14. Wahlperiode

Drucksache **14/299**

HESSISCHER LANDTAG

06. 07. 95

Vorlage der Landesregierung

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

Vorgelegt mit der Stellungnahme zum Dreiundzwanzigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten - Drucks. 13/7165 - nach § 30 Abs. 2 des Hessischen Datenschutzgesetzes vom 11. November 1986.

Eingegangen am 6. Juli 1995 · Ausgegeben am 18. Juli 1995

Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 32 40 · 65022 Wiesbaden

Inhaltsverzeichnis

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

Im Berichtsjahr gingen bei den in Hessen für den Datenschutz im nicht-öffentlichen Bereich zuständigen Regierungspräsidien in Darmstadt, Gießen und Kassel 122 Beschwerden gegen Stellen, die Datenverarbeitung für die Erfüllung eigener Geschäftszwecke betreiben, ein. Alle Beschwerden führten zur Überprüfung der datenverarbeitenden Stellen durch die Aufsichtsbehörden.

Dabei ist grundsätzlich, auch für die Zahlenangaben in den nachfolgenden Kapiteln festzustellen, daß der weitaus überwiegende Anteil der Überwachungstätigkeit vom Regierungspräsidium in Darmstadt zu leisten war.

Die Beschwerden betrafen

- Kreditinstitute in 12 Fällen,
- Kapitalanlagegesellschaften in 10 Fällen,
- den Einzelhandel in 10 Fällen,
- das Gesundheitswesen (Ärzte und Krankenhäuser) in 9 Fällen,
- Kurierdienste in 8 Fällen,
- Vereine in 7 Fällen,
- Versicherungen in 7 Fällen,
- Verlage in 5 Fällen,
- Vermieter in 4 Fällen,
- Kreditkartenunternehmen in 3 Fällen,
- Fluglinien in 3 Fällen,
- den Versandhandel in 3 Fällen,
- Anbieter von Fort- und Weiterbildung in 2 Fällen,
- Reiseveranstalter in 2 Fällen,
- Sicherheitsdienste in 2 Fällen,
- Inkassounternehmen in einem Fall,
- sonstige Unternehmen in 34 Fällen.

In 25 Fällen waren die Beschwerden begründet, davon in drei Fällen gegen Vereine, in je zwei Fällen gegen Kreditinstitute, Versicherungen und Anbieter von Fort- und Weiterbildung sowie in je einem Fall gegen den Einzelhandel, einen Reiseveranstalter, einen Sicherheitsdienst, eine Fluglinie sowie den Versandhandel. Elf weitere begründete Beschwerden richteten sich gegen sonstige Unternehmen.

Bei fünf Beschwerden konnte der den Beschwerden zugrunde liegende Sachverhalt nicht mehr vollständig aufgeklärt werden, so daß eine abschließende Beurteilung, ob die Datenverarbeitung in zulässiger oder in unzulässiger Weise erfolgt war, nicht getroffen werden konnte.
In 51 Fällen sind die Ermittlungen der Aufsichtsbehörden noch nicht abgeschlossen.

Im Berichtsjahr konnten außerdem 28 bereits in den Vorjahren eingereichte Beschwerden abgeschlossen werden. Die Beurteilung der Aufsichtsbehörden ergab, daß davon 12 Beschwerden begründet waren. Dabei hatten in drei Fällen Versicherungen, in je zwei Fällen Kreditkartenunternehmen und der Einzelhandel sowie in je einem Fall ein Hotel, ein Vermieter, ein Verlag, ein Verein und ein Anbieter von Fort- und Weiterbildung personenbezogene Daten unzulässig verarbeitet oder genutzt.
In vier bereits in den Vorjahren eingereichten Fällen konnte eine abschließende Beurteilung, ob die Datenverarbeitung in zulässiger oder in unzulässiger Weise erfolgt war, mangels eindeutigen Sachverhaltes nicht getroffen werden.

Damit liegt der Anteil der begründeten Beschwerden bei ungefähr einem Viertel der den Aufsichtsbehörden zur Überprüfung vorgelegten Fälle.

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

Im Berichtsjahr gingen bei den Aufsichtsbehörden 40 Beschwerden gegen Stellen, die personenbezogene Daten geschäftsmäßig verarbeiten oder nutzen, ein.

Die Beschwerden betrafen
- Kreditinformationsdienste (Wirtschaftsauskunfteien und SCHUFA) in 33 Fällen,

- ein Markt- und Meinungsforschungsunternehmen,
- einen Adreßverlag,
- ein Datenvernichtungsunternehmen und
- weitere Dienstleistungsdatenverarbeiter in vier Fällen.

In fünf Fällen - alle gegen Kreditinformationsdienste - waren die Beschwerden begründet. Bei fünf weiteren Beschwerden - alle gegen eine Wirtschaftsauskunftei, die ihren Betrieb bereits im Vorjahr eingestellt hatte (vgl. Siebter Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden unter Ziffer 5.8) - konnte nicht mehr abschließend festgestellt werden, ob die Datenverarbeitung in zulässiger oder unzulässiger Weise erfolgt war.

In 19 Fällen sind die Ermittlungen der Aufsichtsbehörden noch nicht abgeschlossen.

Im Berichtsjahr wurden außerdem 14 bereits in den Vorjahren eingereichte Beschwerden abgeschlossen. Dabei stellten sich drei Beschwerden gegen Wirtschaftsauskunfteien als begründet heraus.
Bei fünf Beschwerden gegen Wirtschaftsauskunfteien - darunter auch die bereits oben erwähnte Auskunftei - konnte nicht mehr festgestellt werden, ob die Datenverarbeitung in zulässiger oder unzulässiger Weise erfolgt war.

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

3.1 Register

Die Aufsichtsbehörden führen nach § 38 Abs. 2 BDSG ein Register der von Amts wegen zu überprüfenden Stellen, die personenbezogene Daten geschäftsmäßig zum Zweck der personenbezogenen oder der anonymisierten Übermittlung speichern oder im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen. Diese Stellen unterliegen nach § 32 BDSG der Meldepflicht.

Am 1. Februar 1995 waren zu dem Register der meldepflichtigen Stellen bei den Aufsichtsbehörden 601 Unternehmen gemeldet. Im wesentlichen sind dabei die Branchen Auskunfteien, Adreßhändler, Markt- und Meinungsforschungsinstitute sowie Unternehmen, die im Auftrag Dritter Datenverarbeitung als Dienstleistung betreiben - wie Datenerfasser und -entsorger sowie Telefonmarketingunternehmen - erfaßt.

3.2 Prüfungsübersicht

Im Berichtsjahr wurden 74 Prüfungen nach § 38 Abs.2 BDSG durchgeführt. Davon betrafen Datenverarbeiter nach § 32 Abs.1 Ziff. 3 BDSG insgesamt 56, nämlich

- Konzerndatenverarbeiter 17
- Servicerechenzentren 12
- Datenerfasser und Schreibbüros mit Dateiverwaltung 9
- Adreßhändler 9
- Datenträgervernichter 9
- Telemarketing 5
- Mikroverfilmer 1.

Desweiteren wurden 4 Kreditinformationsdienste und 8 Unternehmen aus dem Bereich der Markt- und Meinungsforschung geprüft.
Die Prüfungen brachten folgendes Ergebnis:

- Beanstandungen 22
- Empfehlungen 27
- ohne wesentliche Beanstandungen 25

Folgende wesentliche Mängel wurden am häufigsten festgestellt:

1. keine bzw. verspätete oder unvollständige Registermeldung nach § 32 BDSG
2. keine oder mangelhafte Zugangskontrolle
3. keine oder mangelhafte Zugriffskontrolle
4. kein Datenschutzbeauftragter, Mängel in der Tätigkeit, keine oder zu geringe Mittel
5. fehlende Verpflichtung auf das Datengeheimnis (§ 5 BDSG)
6. keine oder unvollständige Weisungen vom Auftraggeber bzw. an Subunternehmen
7. Mängel in der Datenträgerkontrolle
8. mangelhafte Dokumentation

Neben den Prüfungen im Bereich der Meldepflicht, die immer im Rahmen einer Betriebsbesichtigung durchgeführt werden, wurden nach § 38 Abs.1 BDSG in sieben Beschwerdefällen Überprüfungen "vor Ort" durchgeführt. Eine der Beschwerden ging anonym ein.
Im übrigen wurde bei und einer Prüfung im Regierungsbezirk Neustadt an der Weinstraße Amtshilfe geleistet.

3.3 Meldepflicht bei Service-Datenverarbeitung im Rahmen medizinischer Forschung (Biomonitoring)

Medizinische Marktforschung hat die Verschreibungsgewohnheiten der Ärzte und den Verbrauch beim Kunden (Patienten) zum Gegenstand. Sie unterscheidet sich damit grundsätzlich wenig von der Marktforschung im allgemeinen Konsumbereich.
Werden besondere Unternehmen mit der Marktforschung im medizinischen Bereich beauftragt, so muß bei der Verarbeitung personenbezogener Daten eine Meldepflicht nach § 32 Abs. 1 Ziff. 2 BDSG bejaht werden.

In einem zweiten medizinischen Forschungsbereich wird das Produkt - hier das Medikament - nach § 40 Abs. 1 Ziff. 4 Arzneimittelgesetz (AMG) getestet und die Ergebnisse werden erfaßt und statistisch ausgewertet. Ein Pharmaunternehmen (Sponsor) beauftragt mit einer solchen Studie in der Regel ein Forschungsunternehmen, welches seinerseits einen Leiter für die klinische Prüfung gesetzlich beauftragen muß. Diesem Leiter der klinischen Prüfung wird grundsätzlich eine Studienleitung als Beratungsgremium an die Seite gestellt. Die vom Sponsor oder vom Forschungsunternehmen beauf-

tragten Prüfärzte liefern die Daten der Probanden (Patienten). Das Forschungsunternehmen übernimmt -je nach Vertrag- die Studienkoordination, die Datenerfassung, die Kontrollerfassung, die statistische Auswertung, das Monitoring (= Überwachung der Ärzte) und die Erstellung des Auswertungsberichts.

In anderen Fällen wählt das Pharmaunternehmen(Sponsor) einen geeigneten Leiter der klinischen Prüfung und weitere Prüf-Ärzte/Krankenhäuser selbst und beauftragt das Forschungsinstitut nur mit den Folgearbeiten (z.B. der Datenerfassung und der statistischen Auswertung). Stets wird neben dem mit der medizinischen Durchführung der Studie beauftragten Leiter der klinischen Prüfung eine Studienleitung als Beratungsgremium eingesetzt. Die Ärzte des Beratungsgremiums können u.a. tatsächlichen oder vermeintlichen Verstößen nachgehen.

Das Forschungsinstitut hat nun die Aufgabe, die Daten der Probanden/Patienten (Laborwerte, Arztberichte mit Patientennummer und ggfs. zusätzlichen Initialen des Patienten) zu erfassen und statistisch auszuwerten. Die Identität des Probanden (Patienten) ist nur dem Arzt über die Patientennummer bekannt. Wenn das Forschungsinstitut allerdings auch mit dem Monitoring beauftragt wurde, müssen hierbei teilweise auch die Patientendaten offengelegt werden.

Der Schwerpunkt der Tätigkeit des Forschungsinstituts liegt außerhalb der ärztlichen Sphäre in der Datenerfassung und der Datenverarbeitung. Die Daten werden nach Abschluß aller Prüfungen (auch bzgl. der Prüfärzte) anonymisiert an den Auftraggeber (Sponsor) weitergeleitet und dann - je nach Zielrichtung - vom Auftraggeber auch veröffentlicht.

Die Aufgaben des Forschungsinstitutes, welches sich an Arzneimitteltests beteiligt, sind sicher vielfältiger als in der Konsumgütermarktforschung; die zusätzlichen Aufgaben werden jedoch in der Regel vom Leiter der klinischen Prüfung und vom medizinischem Personal außerhalb des Institutes wahrgenommen. Speichernde Stelle der personenbezogenen Probanden(Patienten-)daten bleibt der Arzt, und die Personenidentität der Betroffenen wird von ihm auch nur in Einzelfällen (z.B. Monitoring) offengelegt. Das Forschungsinstitut ist bei solchen Konstruktionen ein nach § 32 Abs. 1 Ziff. 2 BDSG meldepflichtiges Dienstleistungsunternehmen, welches seinerseits für die Auswertungen lediglich die Daten der beteiligten Prüfärzte anonymisiert.

4. Bearbeitung von Datenschutzverstößen aufgrund sonstiger Anhaltspunkte

Seit der Novellierung des Bundesdatenschutzgesetzes im Jahr 1991 ist es der Aufsichtsbehörde möglich, Datenschutzverstößen nicht nur dann nachzugehen, wenn sie von der betroffenen Person begründet vorgetragen oder zufällig bei Regelüberprüfungen entdeckt werden, sondern auch dann, wenn der Sachverhalt der Behörde auf anderen Wegen, zum Beispiel durch Presseveröffentlichungen oder durch Anzeigen nicht persönlich Betroffener bekannt wird. Im Berichtsjahr hat die Behörde so in drei Fällen Überprüfungen der betrieblichen Datenschutzbeauftragten hinsichtlich ihrer Zuverlässigkeit bzw. Fachkunde eingeleitet, die in einem Fall zur Neubestellung des betrieblichen Datenschutzbeauftragten geführt haben. Aufgrund von Presseveröffentlichungen wurde die Aufsichtsbehörde in zwei Fällen initiativ. In zwei Fällen reklamierte die Aufsichtsbehörde mangelhafte Einwilligungserklärungen für SCHUFA-Übermittlungen bzw. Schweigepflichtentbindungsklauseln. Alle Fälle betrafen Unternehmen, die nicht der Meldepflicht nach § 32 BDSG unterliegen.

5. Wirtschaftsauskunfteien

5.1 Übermittlung von Daten zu "Höchstkrediten"

Anläßlich der Bearbeitung von Beschwerden gegen verschiedene Wirtschaftsauskunfteien hat die Aufsichtsbehörde im Berichtsjahr festgestellt, daß Auskunfteien in ihren Auskünften Aussagen treffen über "zulässige Höchstkredite" bzw. "Kreditrahmen" empfehlen. So wurde in einem Beschwerdefall der anfragenden Stelle über einen Einzelkaufmann mitgeteilt, daß die Geschäftsverbindung zulässig sei, der Höchstkredit jedoch nur 5000 DM betrage. Auf die Anfrage der Aufsichtsbehörde teilte die Auskunftei mit, daß der Höchstkredit in jedem Einzelfall individuell berechnet werde, wobei verschiedene Kriterien, wie z.B. die Branche, der Bonitätsindex und das Reinvermögen - soweit ersichtlich - berücksichtigt werde. In dem fraglichen Fall waren der Auskunftei jedoch nur wenige dieser Kriterien bekannt, einige waren darüber hinaus unrichtig oder lediglich geschätzt.
Bei den Daten zu "Höchstkrediten" handelt es sich, falls eine natürliche Person betroffen ist, um personenbezogene Daten, deren Speicherung und Übermittlung sich nach § 28 BDSG zu richten hat. Für die Schutzwürdigkeit spielt es keine Rolle, ob es sich um objektive Daten oder um subjektive Wertungen der Auskunftei handelt. Die Aufsichtsbehörde betrachtet die Übermittlung solcher Daten sehr kritisch. Selbst wenn die Wertungsgrundlagen objektiv und das Wertungsverfahren logisch ist, können Aussagen zur betroffenen Person entstehen, die nicht mit der Wirklichkeit übereinstimmen. So nimmt eine Kreditauskunftei als Höchstkredit grundsätzlich 10 v.H. des im Handelsregister ausgewiesenen Gesellschaftsvermögens an, wenn die finanziellen Verhältnisse im einzelnen "nicht einsehbar" sind. Insbesondere bei kleineren Gesellschaften mit beschränkter Haftung, deren Gesellschaftsvermögen oft auf die Mindestsumme von 50.000 DM beschränkt ist, muß der Schluß auf eine pro Einzelfall höchstzulässige Kreditierung in Höhe von 5000 DM nicht zwingend sein, ja er kann zu völlig falschen Einschätzungen der Leistungsfähigkeit führen. Sind die Berechnungskriterien gar unrichtig oder zum Teil geschätzt, so verliert eine solche Aussage jeden Bezug zur Wirklichkeit. Die Aufsichtsbehörde hat sich daher diesem Problemfeld verstärkt zugewandt.

6. SCHUFA

In den Vorjahren wurden der Aufsichtsbehörde stets einige begründete Beschwerden von Betroffenen gegen die unzulässige Speicherung oder Übermittlung ihrer personenbezogener Daten durch die SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung) vorgelegt.
Für das Berichtsjahr ist erfreulicherweise festzustellen, daß in diesem Zeitraum keine begründeten Beschwerden wegen unzulässiger Verarbeitung oder Nutzung personenbezogener Daten durch die SCHUFA zu verzeichnen waren.

7. Kreditkartenunternehmen

7.1 Kreditkartenantrag und Einwilligungserklärungen

Die zunehmende Versorgung des Marktes mit Kreditkarten führt für Kreditinstitute und andere Kreditkartenherausgeber dazu, Neuerungen in der Kundengewinnung und in der Risikoverteilung unter den Beteiligten zu überlegen.
So stellte die Aufsichtsbehörde bei einer routinemäßigen Durchsicht von verschiedenen aktuellen Kartenantragsformularen fest, daß ein Kreditkarteninstitut die vor Jahren vereinbarte SCHUFA-Klausel und Datenschutzerklärung auf der Vorderseite des Antragsformulars ersatzlos gestrichen hatte.

Verändert und verkürzt fanden sich diese Einwilligungserklärungen für Übermittlungen an die SCHUFA lediglich auf einem Merkblatt im Vorspann und unter Ziffer 10 von mehreren Einzelziffern der sogenannten Mitgliedschaftsbedingungen.
Einwilligungserklärungen sind jedoch nach § 4 Abs.2 BDSG im äußeren Erscheinungsbild der Erklärung besonders hervorzuheben, wenn die Einwilligung zusammen mit anderen Erklärungen erteilt werden soll. Das Einfügen einer Einwilligungserklärung in umfangreiche allgemeine Geschäftsbedingungen, die der Erklärende zur Kenntnis nehmen kann, jedoch nicht zwingend muß, erfüllt keinesfalls diese Voraussetzungen. Datenschutzrechtlich betrachtet sind sämtliche Datenübermittlungen, die nicht auf der Grundlage von § 28 Abs.1 Ziff.1 oder 2 BDSG erfolgt sind, damit rechtswidrig gewesen. Dies betrifft z.B. alle Einmeldungen dieses Kartenunternehmens an die SCHUFA über die Einrichtung eines Kreditkartenkontos auf der Grundlage dieses Antragsformulars. Das Kreditkartenunternehmen erklärte sich hier umstandslos bereit, den aufgrund gestalterischer Überlegungen zugunsten eines "übersichtlichen" Kartenantrags entstandenen Fehler zu korrigieren und schnellstmöglich das betreffende Formular aus dem Verkehr zu ziehen, bzw. ordnungsgemäße Neudrucke zu veranlassen.

Ein anderes Kreditkartenunternehmen, das aufgrund geplanter haftungsrechtlicher Umstellungen auch die bisher verwendete Datenverarbeitungsermächtigungsklausel verändern muß, verfolgte einen anderen Weg und bat die Aufsichtsbehörde noch in der Planungsphase um beratende Unterstützung.

7.2 Weltweites Telefonieren mit Hilfe einer Kreditkarte

Eine Kreditkartengesellschaft führte als zusätzliche Leistung die weltweite Vermittlung und Abrechnung von Telefonaten mit Hilfe der Kreditkarte ein. Die Leistung stand jedem Kreditkartenteilnehmer ohne besonderen Antrag offen. Die Abwicklung dieses Verfahrens wurde mit Hilfe eines Unternehmens in den USA durchgeführt, dem zu Abrechnungszwecken monatlich aktualisiert die kompletten Kundenstammdaten aus dem Kreditkartenverhältnis übermittelt wurden. Der Kunde, der die Dienstleistung nutzen wollte, konnte dies unter der alleinigen Bedingung tun, daß er seine Kreditkartennummer sowie ein persönliches Paßwort, und zwar sein Geburtsdatum, dem Operator bekanntgab. Nach positivem Abgleich wurde die Verbindung hergestellt.
Die Aufsichtsbehörde monierte hier sowohl die Sicherheit des Verfahrens, da Kreditkartennummer und Geburtsdatum häufig z.B. gegenüber Kfz-Vermietern angegeben werden und damit vielen Dritten bekannt sind. Zudem stellt die komplette Übermittlung aller Kundenstammdaten in die USA ein unzulässige Übermittlung dar. Auf die Intervention der Aufsichtsbehörde gestaltete das Kreditkartenunternehmen die Kartenanträge so um, daß der Kunde seinen Wunsch auf Teilnahme an dieser Dienstleistung positiv bekanntgeben muß. Gleichzeitig mit der Beantragung der Teilnahme an dieser Dienstleistung muß der Kunde ein persönliches Paßwort selbst überlegen und angeben.
Im Antrag wird über den amerikanischen Servicepartner und das Abrechnungsverfahren informiert, so daß dem Kunden die damit verbundene Übermittlung seiner Daten in die USA deutlich wird. Das Abrechnungsverfahren wurde so geändert, daß ausschließlich die Daten von Teilnehmern des Telefonservices in die USA übermittelt werden.
Obwohl hier durch die erforderliche Neugestaltung der Formulare und Verfahren in nicht unerheblichem Umfang Kosten anfielen, ist die Bereitschaft des Unternehmens hervorzuheben, die datenschutzrechtlichen Forderungen in Zusammenarbeit mit der Aufsichtsbehörde zu konkretisieren und umzusetzen.

8. Versicherungen

Auch im Berichtsjahr wurden bei der Aufsichtsbehörde Beschwerden gegen Versicherungen eingereicht. Obwohl die Anzahl der Beschwerden gegen Unternehmen aus der Versicherungsbranche im Vergleich zu den Vorjahren zurückgegangen ist, hat der Anteil der begründeten Beschwerden gegenüber den Vorjahren erheblich zugenommen.

8.1 Der Kettenbrief

Eine Versicherungsnehmerin beschwerte sich bei der Aufsichtsbehörde darüber, daß sie per Post einen Kettenbrief erhalten hatte, auf dem als Absender ein sie betreuender Versicherungsvertreter angegeben war. Da der Betroffenen der Versicherungsvertreter lediglich in seiner Funktion als Mitarbeiter der Versicherung bekannt war, ging sie davon aus, daß der Vertreter die Daten der Versicherten zweckwidrig für private Zwecke genutzt hatte. Die Ermittlungen der Aufsichtsbehörde bestätigten diese Vermutung. Eine Nutzung von Daten von Versicherungsnehmern zum Zwecke der Versendung von Kettenbriefen stellt eine unzulässige Nutzung personenbezogener Daten dar, da für eine solche Nutzung keine Rechtsgrundlage besteht. Die Nutzung von geschäftlich erhaltenen personenbezogenen Daten für den Zweck der Verbreitung eines Kettenbriefes hat nämlich weder etwas mit dem eigentlichen Vertragszweck einer Versicherung zu tun, noch können dafür berechtigte Interessen der Versicherung oder des Versicherungsvertreters geltend gemacht werden. Vielmehr stehen schutzwürdige Belange der betroffenen Versicherungsnehmerin gegen eine solche Verwendung.

8.2 Ein hartnäckiger Irrtum

Eine andere Versicherungsnehmerin bat die Aufsichtsbehörde um Unterstützung bei der Wahrung ihrer datenschutzrechtlichen Belange. Sie hatte von ihrer Lebensversicherung ein ungefähr sechs Monate zuvor datiertes und an eine ihr unbekannte Adresse gerichtetes Schreiben mit der Mitteilung erhalten, dieser an die der Versicherung bisher bekannte Adresse der Betroffenen gerichtete Brief sei als unzustellbar zurückgesandt worden. Die Versicherungsgesellschaft teilte weiter mit, sie habe nun erfahren, daß die Versicherungsnehmerin - die seit 25 Jahren bei diesem Unternehmen versichert war und seit fast 15 Jahren ununterbrochen unter derselben Adresse wohnte - jetzt eine neue Anschrift habe. Bei der angeblich neuen Anschrift handelte es sich tatsächlich aber um die alte Adresse.

Die Beschwerdeführerin erinnerte sich daran, daß sie einige Jahre zuvor von dem Unternehmen ein Schreiben erhalten hatte, das eine ihr unbekannte Versicherte betraf, jedoch an sie adressiert war. Damals hatte sie das Schreiben an die Versicherung zurückgesandt und von dort die Mitteilung erhalten, es habe sich um einen Irrtum gehandelt.

Die Betroffene wandte sich nun nochmals zunächst an das Versicherungsunternehmen, da sie davon ausging, daß die Angelegenheit rasch geklärt werden könne. Da ihr der Datenschutzbeauftragte der Versicherung jedoch lediglich mitteilte, daß die Adresse durch eine versehentliche Eingabe im Kundensatz geändert worden sei und er sich ansonsten von der Korrektheit der Adresse im EDV-System überzeugt habe, wandte sich die Beschwerdeführerin nun an die Aufsichtsbehörde, da sie die Ursache des Versehens ermittelt haben wollte.

Innerhalb weniger Wochen erhielt die Versicherungsnehmerin dann fünf Schreiben der Gesellschaft, die nicht ihr Versicherungsverhältnis, sondern

das einer Dritten betrafen. Darunter befanden sich Berechtigungsscheine für die Verteilung von Überschüssen sowie ein Antrag über die Auszahlung einer Versicherungsleistung.

Da die Versicherungsgesellschaft davon ausging, daß es sich bei der Beschwerdeführerin um die Versicherungsnehmerin handelte, wäre es ihr aller Wahrscheinlichkeit nach problemlos möglich gewesen, sich die offensichtlich einer dritten Person zustehenden Leistungen auch auszahlen zu lassen.

Wie die Ermittlungen der Aufsichtsbehörde ergaben, war bereits einige Jahre zuvor durch ein nicht mehr nachvollziehbares Versehen eines Versicherungsmitarbeiters die Kundennummer der Beschwerdeführerin mit der Kundennummer einer anderen Versicherten gleichen Vor- und Zunamens verknüpft worden. Dieses Versehen wurde erst aufgrund der Ermittlungen der Aufsichtsbehörde bemerkt.
Selbstverständlich waren aus datenschutzrechtlicher Sicht die Übermittlungen personenbezogener Daten einer dritten Versicherungsnehmerin an die Beschwerdeführerin unzulässig.

9. Datenverarbeitung im medizinischen Bereich

9.1 Chipkarte für Arzneimittel

Bereits Ende 1993 hatte die Bundesvereinigung Deutscher Apothekenverbände sich mit einem Konzept einer sog. "A-Card" an die Öffentlichkeit und dann auch an die verschiedenen Datenschutzaufsichtsinstanzen gewandt. Auf der A-Card sollen durch Arzt oder Apotheker Medikationen abgespeichert werden. Der Patient ist im Besitz der Karte und soll bestimmen, welche Medikationen eingetragen werden und wer für diese Speicherungen leseberechtigt sein soll. Der Bezug und die Benutzung der Karte ist für den Patienten bzw. Apothekenkunden freiwillig. Der Betroffene soll in Apotheken jederzeit über dort zur Verfügung stehende Geräte den Speicherinhalt selbst prüfen und erforderlichenfalls löschen können.
Hier wie bei anderen im Gesundheitsbereich geplanten Kartenprojekten stehen grundsätzliche Fragen der Erhaltung und Sicherung von Persönlichkeitsrechten zur Debatte. Wegen ihrer grundsätzlichen Bedeutung ist die Thematik auch im Gesprächskreis der obersten Datenschutzaufsichtsbehörden Diskussionsgegenstand. Von wesentlicher Bedeutung wird die Gestaltung und Formulierung des Kartenantrags bzw. der damit verbundenen Informationsmaterialien sein, da sich hieraus die den Betroffenen zustehenden Rechte an der Karte und an den darin enthaltenen Informationen sowie den Möglichkeiten des Umgangs damit klar und deutlich ergeben müssen. Zu verkennen ist auch nicht die Gefahr, daß verschiedene bisher noch getrennt geplante Kartenprojekte vereinigt werden und dann Daten, die bisher unterschiedlichen Zwecken zugeordnet und auch nur getrennt verfügbar sind, auf einer einzigen, dann sehr informationsbeladenen Karte zusammengeführt werden. Nicht umsonst ist die strikte Speicher- und Zweckbegrenzung eine Kernforderung für die seit 1.1.1995 bundesweit eingeführte Chipkarte der gesetzlichen Krankenversicherung.

9.2 Datenverarbeitung in der Arztpraxis

Wie in jedem Jahr gab es auch im Berichtsjahr Beschwerden über die Art und Weise, wie in einzelnen Arztpraxen mit personenbezogenen Patientendaten umgegangen wird.
Voranzustellen ist, daß die Frage, ob in einer Arztpraxis überhaupt eine von der Aufsichtsbehörde zu kontrollierende Dateiverarbeitung betrieben wird,

zunehmend in den Hintergrund tritt, da fast durchgängig die Patientendaten bereits automatisiert durch Personalcomputer verarbeitet werden. Eingaben, die die Aufsichtsbehörde erreichen, betreffen zum Beispiel häufig die Aufstellung von PC-Bildschirmen, aber auch die Ablage von schriftlichen Patientenunterlagen in einer Weise, die anderen Patienten die Kenntnisnahme von Daten erlaubt. So wurden in einer Gemeinschaftspraxis zweier Ärzte die Patienten durch das Personal in jeweils freie Untersuchungsräume gebeten, die schriftlichen Unterlagen zu dem jeweiligen Patienten wurden in durchsichtige Plexiglastaschen gesteckt, die sich im Flur vor dem jeweiligen Untersuchungsraum befanden. Da Patienten zum Teil auch vor den einzelnen Räumen warten mußten und nicht immer durch das Personal beobachtet werden konnten, war es nicht ausgeschlossen, daß die auf den Faltkarteikarten vorne notierten "Stammdaten" des Patienten, durch die Plexiglastasche Dritten zur Kenntnis gelangten. Hier mußte sichergestellt werden, daß die Daten zumindest nicht ohne weiteres lesbar waren. Nach etwas mühsam errungener Einsicht erklärten die Ärzte sich bereit, die Taschen so zu verändern, daß nicht sofort ersichtlich war, ob überhaupt Unterlagen darin stecken.
Abgelehnt wurde der Vorschlag, die Unterlagen der Patienten jeweils beim zentralen Arbeitsplatz der Gehilfinnen abzuholen, da die damit für die Ärzte verbundenen Wege für nicht zumutbar gehalten wurden. Die Aushändigung der Unterlagen an den wartenden Patienten als weitere Alternative wurde wegen schlechter Erfahrungen ebenfalls abgelehnt.

9.3 Vernichtung von Mikrofilmen und Röntgenfilmen

Bei der Vernichtung von Papier haben sich inzwischen Standards entwickelt (Sammlung in verschlossenen eingriffssicheren Behältnissen, Transport im verschlossenem Fahrzeug, Vernichtung in geschlossenen Räumen), die eigentlich auch bei der Vernichtung von Mikrofilmen und Röntgenfilmen zur Anwendung kommen müßten. Mikrofilme - insbesondere Röntgenfilme - besitzen häufig einen besonders schutzwürdigen Charakter, weil hier - teilweise mit komplett angefügten Diagnosen - auch personenbezogene medizinische Daten betroffen sind. Die insoweit bei einer Überprüfung festgestellten Zustände können jedoch nur als erschreckend bezeichnet werden. Das Problem liegt nicht primär auf der Seite des Vernichters, der im geprüften Fall sofortige organisatorische Maßnahmen ergriffen hat und mit Umbauten die Sicherheit verbessern will, sondern auf der Seite des Lieferanten - d.h. des Unternehmens, des Krankenhauses, des Arztes. Viel zu oft wird von diesen Stellen nicht darauf geachtet, unter welchen Umständen das sensible Datenmaterial entsorgt wird. In der Regel bekommt der billigste, nicht der sicherste Anbieter den Zuschlag. Weisungen nach § 11 BDSG existieren so gut wie nie. Der Transport geschieht in offenen Behältnissen und auf teilweise offenen Fahrzeugen. Der Vernichter erhält in der Regel keinen Hinweis auf die Brisanz des Materials. Dies führt oft dazu, daß - vergleichbar beim Altpapierverwerter - das Material unbestimmt lange ungesichert (zwischen)gelagert wird und - wie nicht nur einmal festgestellt - auf dem Hof des Vernichters vom Boden aufgelesen werden kann.

Die Aufsichtsbehörde hat in solchen Fällen dem Entsorger empfohlen, seine Kunden (Filmlieferanten) über deren Sorgfaltspflicht aufzuklären und eine datenschutzgerechte Vernichtung als Zusatzleistung anzubieten.

Sachgerechter wäre es, die Filme beim jeweiligen Verursacher (z.B. im Krankenhaus) zu zerkleinern und dann erst zur Entsorgung zu geben. Da kein Entsorger bekannt ist, der einen sicheren Transport in verschlossenen Behältnissen zur Datenvernichtung anbietet, würde eine derartige Vorgehensweise auch das offensichtliche Transportproblem lösen.

10. Arbeitnehmerdatenschutz

10.1 Bewerberdaten

Ein nicht unerheblicher und wachsender Anteil von Eingaben und Beschwerden stammt aus dem Bereich des Arbeitnehmerdatenschutzes.
Telefonische Anfragen betreffen hier häufig die Problematik der Erhebung von Bewerberdaten. Arbeitsplatzbewerbern werden vom künftigen Arbeitgeber umfangreiche Fragebögen vorgelegt, die oft nicht nur zulässige Fragen enthalten, deren Beantwortung für die Entscheidung des Arbeitgebers über die Einstellung wesentlich ist, sondern auch Fragen nach persönlichen Umständen, die allenfalls in einem Vorstellungsgespräch gestellt werden sollten, so nach familiären Zusammenhängen oder Hobbys. Da hier bei Nachprüfungen der Aufsichtsbehörde stets der Name des Betroffenen angegeben werden muß, kommt es allerdings relativ selten zu Überprüfungen. Die Bedenken der Betroffenen, daß ihnen dadurch Nachteile entstehen könnten, sind groß. Aber auch wenn die Aufsichtsbehörde den Fall aufnehmen kann und die Umstände der Datenverarbeitung bzw. -erhebung prüfen will, müssen die Ermittlungen oft eingestellt werden, weil Bewerberdaten meistens nicht in Dateien gespeichert werden, sondern die ausgefüllten Fragebögen in Akten abgelegt werden. Da die Aufsichtsbehörde jedoch nur dann Einzelfälle auf die Einhaltung des Datenschutzes überprüfen kann, wenn und soweit personenbezogene Daten in oder aus Dateien verarbeitet werden, kann sie die Betroffenen in solchen Fällen lediglich auf ihre arbeitsrechtlichen Möglichkeiten verweisen.

10.2 Einholung von Auskünften über Arbeitnehmer auf dem Weg über die Einwilligung

Das Fragerecht des Arbeitgebers hat durch die Rechtsprechung der Arbeitsgerichte im Laufe der Zeit fest umrissene Grenzen bekommen. Keine gesetzlichen oder höchstrichterlichen Entscheidungen gibt es jedoch zu der Frage, ob dem Arbeitgeber in irgendeiner Weise Grenzen gesetzt sind, wenn er Informationen über den Bewerber oder Arbeitnehmer, die ihm sonst nicht zugänglich wären, auf dem Umweg über die Einwilligung des Betroffenen oder die Ausnutzung seiner Rechte auf Selbstauskunft (dazu vgl. Tätigkeitsbericht für das Jahr 1993, Ziff. 9.1) zu erlangen versucht. So hatte ein mittelständisches Unternehmen, wie dessen Betriebsrat mitteilte, geplant, Arbeitnehmern und Bewerbern formularmäßig Erklärungen mit der Bitte um Unterzeichnung vorzulegen, mit denen diese den Arbeitgeber ermächtigen sollten, bei der zuständigen Krankenkasse Auskünfte über Vorerkrankungen und Kuren mit Zeiten und Diagnosen der letzten drei Jahre sowie über anstehende Heilverfahren einzuholen. Begründet wurde dieses Vorhaben durch die Personalverantwortliche damit, daß man nur auf diese Weise imstande sei, sich vor Langzeitkranken zu schützen, die in letzter Zeit sehr häufig wären.
Die folgende Prüfung der Aufsichtsbehörde geschah unter der Annahme, daß ihre Zuständigkeit gegeben war, weil die erbetenen Verlaufsdarstellungen, offensichtlich aus einer Datei entnommen werden und wohl auch dateimäßig gespeichert werden sollten.
Hier mußte die geplante Datenerhebung als rechtswidrig beurteilt werden. Dabei ist die Datenerhebung auf dem Weg über die Einwilligung des Bewerbers bzw. Arbeitnehmers nach denselben Grundsätzen zu beurteilen, wie sie durch das Bundesarbeitsgericht auch für die Datenerhebung direkt beim betroffenen Bewerber/Arbeitnehmer entwickelt worden sind. Zu gestatten, daß darüber hinaus Daten per Einwilligung der Betroffenen nach § 4 BDSG erhoben werden dürfen, würde bedeuten, das Abhängigkeitsverhältnis zwischen Bewerber/Arbeitnehmer und dem Arbeitgeber völlig außer acht zu lassen. Da Sozialdaten betroffen waren, mußte auch § 32 des Sozialgesetzbuches Teil I berücksichtigt werden, der verbietet, daß das Sozialgeheimnis

durch privatrechtliche Vereinbarungen zum Nachteil des Sozialleistungsberechtigten eingeschränkt wird.
In diesem Fall wurde auch der Hessische Datenschutzbeauftragte eingeschaltet, um bei der Krankenkasse zu prüfen, ob das Unternehmen dort bereits ohne Kenntnis des Betriebsrats Auskünfte angefragt oder eingeholt hatte.

10.3 Übermittlungen von Arbeitnehmerdaten

10.3.1 Die gehäuften Krankheitsausfälle

Ein ähnlicher Hintergrund wie in dem oben geschilderten Fall lag einer anderen Beschwerde gegen Übermittlungen von Arbeitnehmerdaten zugrunde.
Aufgrund einer Teilbetriebsstillegung wurden in der Montageabteilung eines Unternehmens etliche Aufhebungsverträge zwischen Arbeitnehmern und Arbeitgeber geschlossen. In der Folgezeit schnellte nach Ansicht des Unternehmens die Krankheitsrate in dieser Abteilung auffällig in die Höhe. Wegen sechs namentlich mit Versicherungsnummer und Daten wie Schwerbehinderteneigenschaft genannten Beschäftigten richtete der Arbeitgeber daraufhin eine Anfrage an die zuständige Krankenkasse mit der Bitte um Überprüfung der Krankschreibungen. Durchschriften dieses Schreibens schickte er ohne irgendwelche Schwärzungen auch an die ihm bekannten jeweiligen Hausärzte der Betroffenen. Unabhängig davon, daß in diesem Zusammenhang auch durch den Hessischen Datenschutzbeauftragten die Praxis der Beantwortung solcher Anfragen durch die Krankenkasse geprüft wurde, kam die Aufsichtsbehörde zu dem Ergebnis, daß hier unzulässigerweise Daten von Arbeitnehmern an Dritte, nämlich die jeweils den Betroffenen nicht behandelnden Ärzte, übermittelt worden waren. Offensichtlich sollte damit nachdrücklich auf die Hausärzte eingewirkt werden.

10.3.2 Mitarbeiterfehlliste

Ein datenschutzrechtlich kritischer "Verbesserungsvorschlag" wurde der Aufsichtsbehörde aus dem Bereich der Mitarbeiterschaft eines Unternehmens zur Beurteilung vorgelegt.
Alle an dem PC-Netz des Unternehmens angeschlossene Mitarbeiter sollten täglich eine aktuelle "Mitarbeiterfehlliste" abfragen können, in der Name, Telefonnummer, Abteilung bzw. Stelle und Dauer der Fehlzeit aller Mitarbeiter gespeichert sein sollten.
Die Aufsichtsbehörde betrachtete auch ohne Speicherung des Grundes der Abwesenheit diesen Vorschlag als bedenklich, da nur den personalverwaltenden Stellen, nicht jedoch jedem Mitarbeiter das Recht zusteht, über An- bzw. Abwesenheiten der Mitarbeiter informiert zu sein. Die Information von Mitarbeitern ist nur dann statthaft, wenn ein in der Arbeitsabwicklung liegender Grund sie zur Kenntnis berechtigt, z.B. im Vertretungsfall. Es besteht zudem die Gefahr, daß genaue Abwesenheitsstatistiken über einzelne oder sämtliche Beschäftigte aufgebaut werden, wozu allein die Personalverantwortlichen berechtigt sind.
Aus denselben Gründen hat die Aufsichtsbehörde stets das betriebsöffentliche Aushängen von An- bzw. Abwesenheitszeiten z.B. in Jahreskalendarien, das vielerorts üblich ist, aus datenschutzrechtlicher Sicht kritisch betrachtet, wenn es über den überschaubaren Arbeitsbereich des Einzelnen hinausgeht oder weitergehende Angaben enthält, z.B. "krank", "Urlaub", "Bildungsurlaub" etc.

10.3.3 Übermittlung an beherrschende Unternehmen

Durch Konzentrationsmaßnahmen verlieren immer mehr Unternehmen ihre Selbständigkeit, wenn sie aufgekauft und in - internationale - Konzerne eingegliedert werden. In mehreren Fällen wurde der Aufsichtsbehörde die Frage vorgelegt, ob es mit dem Datenschutz zu vereinbaren sei, wenn das neue herrschende Unternehmen bzw. die Konzernspitze verlangt, daß sämtliche oder bestimmte Arbeitnehmerdaten zur Verfügung gestellt werden.
Die Weitergabe von Arbeitnehmerdaten eines rechtlich selbständigen Unternehmens an einen Dritten stellt stets eine Übermittlung dar, auch wenn der Dritte über gesellschaftsrechtliche und vertragliche Regelungen das andere Unternehmen beherrscht. Daher muß für jede einzelne vorzunehmende Übermittlung eine Rechtsgrundlage entweder aus § 28 BDSG oder aus § 4 BDSG (Einwilligung) gegeben sein. Solange keine Betriebsübernahme stattgefunden hat, also ein neuer Arbeitgeber an die Stelle des alten Arbeitgebers getreten ist, kann nicht davon ausgegangen werden, daß die Übermittlung von Arbeitnehmerdaten an das beherrschende Unternehmen im Rahmen der Zweckbestimmung des - einzelnen - Arbeitsverhältnisses gerechtfertigt ist (§ 28 Abs Ziff. 1 BDSG). Eine Rechtfertigung der Übermittlung nach § 28 Abs. 2 Ziff. 1 a BDSG setzt eine Einzelfallsicht voraus, wobei zwar durchaus ein berechtigtes Interesse des beherrschenden Unternehmens an der Kenntnis bestimmter Daten z.B. von Führungskräften anzuerkennen ist. Gerade hier muß allerdings auch in der Regel ein schutzwürdiges Interesse der Betroffenen an dem Ausschluß der Übermittlung angenommen werden, da ein Druck auf diese Arbeitnehmer mit dem Ziel der Auflösung von Arbeitsverhältnissen bzw. der Auswechslung bestimmter Personen nicht von der Hand zu weisen ist.
Nicht unter die Übermittlungsvorschriften fallen anonymisierte Informationen z.B. über Anzahl, Berufsgruppe, Ausbildung, Betriebszugehörigkeit, Geschlecht oder Altersgruppe, sofern die Angaben trotz Anonymisierung nicht einer einzelnen Person zugeordnet werden können. Personenbezogene Übermittlungen an das herrschende Unternehmen können dagegen nur mit Einwilligung des jeweils Betroffenen rechtmäßig durchgeführt werden.
Inwieweit durch eine Betriebsvereinbarung mit normativer Kraft eine Berechtigung zur Übermittlung von Arbeitnehmerdaten geschaffen werden kann, ist sehr fraglich, da Eingriffe in den besonders geschützten Persönlichkeitsbereich des einzelnen Arbeitnehmers einer kollektiven Regelung unzugänglich sind.

10.3.4 Datenbank für Fahrgemeinschaften

Einen guten Zweck verfolgte ein Bürger mit seinem Plan, eine Datenbank aufzubauen und öffentlich anzubieten, die potentielle Interessenten für Fahrgemeinschaften zur Arbeit zusammenbringen sollte. Arbeitgeber sollten Name, Wohnort, Arbeitsort und dienstliche Telefonnummer ihrer Beschäftigten in die Datenbank melden. Suchte jemand eine regelmäßige Mitfahrmöglichkeit, so sollte sein Wunsch mit den in der Datei vorhandenen Angaben über Start und Ziel abgeglichen werden und die gespeicherten Arbeitnehmer über den Mitfahrwunsch informiert werden. Damit sollte eine direkte Übermittlung von Daten an den Anfrager vermieden werden. Die gespeicherten Arbeitnehmer sollten sich vielmehr selbst entscheiden können, ob sie Kontakt zu dem Anfrager aufnehmen wollen.
Trotz dieser Datenschutzbelange bereits berücksichtigenden Regelung mußte die Aufsichtsbehörde diesem Vorhaben entgegentreten. Die Übermittlung von Arbeitnehmerdaten an die - externe - Datenbank wäre rechtlich nur zulässig auf der Grundlage einer schriftlichen Einwilligung jedes einzelnen Arbeitnehmers. Eine Rechtfertigung über die gesetzlichen Erlaubnistatbestände des § 28 Abs BDSG ist dagegen nicht möglich, da die Übermittlungen nicht der Abwicklung des Arbeitsverhältnisses dienten und trotz

des Ausschlusses der weiteren Übermittlung an Dritte gerade im Arbeitsverhältnis strenge Maßstäbe bei der Abwägung der beiderseitigen Interessen gegeneinander anzulegen sind.

11. Auslandsdatenverarbeitung

In vielen Fällen spielen inzwischen grenzüberschreitende Datenverarbeitungen wie selbstverständlich mit hinein. So wurde die Aufsichtsbehörde des öfteren um die Beurteilung von Outsourcing-Verträgen mit ausländischen Auftragnehmern aus datenschutzrechtlicher Sicht gebeten. Ebenso wie es in inländischen Auftragsverhältnissen sehr oft Mängel an den nach § 11 BDSG erforderlichen Weisungen gibt (s. dazu unten Ziff.16.3), wird dies auch und wohl in verstärktem Maße für grenzüberschreitende Auftragsverhältnisse anzunehmen sein, da hier ausländische Partner in der Regel weniger Verständnis für datenschutzrechtliche Forderungen haben, wie der Aufsichtsbehörde des öfteren entgegengehalten wird. In den Fällen, in denen aufgrund einer Einzelfall- oder Regelprüfung oder aufgrund der Bitte um Bewertung solche Verträge überprüft werden, wendet die Aufsichtsbehörde neben den auch im Fall der Auslandsbeteiligung geltenden Regeln des § 11 BDSG, insbesondere hier dessen Absatz 2, die von den obersten Aufsichtsbehörden 1993 erarbeitete "Checkliste" zu möglichen und empfohlenen Inhalten von Datenschutzverträgen (vgl. Tätigkeitsbericht für das Jahr 1993, 11.1) an.

Einen Fall mit größerer Öffentlichkeitswirkung stellte das im Berichtsjahr neu eingeführte Datenverwaltungssystem der Firma United Parcel Service (UPS) dar.
Die Auslieferungsfahrer von UPS führen einen tragbaren Pen-Computer, genannt DIAD, mit sich, in dem die Daten der Tagesauslieferungen gespeichert sind. Wird ein Paket abgegeben, so setzt der Empfänger seine Empfangsquittung nicht mehr auf Papier, sondern er muß auf einem Schreibfeld des DIADs mit einem speziellen Stift quittieren, nachdem zuvor über eine Tastatur sein Name eingegeben worden ist. Die Unterschrift wird im dem Gerät digital gespeichert. Die Daten über die erfolgte Paketauslieferung werden innerhalb kürzester Zeit nach der Auslieferung über Funk und das unternehmenseigene Netz an das amerikanische Rechenzentrum von UPS gesendet, so daß Auftraggeber (Paketabsender) sich noch am selben Tag die Bestätigung der Durchführung des Auftrags geben lassen können.
Vor allem angesichts der Neuerung, daß eine Unterschrift auf einem elektronischen Gerät gegeben werden muß, wandten sich viele Betroffene an die Datenschutzbeauftragten der Länder und die Aufsichtsbehörden. Allgemein wurde die Frage gestellt, wie mit der digitalisiert gespeicherten Unterschrift von dem Unternehmen umgegangen wird, ob die Unterschrift auf dem Gerät statt wie bisher auf Papier geleistet werden müsse und - vor allem - ob die so gespeicherten und übermittelten Daten auch vor mißbräuchlicher Verwendung geschützt seien.
Die für den Sitz des Unternehmens in Hessen zuständige Aufsichtsbehörde leitete eine Überprüfung ein, die sich jedoch bisher, insbesondere was den technischen Bereich der Datensicherheit betrifft, schwierig gestaltete, da revisionsfähige Unterlagen durch das Unternehmen monatelang nicht vorgelegt werden konnten. Hinsichtlich der Datenübermittlungen in die Vereinigten Staaten zeigte das Unternehmen die Bereitschaft, auf Forderungen der Aufsichtsbehörde hinsichtlich der Verbesserung der datenschutzrelevanten Vereinbarungen mit dem amerikanischen Mutterunternehmen einzugehen. Auch hier sind allerdings noch keine abschließenden Regelungen getroffen worden. Der Fall zeigt deutlich die Schwierigkeiten auf, mit denen Aufsichtsbehörden und deutsche Niederlassungen ausländischer Unternehmen umzugehen haben.
In vielen Unternehmen, die von - ausländischen - Unternehmen abhängig sind und in denen die Datenverarbeitung im Wege des Outsourcing dem

herrschenden Unternehmen überlassen ist, gibt es lediglich ein Anwenderwissen über die Datenverarbeitung. Selbst die Datenverarbeitungsvorgänge, die noch im Einflußbereich des deutschen Rechts bzw. der deutschen Unternehmensorganisation stattfinden, sind für diese nicht mehr von den Grundlagen her überschaubar und revisibel.
Prüfungen der Aufsichtsbehörde sind auf einer solchen Grundlage nicht möglich. Der Aufsichtsbehörde stehen zwar die Möglichkeiten eines Ordnungswidrigkeitenverfahrens z.B. wegen Nichterteilung von Auskünften oder einer Anordnung nach § 38 Absatz 5 BDSG zur Verfügung. Um in angemessener Zeit zu Prüfergebnissen und gegebenenfalls zu Verbesserungen der Verarbeitungsbedingungen zu kommen, ist sie jedoch auf die Kooperation mit den beteiligten Unternehmen angewiesen.

12. Werbewirtschaft

12.1 Nutzung personenbezogener Daten bei Kapitalanlageunternehmen

Die Beschaffung von Adreßdaten potentieller Interessenten für Werbeaktionen ist des öfteren in einer Grauzone angesiedelt, wobei mehrfach festgestellt werden mußte, daß die Datenerhebung gegen § 28 Abs. 1 letzter Satz BDSG (Erhebung nur nach Treu und Glauben und auf rechtmäßige Weise) verstieß.

In einem Fall trat das Unternehmen erst als Markt- und Meinungsforscher auf und nutzte kurz darauf diese Informationen für gezielte Kapitalanlagenwerbung. Bei der Überprüfung teilte der hierfür Verantwortliche mit, daß der betreffende Mitarbeiter entlassen worden sei und derartige Aktionen keinesfalls autorisiert gewesen seien.

In einem anderen Fall wurde anonym bei der Datenschutzaufsichtsbehörde angezeigt, daß ein Anlageberatungs- und vermittlungsunternehmen systematisch personenbezogene Daten (Name und ggfs. Titel, Firmenanschrift, geschäftliche Telefonnummer) von leitenden Mitarbeitern mehrerer großer deutscher Unternehmen aus deren internen Firmentelefonbüchern entnommen und in einer Datenbank gespeichert habe. Den Betroffenen seien dann telefonisch Kapitalanlagenangebote gemacht worden. Das betroffene Unternehmen stritt diesen Sachverhalt entschieden ab. Es konnte jedoch aufgrund der vorgefundenen abweichenden Namensschreibweise in mehreren Einzelfällen nachgewiesen werden, daß Daten einem internen Telefonbuch entnommen worden waren.
Da die Daten nicht nach Treu und Glauben und auf rechtmäßige Art und Weise erhoben wurden (vgl. § 28 Abs. 1 letzter Satz BDSG), ist die Erhebung und damit auch die folgende Speicherung rechtswidrig. Rechtswidrig waren die Speicherungen allerdings auch bereits deswegen, weil das damit beabsichtigte "kalte Telefonmarketing" wettbewerbswidrig war und als berechtigtes Interesse für die Speicherung nicht gelten kann.
Rechtswidriges "kaltes Telefonmarketing" liegt nach der Rechtsprechung des Bundesgerichtshofs (In NJW 91, S. 2087) auch dann vor, wenn geschäftliche Telefonnummern für eindeutig auf private Verfügungszwecke zielendes Marketing genutzt werden. Damit soll das grundsätzlich auch am Arbeitsplatz dem Betroffenen zustehende Recht auf Nichtbeeinträchtigung durch werbende Telefonanrufe geschützt werden, das als Teil des Persönlichkeitsrechts einen sehr hohen grundgesetzlich geschützten Rang hat.

Inwieweit eine Speicherung der Daten ohne Telefonnummer nach § 28 Abs. 1 Ziff. 2 BDSG zulässig wäre, war für die festgestellten Fälle irrelevant, da eine solche Speicherung nicht festgestellt werden konnte. Für Zwecke der schriftlichen Werbung ist eine Speicherung und Nutzung jedoch nur ohne die Telefonnummer zulässig.

12.2 Anti-Abtreibungswerbung

Bereits im Siebten Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden wurde unter Ziff. 13.1 von einem Verein berichtet, der sich u.a. zum Ziel gesetzt hat, gegen die Liberalisierung des Abtreibungsrechts einzutreten. Dieser Verein hatte unverlangte Werbesendungen an Bürger gerichtet, die auf einer Adreßliste "rechtskonservativer Verteilerkreis" geführt wurden. Wie weitere Ermittlungen der Aufsichtsbehörde im Berichtsjahr ergaben, nutzte der Verein auch weitere Adreßlisten mit Titeln wie "konservativer Bereich" und "konservativer Pool". Die Nutzung oder Übermittlung solcher Adreßlisten ist nach § 28 Abs.2 BDSG jedoch in der Regel nicht zulässig, da die Daten sich auf - wahre oder vermutete - politische Anschauungen beziehen.
Im Berichtsjahr beschwerten sich wiederum etliche Bürger gegen die Zusendung des Werbematerials dieses Vereins. So wandten sich Eltern von Kindern im Grundschulalter zunächst an die Presse, dann an die Aufsichtsbehörde, da das Werbematerial mit zum Teil sehr drastischen Bildern und Schilderungen von Abtreibungsmethoden direkt an ihre Kinder gerichtet worden war.
Wie die Ermittlungen der Aufsichtsbehörde ergaben, hatte der Verein die Daten der Kinder über ein Subunternehmen bei einem Adreßverlag angemietet. Die Adreßliste enthielt nach den Angaben des Adreßverlags überwiegend weibliche Bezieher einer Zeitschrift für Kinder zwischen fünf und zehn Jahren. Der kirchliche Zeitschriftenverlag, der die Adreßliste vermietet und jede Nutzung dieser Adreßdaten genehmigen muß, war sich nicht im klaren darüber, daß als Bezieher auch die Adressen von Kindern selbst enthalten waren, die ein Abonnement z.B. von Verwandten geschenkt erhalten hatten.
Die Aufsichtsbehörde hat hier festgestellt, daß die Nutzung der betroffenen Kinderadressen rechtswidrig war. Verantwortlich dafür ist das werbende Unternehmen, in diesem Fall der Verein. Die Nutzung von Adressen Minderjähriger für Werbemailings ist zwar immer problematisch, wenn auch mit zunehmendem Alter der Kinder und Jugendlichen, angepaßt an das beworbene Produkt, immer weniger. Der aktuelle Fall bezog seine besondere Brisanz jedoch zusätzlich aus dem Inhalt der Mailings, bei denen auch im Fall der Adressierung an Erwachsene eine Beeinträchtigung von Persönlichkeitsrechten nicht ganz fern lag.

13. Banken

Im Berichtsjahr gab es sehr wenige Eingaben, die sich gegen Banken richteten. In drei Einzelfällen beschwerten sich Bankkunden darüber, daß sie bei der Eröffnung von Konten bzw. bei der Beantragung von Krediten um ihre Personalausweise gebeten worden waren, obwohl sie z.B. als langjährige Kunden bestens bei dem Institut bekannt gewesen seien. Die Personalausweise sollten unter Berufung auf das Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz) vom 25.10.1993 fotokopiert und die Kopien archiviert werden. Die Betroffenen empfanden dies auch als Verstoß gegen den Datenschutz, da sie sich als "Verdachtsfälle" eingeordnet sahen. Die Geldinstitute, gegen die sich die Beschwerden richteten, waren von der Bitte der Aufsichtsbehörde, zu den dargestellten Vorgehensweisen aus datenschutzrechtlicher Sicht Stellung zu nehmen, nicht besonders angetan. Die neuen Vorschriften hatten nämlich ohnehin bereits für Verdruß gesorgt wegen der auf die betroffenen Institute zukommenden zusätzlichen Aufgaben. So muß vor der Annahme von Bargeld, Wertpapieren oder Edelmetallen im Wert von 20 000 DM und darüber die Identität des Kunden festgestellt und soweit möglich durch Kopie der vorgelegten Dokumente festgehalten werden. Von einer Identifizierung kann nur abgesehen werden, wenn der Kunde beim jeweiligen Angestellten des Instituts persön-

lich bekannt ist und sich zudem bereits früher durch Vorlage seines Ausweises identifiziert hat. Die betroffenen Institute beriefen sich auch auf § 154 Abs. 2 der Abgabenordnung, wonach sie sich z.B. vor einer Kontoeröffnung Gewißheit über die Person und Anschrift des Verfügungsberechtigten zu verschaffen und die entsprechenden Angaben in geeigneter Form festzuhalten haben.

Die Aufsichtsbehörde für den Datenschutz konnte hier nur tätig werden, wenn es sich bei der Aufbewahrung der Ausweiskopien um eine dateimäßige Speicherung handelte. So war zunächst als Vorfrage zu klären, in welcher Form die Kopien aufbewahrt werden. Wurden sie in den einzelnen Kundenakten abgeheftet, so lag keine Datei-, sondern eine Aktenverarbeitung vor, und die Aufsichtsbehörde war nicht zuständig. Wurden die Kopien chronologisch nach dem Datum ihrer Erstellung in Ordnern abgelegt, so handelte es sich um eine Datei, und die Aufsichtsbehörde war zuständig. Bereits für diese Vorfrage wurde seitens der Institute und der Betroffenen wenig Verständnis aufgebracht.

In der Frage, ob Ausweisdaten überhaupt erfaßt und gespeichert werden dürfen, konnte eine Annäherung der Standpunkte nicht erreicht werden. Die Institute beriefen sich auf Verlautbarungen ihrer Verbände und des Bundesaufsichtsamts für das Kreditwesen und interpretierten diese sehr großzügig so, daß nunmehr bei allen Geschäften nach § 154 der Abgabenordnung, also auch bei Konteneröffnungen mit Bareinzahlungen unter 20.000 DM, Kopien der Ausweise erstellt werden sollten. Dem Hinweis, daß eine Datenspeicherung nach § 4 BDSG eine Rechtsgrundlage entweder durch Einwilligung des Betroffenen oder durch Gesetz, und nicht durch Verlautbarungen von Behörden oder Verbänden, benötige, wurde kaum Gehör geschenkt. Der jüngste Beschwerdefall, anläßlich einer Eröffnung eines Jugendkontos mit einem Betrag von 20 DM, ist noch in Bearbeitung.

14. Wohnungsmiete

14.1 Warndatei über Mietverhältnisse

Der Deutsche Mieterbund machte die Aufsichtsbehörde auf die Gründung einer Gesellschaft aufmerksam, deren Geschäftszweck die Erstellung einer Warndatei über Mietverhältnisse darstellt.
Vermieter werden als Mitglieder geführt und erhalten gegen entsprechendes Entgelt auf Anfrage Auskünfte über Mietinteressenten. Das System ist auf Gegenseitigkeit aufgebaut, d.h. das Vereinsmitglied erhält auf Anfrage nicht nur Auskünfte, sondern soll auch seine Erfahrungen mit seinen Mietern in die Warndatei einmelden. Zur Eingabe vorgesehen waren neben Name und Anschrift Daten wie

- positives Mietverhältnis
- Störung des Hausfriedens
- verspätete Mietzahlungen
- vertragswidriger Gebrauch von Wohnraum
- mutwillige Zerstörung von Wohnraum
- Sonstiges.

Dazu wurden Name und Mitgliedsnummer des derzeitigen Vermieters gespeichert.

Die Vermieter sollten von den betroffenen Mietern Einwilligungserklärungen zur Übermittlung von Daten in die Warndatei abverlangen.
Als Auskunft sollte der Vermieter - je nach vorhandener Eintragung in der Warndatei - alternativ drei Hinweise erhalten:

- Eintragung vorhanden
- keine Eintragung vorhanden
- nicht bekannt.

Dem Unternehmen wurde von der Aufsichtsbehörde mitgeteilt, daß seine gegenwärtige Konzeption als Auskunftssystem über Mieter aus datenschutzrechtlicher Sicht nicht zulässig ist bzw. ein Warnsystem über Mieter allenfalls unter sehr eingeschränkten Voraussetzungen akzeptiert werden kann.

Eine Einwilligung i.S.d. § 4 Abs. 1 BDSG setzt eine freiwillige vorherige Zustimmung des Betroffenen voraus. Der Betroffene darf zur Abgabe jedoch nicht genötigt sein oder sich in einer Situation befinden, die ihm keine Möglichkeit zu einer eigenen, selbständigen Entscheidung läßt, so daß die Einwilligung nur einen scheinbar von ihm gebilligten Vorgang abdeckt (Simitis, in Simitis/Dammann/Geiger/Mallmann/Walz, Kommentar zum BDSG 4. Auflage, Stand Juli 1994, § 4 BDSG Rdnr. 27).
Die Situation des Betroffenen als Mietinteressent kann jedoch sehr oft dazu führen, daß keine echte Alternative zur Einwilligung vorhanden ist. Der Mietinteressent wird diese meist erteilen, damit er nicht schon aufgrund dieser Verweigerung als Mieter ausgeschlossen wird. Insofern kann eine Einwilligungsaufforderung vor Abschluß des Mietvertrags datenschutzrechtlich nicht akzeptiert werden.

Nach § 29 Abs. 1 Satz 1 Nr. 1 BDSG ist das geschäftsmäßige Speichern oder Verändern personenbezogener Daten zum Zwecke der Übermittlung zulässig, wenn kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Speicherung oder Veränderung hat. Bei der erforderlichen Interessenabwägung sind dabei Art, Inhalt und Aussagekraft der betreffenden Daten an den Aufgaben und Zwecke zu messen, denen ihre Verarbeitung dient. Die Angaben des Vermieters betreffend "positives Mietverhältnis, Störung des Hausfriedens, verspätete Mietzahlungen, vertragswidriger Gebrauch von Wohnraum sowie mutwillige Zerstörung von Wohnraum" sind als solche zunächst nicht hinreichend objektiv. Vielmehr stammen diese Daten aus der subjektiven Einschätzung des Vermieters. Diese konkreten Daten werden zwar nicht an die anfragenden Vermieter weitergegeben, die Auskunft "Eintragung vorhanden" indiziert jedoch das Vorliegen eines dieser Alternativen. Dem Interesse des Vermieters/Verpächters, vor finanziellen Verlusten im Vermietungs- und Verpachtungsgeschäft durch insolvente Mieter geschützt zu werden, steht das Interesse des Mieters am Besitz von Wohnraum gegenüber. Würde die Warndatei der Vermieterschutzbörse in der vorgesehenen Form verwirklicht, so müßte dies für eine darin mit Negativdaten erfaßte Person dazu führen, daß dieser die Beschaffung einer neuen Wohnung nahezu unmöglich gemacht oder zumindest erheblich erschwert wird. Dem Rechtsgut "Wohnraum" kommt jedoch eine elementare Bedeutung zu, die in dieser Situation gegenüber dem Zweck der beabsichtigten Datenverarbeitung höher zu bewerten ist. Ein überwiegendes Interesse des Vermieters, vor sog. Problemmietern geschützt zu werden, könnte nur dann bejaht werden, wenn gravierende Vertragsverletzungen nachweisbar vorliegen. Als Nachweise kämen z.B. rechtskräftige Räumungstitel oder fruchtlose Zwangsvollstreckungsmaßnahmen aus früheren Mietverhältnissen in Frage. Die denkbare Speicherung von Daten aus öffentlich zugänglichen Quellen, wie z. B. dem Schuldnerverzeichnis ist nur in den Fällen zulässig, in denen die Eintragungen auf einem vertragswidrigen Verhalten aus dem Mietverhältnis beruht.

Solche Daten dürfen jedoch nicht ohne zeitliche Begrenzung gespeichert werden. Es sollte eine Löschung der Daten nach 3 Jahren vorgesehen werden. Die Entwicklung dieser Warndatei wird von der Aufsichtsbehörde sehr aufmerksam beobachtet.

14.2 Mieterfragebögen und SCHUFA-Selbstauskünfte

In mehreren Fällen wurde die Aufsichtsbehörde auf Datenerhebungen durch Großvermieter aufmerksam gemacht. Den Mietern wurden Fragebögen vorgelegt, in denen beispielsweise nach Geburtsname, Familienstand, Nationalität, Geburtsdatum, Beruf und Arbeitgeber gefragt wurde. Solche Daten werden in der Regel auch in automatisierte Dateien aufgenommen. Darüberhinaus werden bis ins einzelne gehend Daten zu Vermögen und Einkünften, Schulden und andere bonitätsrelevante Fakten abgefragt. Soweit diese Daten nicht in automatisierte Verarbeitungen übernommen werden, besteht allerdings keine Prüfungskompetenz der Aufsichtsbehörde.
Auch die Vorlage von SCHUFA-Selbstauskünften als Voraussetzung für den Abschluß eines Mietvertrages wurde moniert.
Nachdem es zunächst in der Regel nicht einfach war, die betroffenen und zum Teil ohne Ankündigung aufgesuchten Vermietungsunternehmen von der Berechtigung aufsichtsbehördlichen Tätigwerdens zu überzeugen, wurde offensichtlich, daß hier im Bemühen um größtmögliche Absicherung der Vermieterinteressen zum Teil erheblich über das Ziel hinausgeschossen wird.
Was Vermieter oft als "Selbstverständlichkeit" betrachten, nämlich die Erfassung und Verarbeitung von Daten der Mietbewerber, bedarf nach geltender Rechtslage stets einer Rechtsgrundlage. Sofern der Vermieter jedoch nicht darlegen kann, inwieweit bestimmte Daten für Zwecke der Durchführung des Mietverhältnisses dienlich und erforderlich sind, d.h. auch inwieweit berechtigte Interessen des Vermieters an der Verarbeitung gegeben sind, kann eine Verarbeitung nur auf der Grundlage der freien Einwilligung des Mietbewerbers zulässig sein. Zweifel waren damit an der Zulässigkeit der - dateimäßigen - Speicherung der oben genannten Daten angebracht. Begründbar ist allerdings in bestimmten Fällen die Frage nach der Nationalität, um eine ungünstige, erfahrungsgemäß oft zu nachbarschaftlichen Konflikten führende Zusammensetzung der Mieterschaft eines Hauses zu vermeiden.

Die Anforderung und Ablage von SCHUFA-Selbstauskünften in Vermieterakten ist als nicht zulässige Datenverarbeitung zu betrachten. Zunächst einmal ist hier trotz Aktenverarbeitung eine Prüfungskompetenz der Aufsichtsbehörde gegeben, da es sich bei SCHUFA-Selbstauskünften stets um Daten handelt, die offensichtlich aus einer Datei entnommen sind (§ 27 Abs. 2 BDSG). Der Auskunftsanspruch des Betroffenen nach § 34 BDSG soll dazu dienen, diesem Klarheit über die zu seiner Person gespeicherten Daten zu verschaffen; darüber hinaus erfährt der Betroffene daraus auch, wer in den letzten 12 Monaten zu seiner Person bei der SCHUFA angefragt hat. Die Auskünfte, die die SCHUFA anfrageberechtigten Dritten gibt, sind dagegen von streng begrenztem Umfang. Anfrageberechtigt sind nur Unternehmen, die Geld- oder Warenkredite vergeben oder die wegen der Überlassung hochwertiger Konsumgüter ein besonderes Interesse an der Überprüfung der Bonität der Kunden haben, wie z.B. Autoleasingunternehmen. Vermieter gehören nicht zum anfrageberechtigten Personenkreis. Die Umgehung dieser mit den Aufsichtsbehörden seit langem geklärten Zugangsbeschränkung zu den Daten der SCHUFA durch Anforderung einer Selbstauskunft gerade bei Mietbewerbern, also einer Gruppe, die ebenso wie Arbeitsplatzbewerber in einer besonderen Zwangssituation stehen, wird als Verstoß gegen Treu und Glauben gewertet. Dem kann nicht entgegengehalten werden, daß dieses Verfahren wohl inzwischen in breitem Umfang üblich geworden ist. Im Gegenteil verschärft sich unter solchen Bedingungen die Zwangssituation für den Betroffenen, der zunehmend nicht mehr die Wahl hat, sich an eine Stelle zu wenden, die nicht vor Abschluß eines Mietvertrages die weitgehende Offenbarung seiner personenbezogenen Daten von ihm verlangt. Da die Erhebung rechtswidrig ist, ist auch die Speicherung, d.h. Aufbewahrung der Auskunftsbögen rechtswidrig. Einer Speicherung steht im übrigen auch entgegen, daß Vermieter an der dauernden Aufbewahrung sämtlicher in der

Selbstauskunft enthaltenen personenbezogenen Daten kein berechtigtes Interesse haben können.

15. Der betriebliche Beauftragte für den Datenschutz

15.1 Fehlende Bestellung eines betrieblichen Datenschutzbeauftragten

Bei Überprüfungen vor Ort, insbesondere bei nicht meldepflichtigen Stellen, ergab sich oft, daß ein betrieblicher Beauftragter für den Datenschutz nicht bestellt war, obwohl nach § 36 Abs 1 BDSG dies erforderlich gewesen wäre.
Bei der Verarbeitung personenbezogener Daten in automatisierten Verfahren ist ein betrieblicher Datenschutzbeauftragter zu bestellen, wenn mindestens fünf Arbeitnehmer im Rahmen ihrer Tätigkeit - auch - mit personenbezogenen Daten umgehen.
Diese Zahl ist auch in kleineren Unternehmen schnell erreicht, wenn die individuelle Datenverarbeitung über Personalcomputer eingeführt wird. Aber nicht nur bei der individuellen Datenverarbeitung zeigen sich diese Versäumnisse, sondern auch bei größeren Datenverarbeitungsanlagen. So sah z.B. ein Unternehmen in seinem ursprünglichen Geschäftsbereich, der Markt- und Meinungsforschung keine weiteren Entwicklungsmöglichkeiten. Man diversifizierte in einen neuen Bereich der Datenverarbeitung, nämlich der Adressenverwaltung für verschiedene Auftraggeber. Dafür wurde ein System installiert, bei dem sieben Bildschirmendgeräte installiert wurden. Für jeden Auftraggeber wurde eine eigene Datenbank aufgebaut und entsprechend gepflegt.
Dieses Unternehmen argumentierte damit, daß man doch keine personenbezogenen Daten verarbeite. Es würden lediglich Name, Anschrift, Telefonnummer, die Kundennummer und allenfalls ein Hinweis zur Kundenbetreuung verarbeitet.
Da jedoch mehr als fünf Mitarbeiter mit der automatisierten Verarbeitung zweifellos personenbezogener Daten beschäftigt waren, bestand hier die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten.

15.2 Versäumnisse in der Tätigkeit

Insbesondere bei meldepflichtigen Unternehmen mußte bedauerlicherweise mehrmals im Berichtsjahr festgestellt werden, daß zwar ein betrieblicher Datenschutzbeauftragter bestellt und auch nach § 32 Abs. 2 Nr. 5 BDSG der Aufsichtsbehörde gemeldet worden war, daß aber diese Person keine Tätigkeiten im Unternehmen - auch nur ansatzweise - durchgeführt hatte. Da auch erhebliche Mängel in der Fachkunde des Bestellten vorlagen, wurde dem Unternehmen zur Abwendung eines Ordnungswidrigkeitenverfahrens empfohlen, den Bestellten zunächst zu Fortbildungsmaßnahmen zu schicken. Bei einer unangekündigten Nachkontrolle stellte sich sehr schnell heraus, daß dem nicht nachgekommen worden war. In solchen Fällen wird die Vorlage von Teilnahmebestätigungen verlangt. Darüber hinaus wird angeregt, daß der Datenschutzbeauftragte entsprechende Unterlagen über seine Tätigkeit führt, mit denen er den Umfang seiner Tätigkeit gegebenenfalls nachweisen kann.

15.3 Probleme der Datenschutzbeauftragten

Aber auch bei ordnungsgemäßer Bestellung eines Datenschutzbeauftragten sind die Probleme dadurch noch nicht gelöst.
So klagen weiterhin viele Datenschutzbeauftragte über mangelndes Verständnis für Datenschutz und Datensicherheit im Unternehmen sowohl im Bereich der Geschäftsführung als auch im Bereich der Mitarbeiter. Daß Datenschutz und Datensicherheit in Zukunft immer mehr ein wesentlicher

Faktor für den Erfolg des Unternehmens sein wird, setzt sich als Überzeugung nur sehr langsam durch.
Ein ganz wesentlicher Problembereich liegt darin, daß im Zuge von Personalabbau der Datenschutzbeauftragte zusätzliche Aufgaben übertragen erhält, oder - bei Neubestellungen - von vorneherein garnicht oder in nicht ausreichendem Umfang von bisher ausgeübten Aufgaben entlastet wird. In etlichen Fällen wurde hier die Aufsichtsbehörde um Hilfe gebeten. Dabei konnten auch Kompromisse gefunden werden, die wenigstens zu einer Mindestfreistellung von anderen Aufgaben führten. So änderte die Geschäftsleitung eines Unternehmens ihre Ansicht, daß für ihre Bedingungen (1200 Mitarbeiter an drei Betriebsorten mit komplexen vernetzten Systemen und Auslandsbezug) ein Anteil von 6 v.H. der Normalarbeitszeit für den Datenschutzbeauftragten ausreichen müsse, dahin, daß ihm nunmehr probeweise ca. 25 v.H. der Arbeitszeit dafür zur Verfügung stehen.
Letztlich mit dieser Zeitfrage, die in Zusammenhang zu sehen ist mit einer notwendigen persönlichen Unabhängigkeit und damit der Möglichkeit zum Engagement, steht und fällt die interne betriebliche Datenschutzkontrolle.
Der Datenschutzbeauftragte wird auch häufig nicht bei allen relevanten Entscheidungen angehört. So erfährt der Datenschutzbeauftragte häufig nicht, daß Mitarbeiter umgesetzt werden, daß neue Stellen eingerichtet werden oder daß Positionen besetzt werden, für die seine Mitwirkung (§ 37 Abs. 1 Nr. 3 BDSG) erforderlich ist.

16. Datensicherheit

In den letzten Jahren hat insbesondere die zunehmende Installation von PCs als Einzelgeräte oder in Netzwerken zu Problemen in der Datensicherheit geführt. Während der Blick der Hersteller und auch der Anwender vorwiegend auf die Steigerung der Rechnerleistung und auf Kostenersparnis gerichtet war, wurde ein wichtiger Aspekt erst spät angegangen: die Datensicherheit. Das Bundesdatenschutzgesetz schreibt jedoch auch für Datenverarbeitungen auf solchen Anlagen Datensicherungsmaßnahmen vor. Unabhängig davon, ob es sich um eine Großrechneranlage handelt oder um einen Einzel-PC, ist z.B. zu gewährleisten, daß Unbefugten der Zugang zu verwehren ist, wenn darauf personenbezogene Daten verarbeitet werden (Zugangskontrolle, Ziff. 1 der Anlage zu § 9 BDSG). Selbst solche einfachen, mit herkömmlichen Mitteln wirksam zu lösende Anforderungen werden jedoch oftmals nicht eingehalten.
Dies soll entsprechend der oben (Ziff. 3.2) festgestellten Häufigkeit an Einzelfällen dargestellt werden.

16.1 Zugangskontrolle

16.1.1 Innerbetriebliche Zustellung von DV-Auswertungen

Die besten Zugangskontrollen sind wertlos, wenn personenbezogene Daten von Unbefugten im Klartext ausgedruckt, fotokopiert und - mißbräuchlich - verwendet werden können.
Derartige Kenntisnahmen werden in der Regel eher zufällig und nicht zielgerichtet erfolgen, weil ein potentieller Angreifer in der Regel nicht weiß, wann bestimmte Daten ausgedruckt und in die interne Post gelegt werden.
In größeren Unternehmen hat es sich eingebürgert, daß DV-Ausdrucke - sofern sie nicht gleich am Arbeitsplatz ausgedruckt werden - per Boten oder über Schließfächer zugestellt werden.
Persönliche Schließfächer stoßen jedoch teilweise auf Akzeptanzprobleme, da jeder Berechtigte selbst sich zu seinem Schließfach bemühen muß.

Hier läßt sich Abhilfe schaffen, indem Schließfächer bestimmten gleich zugangsberechtigten Mitarbeiter-Gruppen - z.B. Personalabrechnung, Debitoren, Kreditoren - zugeordnet werden.
In einem geprüften Fall wurden die Schließfächer vom Rechenzentrum gefüllt; jeder Mitarbeiter konnten allerdings - ohne das Öffnen des für ihn berechtigten Faches - über einen gesonderten Zugang von der Rückseite her die Fächer entleeren. Hier hätte man sich die teure Anlage auch sparen können, ein einfaches Regal hätte den gleiche Zweck erfüllt.
Die Aufsichtsbehörde hat hier gefordert, daß die Schließfachanlage wieder wie ursprünglich geplant in Betrieb genommen und der Zugang zum Rechenzentrum geschlossen wird.

16.1.2 Zugang für mehrere Unternehmen

Bei der Regelüberprüfung eines Outsourcing-Unternehmens stellte die Aufsichtsbehörde folgendes fest: Die gemieteten Räume des Unternehmens befanden sich in einem Gebäudeteil, der auch vom Vermieter genutzt wurde. Das Treppenhaus teilte die Räumlichkeiten. Zusätzlich waren zwei Räume an ein befreundetes Unternehmen untervermietet. Ein Rechner und ein Server waren am Ende eines Ganges installiert. Der Rechner diente nur der Datenübertragung zwischen Auftraggeber und Auftragnehmer. Eine Stellwand teilte diesen hinteren Teil vom restlichen Flur, aus dem man in alle Büroräume gelangte, ab.
Die Aufsichtsbehörde verlangte die vollständige Trennung der verschiedenen Unternehmen in räumlicher Hinsicht sowie die Verlegung der Rechner in abschließbare Räume.

16.2. Zugriffskontrolle

16.2.1 Paßwortschutz

Wie bereits im letzten Tätigkeitsbericht dargestellt (Ziff.19.2) ist es durchaus vorteilhaft, wenn mit Tabellen die Nutzung mehrerer Paßworte dergestalt vereinheitlicht wird, daß ein Mitarbeiter sich nur ein Paßwort merken muß, selbst wenn mehrere unterschiedliche Paßworte in den verschiedenen Anwendungen verwendet werden müssen. Dies hat allerdings zur Voraussetzung, daß das Paßwort überall gleichermaßen geschützt wird. Eine verschlüsselte Speicherung des Paßwortes in den Systemen ist mittlerweile Standard. Es darf jedoch nicht passieren - wie dies in einem geprüften Falle entdeckt wurde -, daß eine Tabelle zur Verknüpfung der Paßworte in den unterschiedlichen Systemen mit allen gültigen Paßworten völlig unverschlüsselt abgelegt ist. Hier liegt der Generalschlüssel für jegliche Selbstbedienung bereit. Das betroffene Großunternehmen hat diesbezüglich eine Verbesserung des Schutzniveaus in Aussicht gestellt.

Allgemein üblich ist eine Paßwortnutzungsdauer von 30 Tagen bei mittlerem Schutzbedarf. Wenn die Mitarbeiter und Mitarbeiterinnen räumlich sehr beengt sitzen, kann aber auch dies schon zu lang sein. Die bei einem stark dialogorientierten Unternehmen vorgefundene Nutzungsdauer desselben Paßworts von 60 Tagen wurde von der Aufsichtsbehörde daher aus grundsätzlichen Überlegungen abgelehnt.

16.2.2 Help Desk

Das Problem der heutigen vor allem dezentralen automatisierten Datenverarbeitung liegt u.a. darin, daß einerseits die Anwendungen immer einfacher ausführbar werden, andererseits diese Vereinfachung durch immer kompliziertere Programme im Hintergrund ermöglicht wird. Zwangsläufig führt

dies dazu, daß ein Help Desk oder sogenannte Technik-Berater dem Benutzer öfter Hilfestellung leisten müssen. Werden von diesen Experten bei solcher Tätigkeit personenbezogene Daten nur - zwangsläufig - zur Kenntnis genommen, um z.B. Fehler beseitigen zu können, ist dies - trotz der auch hierbei bestehenden Mißbrauchsmöglichkeit - noch relativ unproblematisch.
Kritisch wird es jedoch, wenn der Berater - u.U. unter der Kennung des Hilfesuchenden - selbst Eingaben oder Veränderungen vornehmen kann, jedoch nicht als Betriebsfremder dokumentiert wird. Es besteht zwar die Möglichkeit, daß der befugte Anwender auf dem Bildschirm die Aktivitäten des Help-Desk verfolgen kann. Die damit noch gegebene Kontrolle entfällt jedoch, wenn nach Arbeitsende des Anwenders noch Daten durch den Help-Desk verändert werden, damit z.B. Fehler in der Dateneingabe nicht zu einem Abbruch der Tagesverarbeitung führen. Solche Eingriffe sind nur tolerierbar, wenn der Ausführende dokumentiert (Eingabekontrolle) und der Anwender hierüber detailliert benachrichtigt wird.

16.3. Auftragskontrolle

Nach Ziff. 8 der Anlage zu § 9 BDSG hat der Auftragnehmer zu gewährleisten, daß personenbezogene Daten, die er im Auftrag für seinen Auftraggeber verarbeitet, nur entsprechend der Weisungen dieses Auftraggebers verarbeitet werden. Vorausgesetzt werden damit Weisungen des Auftraggebers, die dieser nach § 11 Abs. 2 BDSG dem Auftragnehmer zu erteilen hat. Darin sind die Datenverarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen.
Bei Überprüfungen von Auftragsdatenverarbeitern, die nach § 32 Abs. 1 Ziff. 3 BDSG zum Register gemeldet werden müssen, wird neben anderen Unterlagen auch die Vorlage dieser Weisungen verlangt. In bedenklich vielen Fällen fehlen allerdings solche Weisungen oder sind höchstens rudimentär in schriftlichen Aufträgen zu finden. Formulierungen wie die pauschale Zusicherung, daß die Vorschriften des Bundesdatenschutzgesetzes eingehalten werden, können von der Aufsichtsbehörde nicht als ausreichend anerkannt werden. Verlangt wird eine auf den konkreten Auftrag und die konkreten Verarbeitungsbedingungen zugeschnittene schriftliche Fixierung zu sämtlichen Kontrollzielen der Anlage zu § 9 BDSG, soweit sie für die betreffende Verarbeitung relevant sind.
Verantwortlich für das Fehlen von Weisungen ist allerdings nicht der geprüfte Auftragnehmer, sondern der Auftraggeber, an den sich das Gebot der Auftragskontrolle richtet.

16.4 Organisationskontrolle

Neben verschiedenen Richtlinien und Anweisungen ist im Rahmen der Organisationskontrolle eine Verfahrensdokumentation zu fordern, wenn diese nicht bereits zur Erfüllung der Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden, durch den Datenschutzbeauftragten geschaffen worden ist.
Was letztendlich alles zu einer Dokumentation gehört, hängt von dem einzelnen Verfahren ab. Daß aber überhaupt dokumentiert werden muß, ist unbestritten - auch ohne Berücksichtigung der Vorschriften des BDSG - für eine ordnungsgemäße Datenverarbeitung erforderlich.
Viele Unternehmen sind sich der möglichen Tragweite einer fehlenden Verfahrensbeschreibung nicht bewußt. Viele Geschäftsabläufe werden mit Hilfe automatisierter Verfahren abgewickelt. Immer häufiger ist keiner der Mitarbeiter mehr in der Lage, diese automatisierten Verfahren manuell auszuführen. Um so unverständlicher ist dann, daß eine individuelle Fremd-Software ohne eine ausführliche Dokumentation gekauft wird. Diese

Software wird in der Regel vom Hersteller installiert, der auch für ihre Wartung zuständig ist. Normalerweise wird lediglich eine sogenannte Anwenderbeschreibung mitgeliefert. Die Aussagen solcher Anwender-/Benutzerbeschreibungen beschränken sich jedoch häufig auf Empfehlungen wie: "Wenn Cursor blinkt, Maus klicken, nächste Seite...". Was passiert jedoch, wenn der Software-Lieferant ausfällt? Was passiert, wenn er seine Stellung ausnutzt?
Zumindest sollte daher vertraglich eine Dokumentationspflicht des Software-Herstellers vereinbart sein mit dem Zusatz, daß die Dokumentation zu Prüfungszwecken auch der Aufsichtsbehörde zur Verfügung zu stellen ist.

Im Rahmen der Organisationskontrolle ist auch auf die Dateienübersicht hinzuweisen, die nach § 37 Abs. 2 BDSG das Unternehmen dem betrieblichen Beauftragten für den Datenschutz zur Verfügung zu stellen hat.
Dieses Geräte- und Dateiverzeichnis wird in vielen Unternehmen nicht oder - entgegen der klaren Intention des Gesetzes - wie vor der Novellierung des BDSG durch den Datenschutzbeauftragten selbst geführt.

17. Ordnungswidrigkeitenverfahren

Im Siebenten Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden wurde von einem Adreßverlag berichtet, gegen den die Aufsichtsbehörde im Jahr 1993 drei Verfahren eingeleitet hatte. Das Unternehmen hatte einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 BDSG zuwider gehandelt (Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 7 BDSG), den Zutritt von mit der Überprüfung beauftragten Mitarbeitern der Aufsichtsbehörde zu seinem Grundstück und damit auch zu seinen Geschäftsräumen entgegen § 38 Abs. 4 Satz 4 BDSG nicht geduldet sowie in einem Beschwerdefall Auskünfte entgegen § 38 Abs. 3 Satz 1 BDSG nicht erteilt (Ordnungswidrigkeiten nach § 44 Abs. 1 Nr. 6, 2. bzw. 1. Alternative BDSG). Im Berichtsjahr wurde der Bußgeldbescheid gegen den Adreßverlag erlassen, wobei für die beiden zuerst erwähnten Ordnungswidrigkeiten eine Geldbuße von jeweils 2.000,-- DM festgesetzt wurde, für die Nichterteilung der Auskünfte wurden 500,-- DM festgesetzt. Da der Adreßhändler gegen den Bußgeldbescheid Einspruch eingelegt hat, hat dieser noch keine Rechtskraft erlangt.

Im Berichtsjahr 1994 wurden von der Aufsichtsbehörde sechs Ordnungswidrigkeitenverfahren nach dem BDSG eingeleitet. Diese Verfahren richteten sich gegen vier Unternehmen, wobei zwei dieser Unternehmen jeweils mit zwei Verfahren betroffen waren.

So hat die Aufsichtsbehörde in drei Fällen Ordnungswidrigkeitenverfahren wegen der entgegen § 36 Abs. 1 BDSG seit Aufnahme der Geschäftstätigkeit - die in beiden Fällen bereits einige Jahre zurücklag - nicht erfolgten Bestellung eines betrieblichen Datenschutzbeauftragten eingeleitet (Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 5 BDSG). Bei zwei dieser Unternehmen hat die Aufsichtsbehörde außerdem wegen der verspäteten Abgabe der nach § 32 Abs. 1 BDSG erforderlichen Mitteilung über die Aufnahme einer meldepflichtigen geschäftsmäßigen Datenverarbeitungstätigkeit ein Ordnungswidrigkeitenverfahren eingeleitet (Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 2 BDSG). Das Unternehmen hatte - ohne seiner Meldepflicht nachgekommen zu sein - bereits sechs Jahre lang personenbezogene Daten geschäftsmäßig zum Zwecke der anonymisierten Übermittlung im Bereich der Markt- und Meinungsforschung gespeichert und außerdem zwei Jahre vor der Einleitung des Verfahrens - ebenfalls ohne die Abgabe der erforderlichen Meldung bei der Behörde - die Geschäftstätigkeit um die Verarbeitung

personenbezogener Daten im Auftrag als Dienstleistungsunternehmen erweitert.

Bei dem zweiten Unternehmen, gegen das ein Ordnungswidrigkeitenverfahren wegen der nicht erfolgten Bestellung eines betrieblichen Datenschutzbeauftragten eingeleitet wurde, handelte es sich um eine Vermögensberatungsgesellschaft, die nicht der Meldepflicht gemäß. § 32 BDSG unterliegt.

Hier war der Aufsichtsbehörde die nicht erfolgte Bestellung des betrieblichen Datenschutzbeauftragten anläßlich einer Anlaßüberprüfung in den Geschäftsräumen der Gesellschaft bekannt geworden. Die Überprüfung, die aufgrund der Beschwerde einer Betroffenen gegen die Verarbeitung ihrer personenbezogener Daten durch die Gesellschaft eingeleitet wurde, führte auch zu der Feststellung, daß das Unternehmen die mit der Datenverarbeitung beschäftigten Mitarbeiter entgegen § 5 BDSG nicht auf das Datengeheimnis verpflichtet hatte. Da die Vermögensberatungsgesellschaft auf die mehrmalige Nachfrage der Aufsichtsbehörde, ob die Mitarbeiter inzwischen auf das Datengeheimnis verpflichtet wurden, keine Auskunft erteilte, wurde gegen das Unternehmen auch ein Ordnungswidrigkeitenverfahren wegen der nicht erfolgten Erteilung dieser Auskunft entgegen § 38 Abs. 3 Satz 1 BDSG eingeleitet (Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 6, 1. Alternative BDSG).
Die Ordnungswidrigkeitenverfahren gegen die Vermögensberatungsgesellschaft sind inzwischen durch Bußgeldbescheid rechtskräftig abgeschlossen.

Wegen einer Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 6, 1. Alternative BDSG wurde auch gegen ein weiteres Unternehmen ein Ordnungswidrigkeitenverfahren eingeleitet. Dieses Unternehmen hatte der Aufsichtsbehörde entgegen § 38 Abs. 3 Satz 1 BDSG Auskünfte zu einem Beschwerdefall nicht erteilt.

In den neu eingeleiteten Verfahren hat die Aufsichtsbehörde im Berichtsjahr drei Bußgeldbescheide erlassen, wobei mit zwei dieser Bußgeldbescheide Geldbußen für mehrere Verstöße festgesetzt wurden. Zwei dieser Bußgeldbescheide haben im Berichtsjahr Rechtskraft erlangt.

Wiesbaden, den 3. Juli 1995

Der Hessische Ministerpräsident
Eichel

Der Hessische Minister
des Innern und für
Landwirtschaft, Forsten und Naturschutz
Bökel