen der Aufsichtsbehörden haben gezeigt, daß die Auskunfteien dieses Auskunftsrecht des Betroffenen häufig mit einer direkten Datenerhebung beim Betroffenen verknüpfen wollen, indem vom Betroffenen die Richtigstellung unrichtiger Daten erbeten wird. Darauf braucht der Betroffene jedoch nicht einzugehen. Sind zu seiner Person unrichtige Daten gespeichert, so kann er neben einer Berichtigung auch die Sperrung der unrichtigen Daten verlangen (§ 35 Abs. 1 und 4 BDSG). Folge der Sperrung ist, daß diese Daten grundsätzlich nicht mehr ohne Einwilligung des Betroffenen übermittelt oder genutzt werden dürfen außer unter bestimmten eng umrissenen Voraussetzungen (§ 35 Abs. 7 BDSG).

In aller Regel gibt es keine Schwierigkeiten, wenn Betroffene verlangen, daß bestimmte falsche Daten gesperrt werden. Der Betroffene muß, wie bereits oben erwähnt, nicht das zutreffende Datum angeben, sondern nur die Richtigkeit des gespeicherten bestreiten. In Ausnahmefällen wurde allerdings von Auskunfteien verlangt, daß Beweise über die Unrichtigkeit der bestrittenen Daten vorgelegt werden sollten, oder behauptet, daß die Richtigkeit nicht ausreichend substantiiert bestritten worden sei. Der Betroffene ist jedoch nicht verpflichtet, der Auskunftei gegenüber die tatsächlichen Verhältnisse offenzulegen oder die zutreffenden Angaben zu machen. Das Bestreiten muß daher als ausreichend angesehen werden, wenn der Betroffene für ein bestimmtes Datum oder mehrere bestimmte Daten angibt, daß sie nicht zutreffend seien. Äußern sich Beschwerdeführer allerdings unklar und streben im Grunde, wie oft, die Löschung ihrer Daten ingesamt bei der Auskunftei an, so bittet die Auskunftsbehörde die Beschwerdeführer um Vorlage geeigneter Nachweise, wobei deren Inhalte jedoch selbstverständlich nicht gegen den Willen der Betroffenen offengelegt werden.

Über diese Grundsätze hinausgehende Anforderungen an die Darlegung durch den Betroffenen können sich allerdings dann ergeben, wenn er Auskunft über Herkunft und Empfänger der zu seiner Person gespeicherten Daten verlangt. Diese weitergehende Auskunft bekommt er nämlich nur dann, wenn er begründete Zweifel an der Richtigkeit der Daten geltend macht. Welche Anforderungen an diese Darlegungspflicht gestellt werden müssen, ist in verschiedenen Beschwerdefällen strittig geworden. Sicherlich steht fest, daß der Betroffene auf dem Weg zur Durchsetzung dieses Anspruchs nicht gezwungen werden kann, die zutreffenden Daten preiszugeben oder gar nachzuweisen. Die Aufsichtsbehörden sehen es hier als ausreichend an, daß der Betroffene allenfalls ihnen gegenüber über sein bloßes Bestreiten des konkreten Datums hinausgeht, also zum Beispiel Nachweise vorlegt, sofern dies überhaupt möglich ist. In jedem Fall wird man die Anforderungen an die Geltendmachung begründeter Zweifel nicht zu hoch ansetzen dürfen, da sonst das erweiterte Auskunftsrecht nur unter Verzicht auf geschützte Positionen des Betroffenen einzulösen ist.

In keinem Fall kann es der Auskunftei überlassen werden, dadurch das erweiterte Auskunftsrecht leerlaufen zu lassen, daß sie den Datenempfänger von der Übermittlung bestrittener Daten informiert und im übrigen aufgrund der Nachfrage beim Empfänger behauptet, daß durch die Übermittlung nichtzutreffender Informationen keine Nachteile für den Betroffenen entstanden wären. Die Disposition über das informationelle Selbstbestimmungsrecht wäre damit den Betroffenen völlig aus der Hand genommen.

Erfreulicherweise haben sich fast alle in Frage kommenden Unternehmen auf die durch das neue Bundesdatenschutzgesetz seit 1. Juni 1991 grundsätzlich eingeführte Entgeltfreiheit für Auskünfte rechtzeitig eingestellt. In der Vergangenheit war hier in einigen Fällen der Verdacht

aufgetaucht, daß die Möglichkeit für die Auskunfteien, Entgelt zu fordern, dazu benutzt wurde, zusätzliche Einnahmen zu erzielen (siehe Vorjahresbericht Ziffer 6.1). So hatte ein neu gegründeter Informationsdienst eine Vielzahl unterschiedlicher Unternehmen mittels einer Postkarte darüber informiert, daß er deren unternehmensbezogene Daten zum Zwecke der Übermittlung speichere. Die Betroffenen wurden gleichzeitig in Kenntnis gesetzt, daß sie für eine "Bearbeitungsgebühr" von 45,00 DM Auskunft über die zu ihren Unternehmen gespeicherten Daten verlangen könnten. Die aufgrund zahlreicher Beschwerden eingeleitete Überprüfung des Informationsdienstes durch die Aufsichtsbehörde ergab, daß dort zu den so angeschriebenen Unternehmen über die Anschriften hinaus keine weiteren Daten gespeichert wurden. Der Informationsdienst hat seine Tätigkeit jedoch zwischenzeitlich eingestellt.

Nach dem novellierten Bundesdatenschutzgesetz ist die Auskunft einem Betroffenen unentgeltlich zu erteilen. Werden die personenbezogenen Daten jedoch geschäftsmäßig zum Zweck der Übermittlung gespeichert, so kann dann ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann, § 34 Abs. 5 BDSG. Diese Möglichkeit der Nutzung ist jedoch zur Zeit lediglich bei Auskünften der Schufa möglich, die dementsprechend als einzige Auskunftei zur Zeit noch Entgelte für Selbstauskünfte verlangt. Von anderen Auskunfteien werden nach Kenntnis der Aufsichtsbehörden zur Zeit keine Entgelte für Selbstauskünfte verlangt.

6.5 Speicherung geschätzter personenbezogener Daten

Wie bereits im Vorjahr sind auch im Jahr 1991 bei Prüfungen der Aufsichtsbehörden in mehreren Fällen Speicherungen von Daten bei Auskunfteien festgestellt worden, die jeder tatsächlichen Grundlage entbehrten. Es wird nicht selten in der Weise verfahren, daß bei einer Anfrage über eine Person der Sachbearbeiter der Auskunftei zunächst feststellt, daß die vorhandenen Daten schon einige Jahre alt und wahrscheinlich nicht mehr aktuell sind. Falls der Versuch, bei dem Betroffenen nachzurecherchieren und auf diese Weise aktuelle Daten zu erhalten, scheitert, zum Beispiel, weil der Betroffene auch nach mehrmaligem Versuch nicht angetroffen wird, zieht der Rechercheur, um dem Auftraggeber dennoch einige Angaben liefern zu können, ein eventuell vorhandenes Brancheninformationsprogramm zu Rate. Diese Informationssammlung zeigt aktuelle Entwicklungen branchenmäßig aufgegliedert auf. Der Rechercheur kann daraus beispielsweise entnehmen, welchen Durchschnittsumsatz ein Installateurbetrieb mit zwei Mitarbeitern, der seit drei Jahren besteht, im Vorjahr hatte. Allerdings können dies nur statistisch ermittelte Durchschnittszahlen sein. Der Rechercheur vergleicht diese Zahl nun mit den veralteten Zahlen des Betriebs, über den er gerade erfolglos Ermittlungen angestellt hat. Auf dieser Grundlage wird nun geschätzt, daß sich die neuen realen Zahlen irgendwo in dem Bereich zwischen den alten und den durch das Hilfsprogramm an die Hand gegebenen Zahlen bewegen könnten, und die so geschaffenen neuen Daten werden als Auskunft an den Anfrager übermittelt. Die Herkunft der so gewonnenen Daten ist allerdings weder der nun "aktuellen" Speicherung noch der Übermittlung zu entnehmen.

Dieses Verfahren wurde von der Aufsichtsbehörde beanstandet. Werden personenbezogene Daten zu einem konkreten Betroffenen gespeichert und übermittelt, so müssen diese Angaben zutreffend sein. Es kann allenfalls geduldet werden, daß geschätzte Daten auch bei der Speicherung und Übermittlung als solche bezeichnet werden. Je mehr die geschätzten Daten allerdings von den wirklichen Daten abweichen, um so mehr nähert sich die Speicherung auch der Unzulässigkeit. Die Verwendung solcher Hilfsprogramme wird grundsätzlich kritisch betrachtet werden müssen. Zulässig wird sie allenfalls sein, wenn signifikante Unterschiede bestehen zwischen den Branchendurchschnittszahlen und den eigenen Angaben eines Betroffenen. Auch hier sollten sie jedoch nur dazu dienen, eventuell weitere Recherchen anzustellen oder bei der Übermittlung auf die Herkunft der Daten hinzuweisen.

6.6 Wechselprotestlisten

Seit Jahren ist den Aufsichtsbehörden das Problem bekannt, daß wöchentlich herausgegebene Listen mit Wechselprotestdaten der Arbeits-

gemeinschaft des Bankgewerbes bei den Auskunfteien kursieren und dort in den Datenbestand eingearbeitet werden, obwohl die Listen ausschließlich für Banken bestimmt sind und auf rechtlich zulässigen Wegen nicht an Auskunfteien gelangen können.

Nun wäre aus datenschutzrechtlicher Sicht kaum etwas dagegen einzuwenden, wenn eine Auskunftei diese Daten aufgrund einer Bezugsvereinbarung mit der Arbeitsgemeinschaft des Bankengewerbes erhielte, da damit auch sichergestellt wäre, daß es sich um die von der Arbeitsgemeinschaft autorisierten Daten handelt und aufgrund der wöchentlichen Neubelieferung eine regelmäßige Aktualisierung der Daten stattfindet. Unter den gegenwärtigen Bedingungen werden aber Daten in den Auskunftsdatenbestand eingegeben und übermittelt, von denen weder Authentizität noch Aktualität gesichert ist. Das bedeutet in nicht übersehbarem Umfang ein Risiko der Verletzung von Rechten der Betroffenen. Es muß daher darauf bestanden werden, daß nur solche Daten gespeichert und übermittelt werden, die die Auskunftei auf legale Weise erhalten hat. Ob die Information unmittelbar durch die Auskunftei auf unrechtmäßige Weise erhoben wurde oder ein Weg über Mittelsmänner gewählt wurde, darf hier nicht entscheidend sein. Die Aufsichtsbehörde hat die betroffenen Auskunfteien aufgefordert, entweder den Erhalt der Wechselprotestlisten auf rechtmäßige Weise nachzuweisen oder die Speicherung und Übermittlung dieser Daten einzustellen. Die weitere Verarbeitung dieser Daten zeigt einen erheblichen organisatorischen Mangel bei den betroffenen Auskunfteien auf, der, falls kein freiwilliges Einlenken erfolgt, zu Anordnungen der Aufsichtsbehörde nach § 38 Abs. 5 BDSG berechtigt.

6.7 SCHUFA

Nachdem im Jahre 1990 aus dem Bereich der SCHUFA keine Beschwerden wegen unzulässiger Datenübermittlung aufgrund Verwechslungen der betroffenen Personen bei den Aufsichtsbehörden bekannt wurden, waren im Jahre 1991 einige solcher Beschwerden zu verzeichnen.

In einem Fall waren zu dem vorhandenen Datensatz des Beschwerdeführers Daten einer anderen Person mit gleichem Vor- und Nachnamen sowie gleichem Geburtsdatum, jedoch einer anderen Wohnanschrift gespeichert worden. Die SCHUFA-Speicherung enthielt gehäufte und in kurzer Zeit nacheinander aufgenommene Kreditverpflichtungen. Wegen dieser ungünstigen SCHUFA-Eintragungen wurde ein Antrag des Beschwerdeführers auf Ausstellung einer Kreditkarte abgelehnt.

In einem ähnlichen Fall wurden zu dem Datenbestand eines Betroffenen zwei Negativeintragungen gespeichert, die einer anderen Person mit gleichem Namen und Geburtsdatum, jedoch einer gänzlich anderen Anschrift zuzuordnen gewesen wären. In einem weiteren Fall hatte die SCHUFA-Daten, die jeweils einem der beiden getrennt lebenden Ehepartnerzuzuordnen gewesen wären, zusammengeführt und bei Auskünften zu einem der beiden übermittelt.

Allen Fällen war gemeinsam, daß Daten, deren Zuordnung zweifelhaft war, ohne Nachfrage oder besonderen Hinweis auf diese Zweifelsfragen gespeichert und übermittelt wurden. Die SCHUFA war in keinem der Fälle in der Lage, für dieses Verhalten eine andere Erklärung als ihr Bestreben, Kunden möglichst umfassende Angaben machen zu wollen, und den bei allen SCHUFA-Auskünften angebrachten Hinweis auf die notwendige eigene Identitätsüberprüfung durch den Anfrager anzugeben. Die Entschuldigungen reichten von der Erklärung, daß die betroffene Person zwischenzeitlich umgezogen sein könne bis zum möglichen Schreibversehen bei dem Lieferanten der Daten.

Auf die Beschwerden der Betroffenen bzw. auf Tätigwerden der Aufsichstbehörde hin wurden von der SCHUFA unverzüglich die Falscheintragungen gelöscht und die Empfänger von der Berichtigung benachrichtigt. Die SCHUFA machte jedoch auch deutlich, daß sie nicht gewillt ist, organisatorische Anordnungen gegenüber ihren Mitarbeitern zu treffen, die verhindern, daß bei Anfragen oder Dateneinspeicherungen in bestehende Datensätze zweifelhafte Zuordnungen unterbleiben. Vielmehr sollen nach dem Grundsatz "im Zweifel für die Auskunft" weiterhin möglichst umfassende Auskünfte gegeben werden. Diese Praxis kann von den Aufsichtsbehörden nicht akzeptiert werden.

7. Werbewirtschaft

Der Anteil der Beschwerden gegen die Verarbeitung und Nutzung von personenbezogenen Daten zu Werbezwecken hat sich im Vergleich zu den Vorjahren etwas verringert. Möglicherweise liegt dies mit daran, daß mehr Unternehmen als bisher die Möglichkeit nutzen, ihre Adreßdaten mit den in der "Robinsonliste" des Deutschen Direktmarketing-Verbandes e.V. gespeicherten Daten abzugleichen. In die "Robinsonliste" kann man sich eintragen lassen, wenn man keine adressierte Werbung erhalten möchte. Die Aufnahme in diese Liste wird für fünf Jahre vorgenommen. Im Berichtsjahr wurde zwischen europäischen Direktmarketingverbänden eine Vereinbarung geschlossen, "Robinsonlisten" auch gegenseitig auszutauschen und für grenzüberschreitende Werbeaussendungen verfügbar zu machen.

Durch die Novellierung des Bundesdatenschutzgesetzes wurden für den Bereich der Werbewirtschaft die Betroffenenrechte erweitert. Der Betroffene hat nunmehr das Recht, der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung zu widersprechen (§ § 28 Abs. 3, 29 Abs. 3 BDSG). Dieses Recht wirksam geltend zu machen, wird allerdings durch die Praxis im Marketing-Bereich weitgehend verhindert. Die Adreßlistenvermittler müssen nämlich den Betroffenen weder darüber in Kenntnis setzen, daß er sich auf einer oder mehreren Listen, die unter verschiedenen Kriterien zusammengestellt worden sind, befindet; noch müssen Unternehmen ihre Kunden darüber in Kenntnis setzen, daß sie deren Adressen nicht nur für die Zwecke der Abwicklung des Kundenverhältnisses verwenden, sondern darüber hinaus auch noch anderen Unternehmen oder Adreßvermittlern für Werbezwecke zur Verfügung stellen. Der Betroffene, der Werbepost bekommt, weiß zudem in aller Regel nicht, daß seine Adresse nicht bei dem werbendem Unternehmen selbst gespeichert ist, sondern meistens bei Adreßvermittlern. Wendet er sich an den Absender der Werbepost und widerspricht dort der Verwendung seiner Daten für Werbezwecke, so muß sein Widerspruch erst an den eigentlichen Listeninhaber weitergeleitet werden, also in aller Regel zunächst an den Adreßhändler oder das Direktwerbeunternehmen und über dieses dann an den ursprünglichen Listeninhaber. Bis der Widerspruch auf diesem Weg zu dem Listeninhaber oder dem ursprünglichen Datenbesitzer gelangt ist, werden die Adreßdaten oft schon für andere Werbeaktionen erneut genutzt oder in neue Adreßzusammenstellungen aufgenommen worden sein, so daß der Betroffene seine Bemühungen von neuem aufnehmen kann. Aufgrund solcher Abläufe mußte zum Beispiel ein Betroffener, der die Aufsichtsbehörde eingeschaltet hatte, um adressierte Werbepost an seine minderjährige Tochter zu verhindern, dreimal die Hilfe der Aufsichtsbehörde in Anspruch nehmen.

Sehr empfindlich reagieren viele Betroffene, wenn der Anschein entsteht, das werbende Unternehmen habe die Adressen aus dem Bankbereich erhalten. Dies mußte eine große Geschäftsbank feststellen, die – ohne die Daten tatsächlich herauszugeben – bei ihren Kunden für einen amerikanischen Verlag geworben hatte. Obwohl hier datenschutzrechtlich keine Beanstandungen auszusprechen waren, wird ein solches Vorgehen kaum noch ratsam sein, da die Bankkundschaft merkbar verärgert war.

8. Versand- und Einzelhandel

8.1 Versandhandel

Im Berichtsjahr war eine Häufung von Beschwerden über den Versandhandel auffällig. Gründe waren die trotz Kundenwunsches nicht erfolgte Löschung aus der Kunden- bzw. Werbedatei, eine als zu umfangreich bewertete Datenerhebung über den Bestellschein und in mehreren Fällen die unberechtigte Übermittlung von Kundendaten an ein Inkassounternehmen. Die über das zur Abwicklung des Vertrages Erforderliche hinausgehende Datenerhebung auf dem Bestellschein wurde von dem betroffenen Unternehmen nach Gesprächen mit der Aufsichtsbehörde korrigiert. Deutlich wird damit aber das Bestreben, immer mehr Wissen über den einzelnen Kunden anzuhäufen und im Sinne der Verbesserung von Marketingstrategien auszuwerten. Gerade der Versandhandel speichert nicht nur Daten zur Abwicklung des Versandgeschäfts, sondern dieselben Daten werden genutzt zur Feststellung und Bewertung typischen oder atypischen Kaufverhaltens, zur Feststellung von Konsumschwerpunkten, zur Feststellung des Erfolgs oder Mißerfolgs bestimmter Wer-

bemaßnahmen bis hin zur Zusammenstellung von Inhabern gleichartiger Merkmale für Zwecke der Werbung anderer Unternehmen. Solange keine Übermittlung von Daten an Dritte stattfand, wurden alle diese Nutzungen datenschutzrechtlich früher nicht erfaßt. Mit der Novellierung des Bundesdatenschutzgesetzes gelten für Nutzungen von personenbezogenen Daten nunmehr dieselben Voraussetzungen wie für Übermittlungen, so daß Kundendaten grundsätzlich nicht mehr in jeder nur denkbaren Weise genutzt werden können. Auch bei Profilbildungen, etwa zum Zwecke der Erstellung einer besonderen Liste, muß so immer geprüft werden, ob schutzwürdige Interessen des Betroffenen, also des Kunden, an dem Ausschluß dieser Nutzung das Eigeninteresse des Unternehmens überwiegen.

Die Gruppe der Beschwerden wegen nicht erfolgter Löschung oder wegen unzulässiger Weitergabe personenbezogener Daten an ein Inkassounternehmen hatte schließlich einen eher banalen Grund: Durch das rasche Anwachsen des Versandgeschäftes in den neuen Bundesländern waren Abläufe im Unternehmen teilweise nicht mehr vollständig unter Kontrolle. Ware, die von Kunden zurückgeschickt wurde, staute sich sowohl auf dem Postweg als auch in der internen Abwicklung. Rücksendungen wurden nicht ordnungsgemäß im Datenverarbeitungssystem verbucht, so daß eine erste und eine zweite Mahnung herausgehen konnte, was wiederum automatisch zur Folge hatte, daß die ausstehende Forderung zur Eintreibung an ein Inkassounternehmen abgegeben wurde. Aber auch durch den umfangreichen Einsatz neuen, mit moderner EDV-Bearbeitung zum Teil nicht vertrauten Personals kam es hier zu Versäumnissen. Gleiches galt für die Berücksichtigung von entweder telefonisch eingegangenen oder der zurückgesandten Ware beigefügten Wünschen von Kunden nach Löschung ihrer Daten durch das Unternehmen.

Neben den geschilderten Verstößen gegen das Bundesdatenschutzgesetz war auch zu rügen, daß das Unternehmen offensichtlich zumindest zeitweise nicht in der Lage gewesen war, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des Bundesdatenschutzgesetzes zu gewährleisten (§ 9 BDSG nebst Anlage).

8.2 Einzelhandel

Ein Einzelhandelsunternehmen, das mehr als 200 Geschäftsfilialen betreibt, führte ein Verfahren zur Erfassung von Ladendiebstählen ein. Von dem jeweils angefertigten Diebstahlsprotokoll, dessen Original zur Erstattung der Strafanzeige verwendet wird, wurden drei Durchschriften hergestellt. Eine Durchschrift erhielt der Betroffene, eine weitere verblieb in der Filiale, in der die Tat begangen und das Protokoll aufgenommen wurde. Die dritte Durchschrift wurde an die Zentrale des Unternehmens gesandt und dort gesammelt und ausgewertet. Das Protokoll enthielt, neben den Angaben zur Tat, den Vor- und Zunamen, das Geburtsdatum, die Wohnanschrift und Nationalität des Tatverdächtigen.

Die in der Unternehmenszentrale entstehende Diebstahlsdatei sollte sowohl der Bekämpfung des Schwunds als auch dazu dienen, die Einhaltung des Hausverbots, das dem Tatverdächtigen nach dem ersten Diebstahlsversuch für alle Filialen erteilt wird, zu überwachen. Die Datei sollte es dem Unternehmen ermöglichen, Strafantrag wegen Hausfriedensbruchs gegen solche Personen zu stellen, die gegen das Hausverbot verstoßen und in einer der Geschäftsfilialen erneut tatverdächtig werden.

Gegen dieses Verfahren bestanden datenschutzrechtliche Bedenken. Bei den in der Zentrale gespeicherten Daten zu den Diebstählen und den gesammelten Protokolldurchschriften handelte es sich jeweils um Dateien im Sinn des § 2 Abs. 3 Nr. 3 BDSG (a.F.). Die Speicherung der personenbezogenen Daten mußte deshalb nach § 23 Satz 1 BDSG (a.F.) zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich sein.

Um Strafanträge wegen Hausfriedensbruchs stellen zu können, genügte jedoch die Speicherung von Vor- und Zunamen, Geburtsdatum und Anschrift des Tatverdächtigen. Die Speicherung darüber hinaus gehender Daten, wie der Nationalität, war nicht erforderlich und damit unzulässig. Die Aufbewahrung der Protokolle in der Unternehmenszentrale war

zudem schon deshalb nicht notwendig, da alle Angaben zur Person des Tatverdächtigen ohnehin elektronisch erfaßt wurden.

Aufgrund der datenschutzrechtlichen Bedenken gab das Einzelhandelsunternehmen die Führung der Diebstahlsdatei auf. Es entwickelte ein neues Verfahren, das sowohl das berechtigte Interesse an der Einhaltung und Kontrolle des Hausverbots wahrt, als auch den Vorschriften des Datenschutzrechts gerecht wird. Danach soll das formularmäßig gestaltete Diebstahlsprotokoll nur noch den Vor- und Zunamen, Geburtsdatum und Anschrift des Tatverdächtigen enthalten.

Die an die Zentrale übersandte Durchschrift des Protokolls wird innerhalb von zwei bis drei Tagen nach Eingang ausgewertet und dann vernichtet. Die in der Filiale verbliebene Durchschrift wird höchstens drei Jahre aufbewahrt, um die Erteilung des Hausverbots schriftlich belegen zu können und eine Entscheidungsgrundlage zu haben, wenn die Aufhebung des Hausverbots beantragt wird, sowie um in einem möglicherweise nachfolgenden zivilrechtlichen Verfahren über eine Sachverhaltsschilderung zu verfügen. Zum Schutz der Minderjährigen soll bei Kindern zwar ein Diebstahlsprotokoll angefertigt, aber keine Strafanzeige erstattet werden.

9. Aktienrecht

Eine Aktiengesellschaft verweigerte einem Aktionär die Zusendung einer Liste der Teilnehmer an einer Hauptversammlung und verwies dabei pauschal auf Gründe des Datenschutzes. Die Aufsichtsbehörde hat den Aktionär darauf hingewiesen, daß diese Liste zum Handelsregister genommen werden muß, das jedermann zugänglich ist. Die Aktiengesellschaft hat gegenüber dem Aktionär danach eingeräumt, daß sie die Liste nicht herausgeben wollte, weil sie einen erhöhten Verwaltungsaufwand befürchtete, falls dieses Beispiel Schule machen würde.

10. Versicherungen

Eine Versicherung hatte Gesundheitsdaten eines Beschwerdeführers an den Rückversicherer weitergeleitet. Sie berief sich zur Begründung auf eine AGB-mäßig abgegebene Einwilligung des Betroffenen.

Bei Durchsicht der AGB stellte sich heraus, daß die Einwilligungserklärung entgegen § 4 Abs. 2 Satz 3 BDSG nicht hervorgehoben war.

Nicht nachvollziehbar erscheint zudem die Tendenz der Versicherungsunternehmer, ihre künftigen Kunden über die Verarbeitung ihrer Daten möglichst im unklaren zu lassen. So hängt nach einer – drucktechnisch nicht hervorgehobenen – Wiedergabe der AGB die Wirksamkeit der Einwilligung in den Datenverkehr mit dem Rückversicherer davon ab, daß der Betroffene die Möglichkeit hatte, "in zumutbarer Weise" von einem "bereitgehaltenen Merkblatt Kenntnis zu nehmen". In der Regel wird sich nicht nachweisen lassen, ob das Merkblatt wirklich bereitgehalten wurde. Dieses Risiko scheint den Versicherungen jedoch tragbar im Vergleich dazu zu sein, dem Kunden von vornherein den Umfang der Verarbeitung seiner Daten bei der Antragsbearbeitung zu erläutern.

11. Banken

Eine Bankfiliale verweigerte einem Testamentsvollstrecker die Ausführung von Überweisungsaufträgen, weil die Aufträge nicht angaben, wer der Empfänger der Überweisungen sein sollte. Gleichzeitig teilte die Bank dem Erben, der Kunde bei ihr war, mit, welche Überweisungen beabsichtigt waren. Sie berief sich der Aufsichtsbehörde gegenüber auf ihre Warnpflicht. Es habe die Gefahr des Rechtsmißbrauchs bestanden.

Die Aufsichtsbehörde hat die Mitteilung an den Erben wegen Verstoßes gegen § 24 BDSG (a.F.) beanstandet. Insbesondere war die Übermittlung nicht erforderlich, weil es zum Schutz des Kunden ausgereicht hätte, die Aufträge nicht auszuführen, zumal sich die Bank zu diesem Verhalten berechtigt glaubte. Die Bank war auch nicht befugt, die sich aus § 2218 BGB ergebende Rechenschaftspflicht des Testamentsvollstreckers gegenüber dem Erben zu erfüllen, weil diese Pflicht höchstpersönlicher Natur ist (§§ 2218, 664 BGB).

Die Bank hat sich schließlich nach einigem Schriftwechsel dazu bereitgefunden, ihrer Filiale derartige Auskünfte künftig zu untersagen.

12. Vereine

Unter den Anfragen an die Aufsichtsbehörden gab es auch im Berichtsjahr einige Anfragen von seiten eingetragener Vereine nach den geltenden Regelungen für den Umgang mit den Mitgliederdaten, nach Bewertungen der Aufsichtsbehörde hinsichtlich bestimmter beabsichtigter Verarbeitungen und nicht zuletzt nach den Möglichkeiten der sicheren Verarbeitung von Mitgliederdaten unter den Bedingungen des Einsatzes von Personalcomputern. Die Bandbreite ging hier von Vereinen, die sich zur Förderung besonderer literarischer Interessen mit einer sehr geringen Mitgliederzahl zusammengeschlossen haben, bis zu Vereinen, die im sportlichen Bereich eher wirtschaftlichen Unternehmen gleichen.

Die Aufsichtsbehörden sind nicht der nach der Novellierung des Bundesdatenschutzgesetzes teilweise vertretenen Meinung gefolgt, daß auf die reine Mitgliederverwaltung kleiner Vereine mit sportlichen, karitativen oder sonstigen nichtgeschäftlichen Zwecken das Bundesdatenschutzgesetz keine Anwendung finde. Unter Zugrundelegung der Regeln des Bundesdatenschutzgesetzes für den nicht-öffentlichen Bereich wurde vielmehr versucht, den Vereinen ein praktikables Konzept sowohl hinsichtlich der jeweils beabsichtigten Verarbeitung oder Nutzung als auch hinsichtlich der Datensicherungsmaßnahmen anzubieten, das im Interesse des informationellen Selbstbestimmungsrechts und nicht zuletzt im Interesse einer Absicherung der Vereinsführung auf die Legitimierung der Datenverarbeitung durch Einwilligung der Betroffenen abzielte. An den der Aufsichtsbehörde vorgetragenen Fällen wurde im übrigen deutlich, daß die Gefährdung des Persönlichkeitsrechts auch in den Bereichen vorkommen kann, in denen es zunächst einmal allein um die Verwirklichung ideeller und nicht gewerbsmäßiger Zielsetzungen geht. Ebensowenig läßt sich die Geltung von Datenschutzregeln an der Größe des Vereins festmachen. Aus der Aufsichtspraxis ist hier beispielhaft ein als eingetragener Verein geführter Bundesverband zu nennen, dessen Datenverarbeitungsvolumen trotz der geringen Mitgliederzahl von nur 12 Einzelvereinen es sicher nicht gerechtfertigt hätte, aus dem Geltungsbereich des Bundesdatenschutzgesetzes ausgenommen zu werden.

Beschwerden gegen vereinsinterne Datenverarbeitungen oder Nutzungen sind den Datenschutzaufsichtsbehörden kaum bekannt geworden. Eine Ausnahme machte hier eine Einrichtung, die zwar als privatrechtlicher Verein eingetragen ist, sich selbst aber als eine Religionsgemeinschaft betrachtet. Die Betroffenen, die sich für Literatur zu Methoden der Nutzung des vollen Potentials des menschlichen Geistes interessiert hatten, waren in eine Interessentendatei aufgenommen worden und hatten zum Teil auch einen sehr umfangreichen Persönlichkeitstest abgegeben. Trotz der massiven und zum Teil über Monate wiederholten Forderungen der Betroffenen, weitere Werbezusendungen zu unterlassen und die über sie gespeicherten Daten restlos zu löschen, erhielten sie weiterhin Post von der betroffenen Einrichtung.

Bei einer nicht angekündigten Überprüfung des Vereins hat die Aufsichtsbehörde festgestellt, daß die Befürchtung der Betroffenen, es würden in großem Umfang personenbezogene Daten in Dateien gespeichert, in dieser Weise nicht zutraf. Gespeichert waren lediglich die Daten von Buchbestellern mit Anmerkungen zu ihrer Einstellung gegenüber dem betroffenen Verein. Die Daten dieser Personen waren bereits ohne deren Einwilligung an die amerikanische Mutterorganisation weitergegeben worden. Die Aufsichtsbehörde untersucht noch, ob diese Übermittlung in ihrem Zuständigkeitsbereich stattgefunden hat. Die Aufsichtsbehörde kann allerdings nicht mehr verhindern, daß die Betroffenen nun aus dem Ausland mit unerwünschtem Material belästigt werden.

Schließlich muß auch an dieser Stelle wieder darauf hingewiesen werden, daß die Aufsichtsbehörde nicht die gesetzliche Befugnis hatte, die Beachtung des Datenschutzes durch den Verein zu überprüfen, soweit die persönlichen Daten der Mitglieder nur in Akten enthalten sind.

13. Auslandsdatenverarbeitung

Auch in diesem Berichtsjahr wurde die Aufsichtsbehörde häufiger bei geplanten Übermittlungen ins Ausland um Rat gefragt, sei es bei der Verlagerung von gesamten Datenbeständen zur Datenverarbeitung in ausländische Rechenzentren oder bei mehr oder weniger regelmäßigen

Übermittlungen von Personal- oder Kundendaten an das ausländische Mutterunternehmen.

Ein typischer Anlaß für die Einholung einer beratenden Stellungnahme durch die Aufsichtsbehörde war zum Beispiel das Vorhaben eines internationalen Unternehmens, über eine Marktforschungsgesellschaft in mehreren europäischen Ländern die Marktplazierung und das Image des Unternehmens durch Befragung von Kunden und Händlern feststellen und bewerten zu lassen. Das deutsche Beratungsunternehmen setzte dabei für die Datenerhebung in den jeweiligen Ländern nationale Unternehmen ein. Dabei stellte sich die Frage, welche Datenschutzregelungen gelten, ob die jeweiligen Länderregelungen miteinander verträglich sind, so daß bereits dadurch ein einheitlicher Standard gesichert ist, oder ob und gegebenenfalls wie ein einheitlicher Datenschutz für das Gesamtprojekt gesichert werden kann. Da sämtliche erhobenen Daten letztlich im Inland verarbeitet werden sollten, wurde dem Unternehmen empfohlen, einen einheitlichen Datenschutzstandard dadurch festzulegen, daß die nationalen Subunternehmer per Vertrag auf die Einhaltung von Regeln verpflichtet wurden, die dem deutschen Datenschutzrecht entsprechen. Auf diese Weise wurde auch sichergestellt, daß die Verarbeitung der Daten einer strengen Zweckbindung unterworfen wurde und für die einzelnen Verarbeitungsphasen, die zum Teil auch im Ausland stattfinden sollten, ein einheitlicher Ablauf und Sicherheitsstandard festgelegt wurde. Allerdings konnte durch solch eine Regelung nicht die Geltung der jeweiligen nationalen Regelungen für die ausländischen Subunternehmer mit eventuellen Melde- oder Registrierpflichten in irgendeiner Weise beeinflußt werden. Sobald aber die Daten in den Geltungsbereich des Bundesdatenschutzgesetzes gelangen, unterliegt ihre Verarbeitung ausschließlich den deutschen Regeln.

Problematisch waren in einigen Fällen Datenübermittlungen in das europäische Ausland, wenn das Land weder der europäischen Datenschutzkonvention Nr. 108 von 1981 beigetreten ist, noch über eine eigene Datenschutzgesetzgebung für den nicht-öffentlichen Bereich verfügt. Das gilt auch für außereuropäische Länder, bei denen dieselben Bedingungen vorliegen. So bat eine Unternehmensberatung um Auskunft darüber, ob ihr Mandant, ein in der Bundesrepublik ansässiges Unternehmen, personenbezogene Daten an Tochterunternehmen in Österreich und in der Schweiz übermitteln dürfe. Hinsichtlich der Übermittlungen nach Österreich, das der europäischen Datenschutzkonvention beigetreten ist und über eine eigene Datenschutzgesetzgebung verfügt, bestanden keine Probleme, insbesondere weil es sich um für die Abwicklung von Verträgen erforderliche Daten handelte und die Übermittlungen bereits aufgrund der ersten Alternative des § 28 Abs. 1 Ziffer 1 BDSG gerechtfertigt waren. Für die Datenübermittlungen in die Schweiz, die weder der europäischen Datenschutzkonvention von 1981 beigetreten ist noch über eine Datenschutzgesetzgebung für den nicht-öffentlichen Bereich verfügt, hat die Aufsichtsbehörde eine Lösung über ein Vertragsmodell vorgeschlagen, das den ausländischen Datenempfänger zur Schaffung eines mindestens der Europaratskonvention entsprechenden Datenschutzstandards verpflichtet.

Die internationale Verflechtung von Unternehmen führt auch im Personalbereich zu einem immer stärkeren Wunsch nach Austausch von Personaldaten. So bat ein Unternehmen um Beratung, das von der in den USA ansässigen Muttergesellschaft aufgefordert worden war, Personaldaten seiner Mitarbeiter zur Verfügung zu stellen.

Zunächst wurde klargestellt, daß es sich bei dieser Weitergabe von Personaldaten um Übermittlungen handelt, die nach § 28 BDSG zu beurteilen sind. Hat der Mitarbeiter zu der geplanten Übermittlung kein schriftliches Einverständnis gegeben und ist auch nicht aus dem Inhalt und Zweck seines Arbeitsvertrages die Möglichkeit bzw. Notwendigkeit einer solchen Übermittlung klar ersichtlich (z.B. bei Mitarbeitern, die die Bereitschaft zum Auslandseinsatz oder zum turnusmäßigen Wechsel im Rahmen ihrer Aus- oder Fortbildung erklärt haben), so richtet sich die Zulässigkeit der Übermittlung nach § 28 Abs. 1 Ziffer 2 BDSG. Danach muß vor allem ausgeschlossen sein, daß schutzwürdige Interessen des Betroffenen bestehen, die höher zu bewerten sind als das Interesse des übermittelnden oder des die Daten empfangenden Unternehmens. Für den Fall von Listenübermittlungen nach § 28 Abs. 2 Ziffer 1b BDSG legt das Gesetz fest, daß in bestimmten Fällen eine gesetzliche Vermutung dafür besteht, daß ein solches überwiegendes Interesse des Betroffenen besteht.

Dies gilt danach zum Beispiel für die Übermittlung von Daten durch den Arbeitgeber, die sich auf arbeitsrechtliche Rechtsverhältnisse beziehen. Diese gesetzliche Vermutung ist als Auslegungshinweis auch in den Fällen heranzuziehen, in denen es sich um eine Einzelübermittlung handelt oder jedenfalls nicht um eine listenmäßige Übermittlung nach § 28 Abs. 2 Ziffer 1b, weil die zu übermittelnden Daten über die dort möglichen Datengruppen hinausgehen. Ist sich also der Arbeitgeber in jedem einzelnen Übermittlungsfall nicht sicher, daß der Betroffene keine schutzwürdigen Interessen an dem Ausschluß der Übermittlung hat, so bleibt als einzige Möglichkeit, die Übermittlung zu rechtfertigen, wiederum nur die Einholung der schriftlichen Einverständniserklärung durch den Betroffenen. In jedem Fall ist von der übermittelnden Stelle zu klären, zu welchen Zwecken die Daten verwendet werden sollen. Nur mit diesen Angaben kann einerseits das berechtigte Interesse des Datenempfängers, andererseits die Möglichkeit eines schutzwürdigen Interesses des Betroffenen an dem Ausschluß der Übermittlung beurteilt werden. Bezogen auf den Zweck ist auch zu prüfen, in welchem Umfang die Übermittlung notwendig ist.

Bei den in Frage kommenden Beschäftigten, deren personenbezogene Daten voraussichtlich an die ausländische Muttergesellschaft zu übermitteln sind, ist es ratsam, eine Einwilligungserklärung bereits in den Arbeitsvertrag mit aufzunehmen. Der Arbeitsvertrag sollte allerdings auch die zulässigen Übermittlungszwecke (z.B. Personallenkungs- und Förderungszwecke) festlegen.

Die Unternehmen sind schließlich darauf hingewiesen worden, daß in vielen Fällen die Beteiligung der betrieblichen Vertretung der Beschäftigten erforderlich sein wird.

14. Arbeitnehmerdatenschutz

Gleich durch mehrere Beschwerden und Anfragen wurde bemängelt, daß Arbeitgeber nach Abschluß des Bewerbungsverfahrens auch auf Nachfrage der Betroffenen die Bewerbungsunterlagen nicht zurückgaben. Auf Bitten der Aufsichtsbehörde ist dies dann jeweils umgehend geschehen.

Die Aufsichtsbehörde konnte sich in diesen Fällen allerdings nur auf Anregungen beschränken, weil ihr das Gesetz keine Handhabe für ein Eingreifen bietet. § 38 Abs. 1 des neuen BDSG enthält, anders als die alte Regelung, die nunmehr eindeutige Feststellung, daß die Aufsichtsbehörde andere Vorschriften über den Datenschutz nur überprüfen darf, soweit die Verarbeitung und Nutzung von Daten in oder aus Dateien erfolgt. Bewerbungsunterlagen werden aber regelmäßig nicht in Dateien verarbeitet.

Auch folgender Fall läßt sich wegen der Beschränkung der Aufsicht auf Dateien nicht bearbeiten, obwohl dies unter Datenschutzgesichtspunkten erforderlich wäre:

Einem Unternehmen wurde vorgeworfen, einem Bewerber eine Liste vorgehalten zu haben, aus der hervorging, daß er unter anderem gegen einen Bebauungsplan, der Erweiterungsabsichten des Unternehmens betraf, Einwendungen erhoben hatte. Im Lauf des Verfahrens stellte sich heraus, wie das Unternehmen an diese Unterlagen gekommen sein könnte. Sie waren nämlich anläßlich der öffentlichen Beratung des Bebauungsplans an die Gemeindevertreter verteilt worden.

Die Nutzung solcher Unterlagen im Bewerbungsgespräch ist vom Bundesdatenschutzgesetz nicht erfaßt, da sie nicht aus einer Datei stammen.

Wegen des fehlenden Dateibezugs bestehen dementsprechend auch keine Überprüfungsbefugnisse in folgendem Fall:

Eine genossenschaftlich organisierte Taxizentrale beabsichtigte, alle eingehenden Telefongespräche auf Band aufzuzeichnen. Zweck der Aufzeichnungen sollte die Dokumentation von Fehlfahrten zum Zweck der Rationalisierung, die Aufzeichnung von Anruferstimmen für die Identifikation von Überfalltätern und das Unterbinden von Privatgesprächen der Mitarbeiter sein. Aus Sicht der Aufsichtsbehörde handelt es sich bei den geplanten Aufzeichnungen um einen Verstoß gegen § 201 Abs. 1 Nr. 1 StGB. Eingriffsmöglichkeiten gibt es für die Datenschutzbehörden jedoch nicht. Es bestehen nicht einmal Auskunftsansprüche, sobald feststeht, daß eine dateimäßige Aufbewahrung der Tonbänder nicht beabsichtigt ist.

15. Datenverarbeitung im medizinischen Bereich

15.1 Rechtsgrundlagen

Der Umgang mit personenbezogenen Daten aus dem Bereich ärztlicher Tätigkeiten berührt in besonderer Weise die Persönlichkeitsrechte. Das novellierte Bundesdatenschutzgesetz enthält dennoch nur einen kurzen Hinweis auf die besondere Schutzwürdigkeit dieser Daten, nämlich in § 28 Abs. 2 Satz 2 BDSG, der bei Listenübermittlungen eine gesetzliche Vermutung für ein schutzwürdiges Interesse des Betroffenen an einem Ausschluß der Übermittlung für solche Daten enthält, die sich auf gesundheitliche Verhältnisse beziehen.

Die Anwendung des Bundesdatenschutzgesetzes ist auch nach der Novellierung im Bereich der Tätigkeit der frei praktizierenden Ärzte auf die Verarbeitung und Nutzung personenbezogener Daten in oder aus Dateien beschränkt. Auf Akten findet es nur dann Anwendung, wenn die darin enthaltenen Daten offensichtlich aus einer Datei entnommen worden sind (§ 27 BDSG). Gerade in diesem Bereich befinden sich noch häufig besonders sensible Daten ausschließlich in Akten. Neben spezifisch datenschutzrechtlichen Regelungen, die allerdings mit zunehmender Verbreitung der elektronischen Datenverarbeitung in der Arztpraxis auch dort immer größere Bedeutung gewinnen, sind Ärzte allerdings immer schon an die Wahrung der ärztlichen Schweigepflicht (§ 203 Abs. 1 Nr. 1 Strafgesetzbuch) gebunden. Darauf beruhend gibt es einige wenige Regelungen in der Berufsordnung für Ärzte in Hessen, deren Aktualisierung dringend geboten ist.

Im Berichtsjahr ist allerdings insbesondere durch neue höchstrichterliche Entscheidungen Bewegung in die Erörterung des Datenschutzes in der Arztpraxis geraten.

15.2 Datenübermittlung an ärztliche Verrechnungsstellen

Immer wieder wurde an die Aufsichtsbehörden die Anfrage gerichtet, ob es zulässig sei, daß Ärzte vollständige Behandlungsunterlagen ihrer Privatpatienten ohne deren Einwilligung an privatärztliche Abrechnungsstellen weitergeben. Die Datenschutzaufsichtsbehörden haben bereits seit einiger Zeit Bedenken gegenüber dieser Praxis angemeldet. Aufgrund der bisherigen höchstrichterlichen Rechtsprechung, die von einer möglichen stillschweigenden Einwilligung des Patienten in diese allseits üblichen Datenübermittlungen ausgegangen war, wurde jedoch eine "Widerspruchslösung" akzeptiert: Es wurde als noch zulässig erachtet, daß der Arzt seine Privatpatienten durch Informationszettel oder in den Praxisräumen gut sichtbar ausgehängte Hinweise auf die in seiner Praxis übliche Einschaltung von privatärztlichen Verrechnungsstellen hinwies. Sofern der Patient dem nicht widersprach, wurde sein Einverständnis mit diesem Verfahren unterstellt.

Diese Praxis hat der Bundesgerichtshof nunmehr mit Urteil vom 10. Juli 1991 (Aktenzeichen VII ZH zu 196/90, NJW 1991, Seite 2955) als unvereinbar mit dem sich aus Artikel 2 Abs. 2 Grundgesetz ergebenden Recht des einzelnen auf informationelle Selbstbestimmung erklärt. Es obliegt danach grundsätzlich dem Arzt, die Zustimmung des Patienten zu einer Weitergabe seiner personenbezogenen Daten in eindeutiger und unmißverständlicher Weise einzuholen. Dennoch veranlaßte Übermittlungen erfüllen den Straftatbestand des § 203 Abs. 1 Nr. 1 StGB.

Das Urteil erregte erhebliches Aufsehen und führte auch zu etlichen Anfragen an die Datenschutzaufsichtsbehörden. Ein wegen derselben Problematik anhängig gemachter Beschwerdefall konnte mit der Zusicherung der beteiligten großen privatärztlichen Verrechnungsstelle abgeschlossen werden, daß sie alle Mitglieder auf das genannte Urteil durch Rundschreiben hingewiesen habe und ihnen kostenlose Vordrucke für Einwilligungserklärungen bezüglich der Datenübermittlung zur Verfügung stellen werde.

15.3 Diagnoseangabe auf Rechnungen

Im Zusammenhang mit der öffentlichen Kritik an den umfangreichen Datenübermittlungen zwischen niedergelassenen Ärzten und Krankenkassen stellte ein Betroffener die Frage, ob die Übermittlung der Diagnose an die ärztliche Verrechnungsstelle datenschutzrechtlich zulässig sei. Auch

wenn der betroffene Patient seine Einwilligung erteilt hat, daß der Arzt zur Erstellung der Rechnung Angaben über die Behandlung an eine privatärztliche Verrechnungsstelle weitergeben kann, gilt das unter Umständen nicht für die Übermittlung der Diagnose. Die Einwilligung wird sich regelmäßig nur auf solche Daten erstrecken, die zum Erstellen der Rechnung notwendig sind. Die Angabe der Diagnose ist dazu nicht erforderlich. Allerdings wird meist die Krankenversicherung, der die Rechnungen später durch den Betroffenen selbst vorgelegt werden, die Angabe der Diagnose auf der Rechnung verlangen. Dies ist für die private Krankenversicherung auch sinnvoll, um beurteilen zu können, ob angemessene und erstattungsfähige Behandlungsleistungen erbracht worden sind. Insoweit wird die Übermittlung der Diagnose bei entsprechender Einwilligungserklärung auch noch abgedeckt sein.

In einem anderen Beschwerdefall fragte ein Betroffener bei der Aufsichtsbehörde an, ob seine private Krankenversicherung von ihm verlangen könne, daß die Rechnung die Angabe der Diagnose enthalte, wenn dies aus Gründen des Datenschutzes doch unzulässig sei, wie er Presseberichten entnommen habe. Dem Betroffenen konnte zum damaligen Zeitpunkt daraufhin lediglich die Auskunft erteilt werden, daß es sich bei der an ihn gerichteten Aufforderung der Krankenversicherung um ein Verfahren zur Datenerhebung handele, das durch das Bundesdatenschutzgesetz 1977, das zum gegebenen Zeitpunkt noch galt, nicht geregelt sei. Der Betroffene hatte außerdem bei Vertragsschluß die "Allgemeinen Vertragsbedingungen" der Krankenversicherung akzeptiert, die ausdrücklich verlangen, daß die vorgelegten Rechnungen auch die Bezeichnung der behandelten Krankheiten enthalten müssen. Dem Betroffenen mußte deshalb mitgeteilt werden, daß seine Krankenversicherung die Vorlage von Rechnungen mit Angabe der Diagnose verlangen kann, bevor sie die entstandenen Behandlungskosten erstattet, und ihm im übrigen nur die Möglichkeit bleibe, die Gültigkeit der entsprechenden Vertragsklausel auf zivilrechtlichem Wege klären zu lassen.

15.4 Behandlung von Patientendaten bei der Praxisaufgabe und beim Austausch zwischen Ärzten

Immer wieder werden Aufsichtsbehörden eingeschaltet, wenn Bürger Unterlagen aus Arztpraxen im Altpapier oder in Müllcontainern finden. In einem Fall meldeten sich die Vermieter von Praxisräumen bei der Aufsichtsbehörde, da sie ärztliche Unterlagen in der zum Haus gehörenden Altpapiertonne gefunden hatten. Es handelte sich dabei um einfache Arztschreiben, Berichte von oder für andere Ärzte und teilweise umfangreiche ärztliche Gutachten zum Gesundheitszustand einzelner Patienten, deren voller Name und Anschrift den Papieren zu entnehmen war. Die Patientenunterlagen stammten offensichtlich aus dem Bestand des früheren Praxisinhabers, der seine ärztliche Tätigkeit aufgegeben hatte. Wie die Unterlagen in die Altpapiertonne gelangt waren, war nicht aufklärbar. Die Aufsichtsbehörde konnte jedoch bereits deswegen nicht weiter tätig werden, weil die Unterlagen keine Datei im Sinne des § 3 Abs. 2 BDSG darstellten und auch nicht offensichtlich aus einer Datei entnommen worden waren, so daß eine Anwendung des Bundesdatenschutzgesetzes entfiel.

Die Aufsichtsbehörde benutzt dennoch solche Gelegenheiten, um auf die Notwendigkeit des besonders sorgfältigen Umgangs mit solchen Unterlagen hinzuweisen und über die Möglichkeiten einer sicheren Entsorgung zu informieren. Hinzuweisen ist hier jedoch auf ein Urteil des Bundesgerichtshofes vom 11.12.1991 (Az.: VIII ZR 4/91). Ein Arzt, der seine Tätigkeit einstellt, kann danach nicht ohne die ausdrückliche und im Geltungsbereich des Bundesdatenschutzgesetzes schriftliche Einwilligung seiner Patienten Behandlungsunterlagen oder Informationen über seine Patienten an den Nachfolger übergeben. Andernfalls macht er sich eventuell wegen Verletzung der ärztlichen Schweigepflicht strafbar. Der Bundesgerichtshof hat damit in Folge der Entscheidung über die Weitergabe von Patientendaten an ärztliche Verrechnungsstellen (siehe oben) eine wichtige Entscheidung getroffen, um dem informationellen Selbstbestimmungsrecht auch in diesem Bereich Geltung zu verschaffen.

Eine andere Anfrage weist auf einen besonderen Bereich des Datenschutzes hin, der in der alltäglichen Praxis des Informationsaustausches eine nicht unerhebliche Rolle spielen dürfte. Die Anfragende erkundigte

sich danach, ob ein behandelnder Arzt (z.B. der Hausarzt) Informationen über einen Patienten an einen Werksarzt weitergeben dürfe, welche Voraussetzungen dazu erfüllt sein müßten und bei welchen Informationen dies möglich sei. Gegenstand einer weiteren Beschwerde war der umgekehrte Fall, nämlich die Zulässigkeit der Übermittlung durch den Werksarzt eines Unternehmens an einen Arzt des staatlichen Gesundheitsamtes. Grundsätzlich unterliegen Ärzte, gleich welcher Fachrichtung oder Tätigkeit, auch untereinander der ärztlichen Schweigepflicht. Die Übermittlung personenbezogener Daten auch von Arzt zu Arzt ist deshalb ebenso nur mit Einwilligung des betroffenen Patienten zulässig. Der Umfang der Einwilligung bestimmt dabei, welche Daten weitergegeben werden dürfen. Grundsätzlich sollten nur die für die anstehende Behandlung oder Begutachtung notwendigen Angaben übermittelt werden, nicht die gesamte vorhandene Patientengeschichte. Diese Grundsätze gelten zwischen Hausarzt und Facharzt genauso wie zwischen dem Werksarzt und dem Hausarzt oder im öffentlichen Gesundheitswesen beschäftigten Ärzten.

Ein krasser Fall wurde durch eine telefonische Anfrage an die Aufsichtsbehörde herangetragen. Sechs Ärzte eines Ärztehauses, die verschiedenen Fachrichtungen angehörten, wollten eine gemeinsame EDV-Anlage installieren. Mit Hilfe der EDV sollten in Zukunft auch die Patientendaten verwaltet werden. Hiergegen ist dann nichts einzuwenden, wenn die Patientendaten jedes Arztes bzw. jeder Praxis strikt getrennt gehalten werden von den Daten der anderen Praxen. Die Ärzte hatten jedoch erwogen, jedem der beteiligten Ärzte den Zugriff zu allen Patientendaten zu gewähren, damit in den häufigen Fällen der Überweisung eines Patienten von einem Arzt zum anderen nicht jedes Mal neu Daten erhoben werden müßten. Jedem Arzt hätten auf diese Weise auch sofort alle wichtigen Daten über den Patienten vorgelegen. Ein solches Vorhaben konnte nur auf die unbedingte Ablehnung durch die Aufsichtsbehörde stoßen.

15.5 Datenschutz im Krankenhaus

Anders als bei niedergelassenen Ärzten ist die Aufsichtsbehörde in privaten Krankenhäusern in der Lage, die Einhaltung des Datenschutzrechts bei der Verarbeitung personenbezogener Daten auch in Akten zu überprüfen. Das beruht auf einer – wenig übersichtlichen – besonderen gesetzlichen Regelung. Für private Kliniken in Hessen findet nämlich über § 12 des Hessischen Krankenhausgesetzes vom 18. Dezember 1989 (Gesetz und Verordnungsblatt für das Land Hessen Teil I Seite 452) das Hessische Datenschutzgesetz Anwendung. Das Hessische Datenschutzgesetz wiederum regelt die Datenverarbeitung sowohl in Dateien als auch alle sonstigen Datenverarbeitungen, also auch die in Akten.

Die im Vergleich zum Bundesdatenschutzgesetz restriktiveren Regelungen des Hessischen Datenschutzes sind der Anlaß für eine Auseinandersetzung mit einer privaten Klinik. Fraglich ist hier, inwieweit die Klinikleitung berechtigt ist, Einblick in Patientenunterlagen sowie in den ein- und ausgehenden Schriftverkehr insbesondere von Ärzten zu nehmen. Die Klinikleitung vertrat hierzu den Standpunkt, daß der volle Einblick in den ausgehenden Schriftverkehr, auch in Arztbriefe, für die § 203 StGB gilt, zur Kontrolle der Schreibkräfte erforderlich sei. Im übrigen müßten auch eingehende Arztschreiben und Patientenunterlagen jederzeit zu Kontrollzwecken zugänglich sein, um die Abrechnung und die Überprüfung der erbrachten Leistungen möglich zu machen. Die Aufsichtsbehörde stellte demgegenüber klar, daß die Öffnung von Arztbriefen, insbesondere wenn sie an Ärzte der Klinik mit dem Vermerk "zu Händen", "persönlich" oder "vertraulich" gerichtet sind, zumindest ein Verstoß gegen das Briefgeheimnis (§ 202 StGB) darstellt. Die unbeschränkte Einsichtnahme in Patientenunterlagen sowie die umfassende Kontrolle ausgehender Arztbriefe ist dagegen sowohl unter dem Gesichtspunkt des Arztgeheimnisses als auch unter datenschutzrechtlichen Aspekten problematisch. Nach Meinung der Aufsichtsbehörde ist im Regelfall weder zu Abrechnungszwecken noch zur Kontrolle der Schreibleistungen eine unbeschränkte Einsichtnahme erforderlich und zulässig.

16. Betrieblicher Datenschutzbeauftragter

Nicht-öffentliche Stellen, die personenbezogene Daten verarbeiten und in der Regel damit bei automatisierter Verarbeitung mindestens fünf Arbeit-

nehmer ständig beschäftigen, haben einen betrieblichen Datenschutzbeauftragten schriftlich zu bestellen. Werden personenbezogene Daten auf andere Weise verarbeitet, so besteht die Verpflichtung zur Bestellung eines Datenschutzbeauftragten ab einer Arbeitnehmerzahl von 20 (§ 36 Abs. 1 BDSG). Ein häufig festzustellendes Mißverständnis ist, daß nur die Arbeitnehmer in die Berechnung mit einbezogen werden, die im Bereich der Auftragsdatenverarbeitung, also im meldepflichtigen Bereich, tätig sind. Es sind jedoch alle Arbeitnehmer, die mit personenbezogenen Daten umgehen, zu berücksichtigen, also auch diejenigen, die in der eigenen Personal- und Kundenverwaltung tätig sind.

Vielen Unternehmen bereitet es sichtlich Schwierigkeiten, für die Aufgabe des Datenschutzbeauftragten die richtige Person auszuwählen. Bei kleineren Unternehmen fehlt häufig zwischen Geschäftsleitung und Mitarbeitern die mittlere Führungsebene, die in der Regel für diese Aufgabe geeignet ist. Ein Datenschutzbeauftragter darf aber auch nicht durch seine anderweitigen Aufgaben im Unternehmen so belastet sein, daß er die Aufgaben nach dem Bundesdatenschutzgesetz nicht in ausreichendem Maße wahrnehmen kann. Die Arbeitsüberlastung des bestellten Datenschutzbeauftragten war häufig Grund für eine Beanstandung durch die Aufsichtsbehörde. Ist eine Entlastung nicht möglich, so muß gegebenenfalls ein externer Datenschutzbeauftragter bestellt werden, wenn dies von seiten der Aufsichtsbehörde auch nicht als ideale Lösung betrachtet wird, da externe Datenschutzbeauftragte in der Regel nicht in der wünschenswerten Weise mit den internen Gegebenheiten des Betriebes vertraut sind. Zu beachten ist jedoch sowohl bei der Bestellung interner als auch bei der Bestellung externer Datenschutzbeauftragter, daß sie durch die Beibehaltung ihrer anderen Funktionen nicht mehr als unvermeidlich in Interessenkonflikte geraten. Die Aufsichtsbehörden sehen daher die Bestellung des EDV-Leiters, aber auch die Bestellung des Geschäftsführers der Firma, die im Hause die Software liefert und betreut, als nicht zulässig an.

Nach der Forderung des Gesetzes muß der Beauftragte für den Datenschutz die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen (§ 36 Abs. 2 BDSG). In den Kommentaren zum Bundesdatenschutzgesetz wird der Begriff der Zuverlässigkeit in der Regel hauptsächlich mit der Frage einer möglichen Inkompatibilität der Funktionen in Verbindung gebracht. Um der Praxis gerecht werden zu können, ist es jedoch erforderlich, diesen Begriff weiter zu interpretieren. Nur ein engagierter, verantwortungsbewußter Datenschutzbeauftragter wird in der Lage sein, die Unternehmensleitung entsprechend seiner Aufgabe im Hinblick auf die Maßnahmen zum Datenschutz und zur Datensicherung zu beraten und auch dann seine eigene Meinung zu vertreten, wenn ihm andere Interessen des Unternehmens entgegengehalten werden. Eine Bestellung, die sich bei der Überprüfung durch die Aufsichtsbehörde lediglich als eine Maßnahme darstellt, um dem Gesetz Genüge zu tun, entspricht diesen Anforderungen nicht.

Auch die fehlende Fachkunde von betrieblichen Datenschutzbeauftragten war in nicht unerheblichem Umfang Grund für Beanstandungen. Häufig wurde auch hier eine Überlastung des Datenschutzbeauftragten ins Feld geführt. Kann der Datenschutzbeauftragte, insbesondere wegen der Größe des zu betreuenden Unternehmens, seine Aufgabe nicht alleine erledigen, so ist er nach § 36 Abs. 5 BDSG nunmehr berechtigt, vom Unternehmen die Bereitstellung von Hilfspersonal zu verlangen. In vielen Unternehmen, in denen der Datenschutzbeauftragte nicht nur eine Hauptstelle, sondern auch dezentrale Unternehmensteile zu betreuen hat, ist eine Bestellung von Hilfspersonal oder besonders geschulten Ansprechpartnern für den Datenschutzbeauftragten in den Unternehmensteilen sinnvoll. Beispiele dieser Art konnte die Aufsichtsbehörde erfreulicherweise bereits feststellen.

Wünschenswert wäre auch eine bessere Zusammenarbeit zwischen betrieblichem Datenschutzbeauftragten und Betriebsrat. Beide haben in einem wichtigen Bereich der Datenverarbeitung eine gemeinsame Aufgabe, nämlich darüber zu wachen, daß die personenbezogenen Daten der Beschäftigten den Datenschutzregeln entsprechend verarbeitet werden. Nachdem die Novellierung des Bundesdatenschutzgesetzes die Unabhängigkeit des betrieblichen Datenschutzbeauftragten wesentlich mehr betont, als dies früher der Fall war, müßte es möglich sein, im Interesse der Beschäftigten einen Abbau der doch hin und wieder anzutreffenden Fronten zu bewirken. In einigen Unternehmen zeichneten sich auch

erfreuliche Entwicklungen ab. Es wurden Kommissionen gebildet, die mit dem betrieblichen Datenschutzbeauftragten und Fachleuten aller betroffenen Bereiche, also auch des Betriebsrates, besetzt sind und sich umfassend mit der Informationsverarbeitung beschäftigen.

17. Datensicherung

Die nicht-öffentlichen Stellen, die für eigene Zwecke oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des Bundesdatenschutzgesetzes insbesondere die in der Anlage hierzu genannten Anforderungen, zu gewährleisten (§ 9 BDSG). Für Stellen, die personenbezogene Daten nicht automatisiert verarbeiten, ist damit Aufgabe und Ziel abschließend umschrieben. Für die automatisierte Verarbeitung werden in der Anlage zu § 9 Satz 1 BDSG nochmals besondere Sicherungsziele formuliert. Die danach zu treffenden Maßnahmen müssen, wie § 9 Abs. 1 Satz 2 BDSG festlegt, allerdings nur soweit gehen, daß ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Dies bedeutet, daß die "Sensibilität" der Daten, die Verarbeitungszusammenhänge und die Verarbeitungsziele zu berücksichtigen sind, um feststellen zu können, ob die getroffenen Maßnahmen ausreichen.

Hinsichtlich der bei Überprüfungen angetroffenen Datensicherungsmaßnahmen sind wesentliche neue Mängelschwerpunkte im Vergleich zu den bereits in früheren Berichten festgestellten nicht ausdrücklich hervorzuheben. Dennoch soll auf einige Punkte hier besonders eingegangen werden.

17.1 Zugangskontrolle

Die Zugangssicherung ist nach wie vor eines der Hauptprobleme.

In einem Fall hatte eine Bank ein sehr ausgefeiltes Zugangskontrollsystem, eine hintere massive Stahltür im Rechenzentrum war jedoch völlig ungesichert. Diese Tür wurde täglich zum Abtransport von Papierabfällen genutzt. Weite Türen sind sicherlich erforderlich, um größere Transportgegenstände wie Abfalltonnen oder Hardwareeinheiten durchzulassen. Ein Freiraum zur täglichen bequemen Nutzung darf an dieser Stelle aber nicht entstehen. Die Außensicherung ist als eine einheitliche Sicherungsaufgabe zu betrachten. Abseitig gelegene Zugänge dürfen dabei nicht geringer bewertet werden. Im vorliegenden Fall bestanden keine besonderen Gefahren, da auch die genannte hintere Tür noch zum inneren Bankbereich gehörte. Der zu fordernde closed-shop-Betrieb des Rechenzentrums war jedoch durch die geschilderte Schwachstelle aufgehoben. Die teuren Zugangsschleusen insbesondere an dem Hauptzugang zum Rechenzentrum waren gleichsam "durch die Hintertür" entwertet.

Nach wie vor stellt es ein Problem dar, daß zwei Unternehmen, die sich aus ursprünglich einem Unternehmen entwickelt haben, ihre Datenverarbeitung nicht gegeneinander möglichst umfassend abgrenzen. Beide Unternehmen stellen eigene Rechtspersönlichkeiten dar, auch wenn sie wie nicht selten von derselben Person als Geschäftsführer geleitet werden. Oft werden in diesen Fällen dieselben Räumlichkeiten genutzt, ja sogar dieselben Datenverarbeitungsgeräte. Datenschutzrechtlich müssen dennoch die Verantwortungsbereiche klar und nachvollziehbar gegeneinander abgegrenzt sein. Dies bedeutet, sofern nicht Auftragsverhältnisse vorliegen, auch die strikte räumliche Trennung. Diese wurde zum Beispiel von der Aufsichtsbehörde zwischen zwei Unternehmen verlangt , wovon das eine Software erstellte und das andere Marktforschungsdaten verarbeitete und auswertete.

17.2 Zugriffskontrolle

Mit den Maßnahmen zur Zugriffskontrolle soll gewährleistet werden, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Wie bereits in den Vorjahren wurde in etlichen Fällen beanstandet, daß die vollständige Systemberechtigung, also die Berechtigung, auf alle Daten und Dateien zugreifen zu können, an einen viel zu großen Personenkreis vergeben wurde. Eine solch umfassende Berechtigung darf nur einem, allerhöchstens zwei Mitarbeitern gegeben werden.

Nichtsdestoweniger wird die vollständige Systemberechtigung jedoch manchmal als Prestigeangelegenheit betrachtet und zum Beispiel an alle Geschäftsführer ausgegeben, ohne daß sachliche Erwägungen noch eine wesentliche Rolle spielen. Eine Vorsorge für Notsituationen, die zur Rechtfertigung immer angeführt wird, rechtfertigt nach Meinung der Aufsichtsbehörde diese Praxis nicht. Tritt tatsächlich einmal die Situation ein, daß die Benutzung der vollständigen Systemberechtigung erforderlich und der Berechtigte nicht anwesend ist, so kann der Berechtigungscode immer noch verfügbar gemacht werden, wenn er in einem versiegelten Umschlag sicher zum Beispiel bei der Geschäftsleitung hinterlegt ist. Anlaß und Öffnung des Umschlags müssen dann genau protokolliert werden. Außerdem muß nach einer solchen Situation das Berechtigungskennwort geändert werden. Ein in jedem Bericht bisher angesprochenes Problem ist die immer noch zu sorglose Auswahl von Passwörtern. Selbst wenn die von den Aufsichtsbehörden geforderten mindestens sechs Stellen eines Passworts genutzt werden, so sind das eigene Geburtsdatum oder der eigene Name rückwärts gelesen als Passwort gänzlich ungeeignet. Zu empfehlen ist dagegen die Verwendung von aus Buchstaben und Ziffern gemischten Passwörtern. Eine solche Lösung muß nicht so kompliziert sein, daß sich kein Beschäftigter mehr sein Passwort merken kann. Beispielsweise kann ein leicht zu merkender Begriff in der Weise verfremdet werden, daß bestimmte darin vorkommende Buchstaben durch eine bestimmte Ziffer oder durch eine aufsteigende Ziffernfolge ersetzt werden. Der Phantasie sollten hier kaum Grenzen gesetzt sein.

17.3 Eingabekontrolle

Nach Ziffer 7 der Anlage zu § 9 Satz 1 BDSG ist zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind. Im Bereich dieser Forderung sind erhebliche Mängel zu verzeichnen. Gerade bei Auskunfteien hat die oft feststellbare Vernachlässigung der Eingabekontrolle zur Folge, daß im Nachhinein zwar vielleicht noch feststellbar ist, wann Auskünfte über eine bestimmte Person an Dritte gegeben worden sind. Sind zwischenzeitlich die Angaben zu diesem Betroffenen jedoch verändert worden, und liegt der gesamte Vorgang schon einige Zeit zurück, so wird kaum noch nachvollziehbar sein, welchen Inhalt die damals gegebene Auskunft hatte, ob diese Angaben zutreffend waren und welcher Beschäftigte der Auskunftei falsche Daten eingespeichert hat. Im Zusammenwirken damit, daß Auskunfteien, wie oben geschildert, aufgrund spezialgesetzlicher Normen noch nicht verpflichtet sind, die Herkunft der Daten zu dokumentieren, ergeben sich immer wieder Situationen, in denen die Aufsichtsbehörden Beschwerdeführern mitteilen müssen, daß nicht mehr feststellbar ist, aufgrund welcher Ursachen falsche Daten über sie gespeichert und weitergegeben wurden. In mehreren Prüfungen des Berichtsjahres wurden hier Verbesserungen angemahnt.

17.4 Datenträgerkontrolle

Durch die Datenträgerkontrolle soll verhindert werden, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dies gilt auch für die Behandlung von Datenträgern während des Transports (Transportkontrolle). Insbesondere unter der Bedingung des zunehmenden Einsatzes von Personalcomputern mit eigenen Diskettenstationen ist die Datenträgerkontrolle schwierig und wird nach den Feststellungen der Aufsichtsbehörde in vielen Fällen als nicht realisierbar kaum ernst genommen. Hier mangelt es an entsprechendem Bewußtsein sowohl bei den Verantwortungsträgern wie bei den Mitarbeitern. So werden Personalcomputer mit Diskettenstation verwendet, obwohl die Verwendung von Disketten nach Einspielen der Originalsoftware nicht mehr erforderlich ist und auch die Datensicherung mit anderen Mitteln, zum Beispiel über Streamer erfolgen kann. Müssen Disketten verwendet werden, so sind diese oft weder geprüft noch markiert. Eine ordnungsgemäße Diskettenverwaltung ist so nicht möglich. Auch die sichere Aufbewahrung von Disketten ist nicht überall selbstverständlich. Ebenso häufig werden Datenträger völlig ungesichert versendet. Fast alle Maßnahmen, die in der Behandlung von anderen Datenträgern in der EDV üblich sind, werden so mißachtet. Rein sachlich gesehen kann dafür jedoch keine Entschuldigung angeführt werden.

Nur in sehr wenigen Fällen konnte vor Ort festgestellt werden, daß Minimalanforderungen eingehalten werden. Datenträgerkontrolle ist jedoch nur möglich im Zusammenwirken von technischen mit organisatorischen Maßnahmen.

So muß den an PCs Beschäftigten klar gemacht werden, daß mit personenbezogenen Daten beschriebene Disketten nicht nur in verschlossenen Behältnissen, sondern diese geschlossenen Behältnisse nach Arbeitsende auch in verschlossenen Schränken aufzubewahren sind. Je nach Qualität der Daten werden auch noch besondere Anforderungen an die Absicherung der Schränke zu stellen sein. Ein einheitliches Datenträgermanagement ist nur in seltenen Fällen anzutreffen. Es ist dagegen leider festzustellen, daß im Bereich der Benutzung von PCs vergleichsweise der Stand der Ordnungsmäßigkeit der Datenverarbeitung erreicht ist, der bei der Groß-EDV vor 20 Jahren aktuell war.

17.5 Auftragskontrolle

Nach Ziffer 8 der Anlage zu § 9 Satz 1 BDSG ist zu gewährleisten, daß personenbezogene Daten, die im Auftrag bearbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Durch die Novellierung des Bundesdatenschutzgesetzes ist festgelegt, daß diese Weisungen des Auftraggebers in einem schriftlichen Auftrag festzulegen sind (§ 11 Abs. 2 BDSG). Hinter dieser etwas untechnischen Ausdrucksweise des Gesetzes steht die Forderung, daß in dem Vertrag zwischen Auftragnehmer und Auftraggeber die beabsichtigte Datenverarbeitung nicht nur zu bezeichnen ist, sondern auch festgelegt werden muß, ob und welche Subunternehmer für diesen Auftrag eingesetzt werden. Für diesen Auftrag möglicherweise geltende besondere technische und organisatorische Maßnahmen nach § 9 BDSG müssen mit dem Auftraggeber vereinbart werden. Daher ist es nicht ausreichend, wenn in dem Vertragstext lediglich die ohnehin schon für den Auftragnehmer geltende gesetzliche Forderung wiederholt wird, daß er nämlich die nach § 9 BDSG erforderlichen technischen und organisatorischen Maßnahmen zu treffen habe.

Unsicherheit besteht jedoch darin, wie weit ins einzelne gehend die Weisungen des Auftraggebers sein müssen. Für die Forderung, Musterverträge zu erstellen, ist die Aufsichtsbehörde jedoch nicht der richtige Adressat. Gerade in der Formulierung eines allgemein gültigen Vertragstextes dürfte nach dem oben gesagten nämlich ein erhebliches Problem liegen, da in den verschiedenen Branchen viel zu unterschiedliche Verhältnisse herrschen.

Wichtiger als die bis in alle Einzelheiten gehende Beschreibung der erforderlichen technischen und organisatorischen Maßnahmen ist jedoch, daß der Auftraggeber, insbesondere in den Fällen der Beauftragung von Datenerfassern, sich darüber vergewissert, daß der Auftragnehmer bei der zuständigen Aufsichtsbehörde gemeldet ist, und – gegebenenfalls durch eigenen Augenschein – die Verhältnisse beim Auftragnehmer selbst überprüft. Offensichtlich sind sich jedoch manche Auftraggeber – darunter eine große Versicherung und eine große Bundesbehörde – gar nicht darüber im klaren gewesen, wohin manchmal ihre Geschäftsunterlagen geraten, wenn sie zur Datenerfassung an Dritte gegeben werden.

Unter den geprüften Auftragsdatenverarbeitern sind zwei Behindertene inrichtungen besonders zu erwähnen, die im Bereich der Erfassung und Verfilmung arbeiten. Bei einer sinnvollen Gestaltung der Arbeitsplätze und mit der entsprechenden Organisation der Abläufe haben die Einrichtungen erreicht, daß zu betreuende Behinderte in der Datenverarbeitung tätig sein können. Wichtig dabei ist die Lage der Räumlichkeiten in den Einrichtungen. Die Räume sollten so angelegt sein, daß Besucher keinen Zugang haben. Besondere Anforderungen sind an das zur Betreuung vorhandene Personal zu stellen, weil die Anwendung der Vorschriften des Bundesdatenschutzgesetzes besonders praxisorientiert zu erfolgen hat. Bei beiden Einrichtungen gab es unter Berücksichtigung der vorhandenen Besonderheiten keine datenschutzrechtlichen Einwände.

17.6 Organisationskontrolle

Durch Maßnahmen der Organisationskontrolle soll die innerbehördliche oder innerbetriebliche Organisation so gestaltet werden, daß sie den

besonderen Anforderungen des Datenschutzes gerecht wird. Diese Forderung betrifft somit einen sehr weiten Bereich. Besonders betroffen sind die allgemeinen Arbeitsanweisungen an die Mitarbeiter und die Gestaltung der Arbeitsabläufe.

Auch hier ist wieder vor allem der Bereich der Datenverarbeitung auf dem Personalcomputer negativ hervorgetreten. Regelungen zur Verfahrensdokumentation sind oft unbekannt. Programmprüfungen werden als nicht erforderlich angesehen. Listenausdrucke aus diesen Systemen werden weder besonders gesichert aufbewahrt noch gesichert entsorgt. Ausdrucke und – noch problematischer – beschriebene Disketten werden zur Weiterarbeit auf dem privaten PC mit nach Hause genommen. Bei einer Datenverarbeitung, die die gröbsten Risiken vermeiden soll, dürften diese Verfahrensweisen nicht vorkommen. Bemühen ist lediglich zu erkennen bei der Einführung von Arbeitsanweisungen zur Benutzung von PCs. Aber auch hier muß davon ausgegangen werden, daß die bestehende "großzügige" Praxis die Verhaltensweisen bereits geprägt hat.

18. Ordnungswidrigkeitenverfahren

Im Berichtjahr wurden 21 Ordnungswidrigkeitenverfahren eingeleitet.

Wie bereits in den Vorjahren lag der Schwerpunkt der Verfahren bei Verstößen gegen die in § 32 Abs. 1 BDSG geregelte Meldepflicht. Nach dieser Vorschrift haben Stellen, die personenbezogene Daten geschäftsmäßig verarbeiten oder nutzen – wie Auskunfteien, Markt- und Meinungsforschungsunternehmen und Dienstleistungsdatenverarbeiter – die Aufnahme ihrer Tätigkeit der zuständigen Aufsichtsbehörde innerhalb eines Monats mitzuteilen. So hat die Aufsichtsbehörde in 8 Fällen Ordnungswidrigkeitsverfahren wegen verspäteter Abgabe der erforderlichen Meldung eingeleitet (§ 44 Abs. 1 Nr. 2 BDSG), wobei die betroffenen Unternehmen in der Regel bereits 5 bis 10 Jahre die meldepflichtige Tätigkeit ausgeübt hatten. Darüber hinaus hatten 3 Unternehmen Änderungsmeldungen entgegen § 32 Abs. 4 BDSG nicht oder nicht rechtzeitig abgegeben (§ 44 Abs. 1 Nr. 2 BDSG). Auch in diesen Fällen waren die Änderungen etwa der Geschäftsadresse oder der Art der eingesetzten automatisierten Datenverarbeitungsanlagen bereits vor einigen Jahren eingetreten. Bei 3 der Unternehmen, die von Ordnungswidrigkeitsverfahren nach § 44 Abs. 1 Nr. 2 BDSG betroffen waren, kam hinzu, daß seit Jahren entgegen § 36 Abs. 1 BDSG kein Datenschutzbeauftragter bestellt worden war (Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 5 BDSG).

In den 2 weiteren Verfahren waren meldepflichtige Unternehmen der Auskunftspflicht gegenüber der Aufsichtsbehörde aus § 38 Abs. 3 Satz 1 BDSG nicht nachgekommen (Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 6 BDSG).

5 Ordnungswidrigkeitsverfahren sind gegen Auskunfteien eingeleitet worden, weil sie die Betroffenen entgegen § 33 Abs. 1 BDSG nicht von der Datenspeicherung benachrichtigt hatten (Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 3 BDSG).

8 der genannten Verfahren sind bereits durch Bußgeldbescheid rechtskräftig abgeschlossen, in 8 Fällen wurde nach Zustellung der Bußgeldbescheide Einspruch eingelegt. 2 Verfahren wurden eingestellt, in 3 Fällen wurde der Bußgeldbescheid noch nicht erlassen.

Wiesbaden, den 7. August 1992

Der Hessische Ministerpräsident
Eichel

Der Hessische Minister des Innern
und für Europaangelegenheiten
Dr. Günther