13. Wahlperiode

HESSISCHER LANDTAG

Drucksache **13/4809**

13 Seiten

13. 09. 1993

Vorlage der Landesregierung

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

Vorgelegt mit der Stellungnahme zum Einundzwanzigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten - Drucks. 13/3887 - nach § 30 Abs. 2 des Hessischen Datenschutzgesetzes vom 11. November 1986

Eingegangen am 13. September 1993 · Ausgegeben am 21. September 1993

Herstellung: Wiesbadener Graphische Betriebe GmbH, 65199 Wiesbaden · Auslieferung: Kanzlei des Hessischen Landtags Postf. 3240 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

Die Anzahl von Beschwerden gegen Stellen, die Datenverarbeitung für die Erfüllung eigener Geschäftszwecke betreiben, ist im Berichtsjahr erneut gegenüber den Vorjahren angestiegen. Dies ist unter anderem darauf zurückzuführen, daß die Aufsichtsbehörde seit der Novellierung des BDSG auch Beschwerden nicht direkt Betroffener nachzugehen hat, wenn ihr ausreichende Anhaltspunkte dafür vorliegen, daß Datenschutzbestimmungen durch nicht-öffentliche Stellen verletzt sind.

Im Jahr 1992 gingen bei den drei hessischen Aufsichtsbehörde 136 Beschwerden ein. Alle Beschwerden führten zu einer Überprüfung durch die Aufsichtsbehörden.

Die Beschwerden betrafen:

- Kreditkartenunternehmen in 30 Fällen,
- Versicherungen in 15 Fällen,
- Kreditinstitute in 13 Fällen,
- den Versandhandel in 10 Fällen,
- den Einzelhandel in 6 Fällen,
- Vereine in 9 Fällen,
- Anbieter von Fort- und Weiterbildung in 5 Fällen,
- das Gesundheitswesen (Ärzte, Krankenhäuser) in 4 Fällen,
- Verlage in 4 Fällen,
- EDV-Service-Betriebe in 4 Fällen,
- Fluglinien in 2 Fällen,
- Hotels in 2 Fällen,
- sonstige Unternehmen in 32 Fällen.

In 29 Fällen waren die Beschwerden begründet, davon in drei Fällen gegen Kreditkartenunternehmen, in vier Fällen gegen Versicherungen, in je zwei Fällen gegen Kreditinstitute, den Versandhandel, Anbieter von Fort- und Weiterbildung, EDV-Service-Betriebe und Fluglinien, in je einem Fall gegen den Einzelhandel, einen Verein, einen Verlag und ein Hotel sowie in acht Fällen gegen sonstige Unternehmen.

Bei vier Beschwerden konnte nicht abschließend festgestellt werden, ob die Datenverarbeitung in zulässiger oder in unzulässiger Weise erfolgt ist.

In 29 Fällen sind die Ermittlungen der Aufsichtsbehörde noch nicht abgeschlossen.

Im Berichtsjahr wurden 16 noch aus den Vorjahren übernommene Beschwerdefälle abgeschlossen. Davon war eine Beschwerde gegen ein Krankenhaus begründet, in einem weiteren dieser Fälle konnte nicht mehr abschließend festgestellt werden, ob die Datenverarbeitung in zulässiger oder in unzulässiger Art und Weise erfolgt ist.

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

Im Berichtsjahr gingen 43 Beschwerden gegen Stellen, die personenbezogene Daten geschäftsmäßig verarbeiten, ein. Im Vergleich zu den Vorjahren richteten sich diese Beschwerden nicht mehr fast ausschließlich gegen Kreditinformationsdienste und Adresshändler, sondern betrafen auch den Bereich der Unternehmen, die personenbezogene Daten im Auftrag als Dienstleistung verarbeiten oder nutzen. Alle Beschwerden führten zu einer Überprüfung durch die Aufsichtsbehörde.

Die Beschwerden betrafen:

- Kreditinformationsdienste (Wirtschaftsauskunfteien und SCHUFA) in 29 Fällen,
- Dienstleistungsdatenverarbeiter in 10 Fällen,

- Adresshändler in 2 Fällen,
- Markt- und Meinungsforschungsunternehmen in 2 Fällen.

In 16 Fällen waren die Beschwerden begründet, davon in 13 Fällen gegen Kreditinformationsdienste, in zwei Fällen gegen Dienstleistungsdatenverarbeiter und in einem Fall gegen einen Adresshändler. Bei drei Beschwerden konnte nicht mehr abschließend festgestellt werden, ob die Datenverarbeitung in zulässiger oder unzulässiger Weise erfolgt ist. In vier Beschwerdefällen gegen Kreditinformationsdienste sind die Ermittlungen der Aufsichtsbehörde noch nicht abgeschlossen. Bei weiteren fünf noch aus dem Vorjahr übernommenen Beschwerdefällen stellten sich drei Beschwerden - zwei gegen Kreditinformationsdienste sowie gegen einen Adressverlag - als begründet heraus.

3. Bearbeitung von Anfragen zu Problemen des Datenschutzes

Im Berichtsjahr wurden an die Aufsichtsbehörden wiederum in erheblichem Umfang schriftliche und mündliche Anfragen gerichtet.

So baten Bürger um Auskunft über die Zulässigkeit bestimmter Datenverarbeitungen, ohne daß damit stets die Behauptung der Beeinträchtigung datenschutzrechtlicher Belange verbunden wurde. Unternehmen und Datenschutzbeauftragte, aber auch Angehörige beratender Berufe wie Rechtsanwälte und Unternehmensberater wandten sich häufig an die Aufsichtsbehörden mit der Bitte um Informationen zur Praxis der Aufsichtsbehörde bzw. um Vorabprüfung von geplanten Verarbeitungen, Nutzungen oder Verfahren. Inhaltlich richteten sich die Anfragen auf die verschiedensten Bereiche.

Erwähnenswert ist, daß häufig von Vereinen und Verbänden Informationen über die Zulässigkeit der Verarbeitung von Mitgliederdaten angefordert wurden. Auch die Problematik der Datenübermittlung ins Ausland wurde in wachsendem Maße zum Thema von Anfragen gemacht (hierzu unten 12.).

Mit einer neuen Thematik mußten sich die Aufsichtsbehörden im nicht-öffentlichen Bereich aufgrund der Einführung von Telekommunikationsdienstleistungen durch private Unternehmen (D1-Netz) befassen. Zwar befindet sich das bisher einzige Unternehmen neben der Telekom, das eine Fernmeldeanlage betreibt und damit Telekommunikationsdienstleistungen anbietet, die Mannesmann AG, nicht im Zuständigkeitsbreich der hessischen Aufsichtsbehörden, wohl aber Dienstanbieter und mit Abrechnung und internationalem Clearing beauftragte Unternehmen. Da die Datenschutzkontrollbehörden nach § 6 Abs. 8 der Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (Teledienstunternehmen-Datenschutzverordnung-UDSV) vom 18. Dezember 1991 (BGBl. I, S. 2337), über Abrechnungsverfahren zu unterrichten sind, wurden seitens des beteiligten Unternehmens Kontakte aufgenommen. Ins Bewußtsein breiterer Schichten der Bevölkerung ist dagegen die datenschutzrechtliche Relevanz des stark wachsenden Telekommunikationsbereichs noch nicht gedrungen. Dies mag nicht zuletzt auf die sehr dürftige Informationspolitik durch Verordnungsgeber und Telekommunikationsunternehmen zurückzuführen sein.

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

4.1. Register

Die Aufsichtsbehörde führt nach § 38 Abs. 2 BDSG ein Register der Stellen, die personenbezogene Daten geschäftsmäßig zum Zweck der personenbezogenen oder der anonymisierten Übermittlung speichern oder im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen und damit nach § 32 BDSG der Meldepflicht unterliegen. Zur Zeit sind zu diesem Register 587 Unternehmen gemeldet.

4.2. Meldepflicht nach § 32 BDSG

Nicht immer läßt sich zweifelsfrei beurteilen, ob ein Unternehmen eine meldepflichtige Tätigkeit betreibt oder nicht. Im südhessischen Bereich findet sich ein Schwerpunkt von Verlagen, die zum Großteil seit Jahrzehnten in schriftlicher Form Informationen über Wirtschaftsunternehmen aber zum Beispiel auch über Führungskräfte in der Wirtschaft herausgeben und zu diesem Zweck in erheblichem Umfang personenbezogene Daten erheben und verarbeiten. Die gleichen Informationen werden seit einiger Zeit jedoch auch als Datenbanken über Fachinformationszentren und auf CD-ROM angeboten. Insbesondere hinsichtlich der Angebote über Datenbanken und CD-ROM war fraglich, ob die betroffenen Unternehmen das Medienprivileg in Anspruch nehmen konnten, also von den Bestimmungen des Bundesdatenschutzgesetzes nur die §§ 5 und 9 zu beachten hatten. Erst durch die Novelle des BDSG sind diese Unternehmen besonders erwähnt worden. Das Medienprivileg gilt danach nur, soweit Verlage personenbezogene Daten zur Herausgabe von Adressen-, Telefon-, Branchen- oder vergleichbaren Verzeichnissen verarbeiten oder nutzen und mit der Herausgabe zugleich eine journalistisch-redaktionelle Tätigkeit verbunden ist (§ 41 Abs.1 Satz 2). Daran, daß die Verlage Daten geschäftsmäßig zum Zweck der Übermittlung speichern, kann es keinen Zweifel geben. Fraglich war allein, ob eine "journalistisch-redaktionelle Tätigkeit" angenommen werden konnte. Nach Auffassung der Aufsichtsbehörden ist damit ein Mindestmaß journalistischer Arbeit angesprochen, die zwar in der Zielrichtgung nicht unbedingt meinungsbildend sein, jedoch über die unbearbeitete Datenwiedergabe hinaus gehen muß. Die Herausgabe von Brancheninformationen und anderen Verzeichnissen dieser Art erfüllt eben noch diese Voraussetzungen. Dies muß auch für die Veröffentlichung über Datenbanken und mittels CD-ROM gelten, da auch sie ohne eine vorangehende journalistische Tätigkeit der Aufbereitung und Würdigung nicht denkbar ist. Es kann also nicht alleine darauf ankommen, ob - wie es in den schriftlichen Verzeichnissen üblich ist - Bilder oder eigenerstellte Textblöcke zwischen die Datengruppen eingefügt werden. Auch die Herausgabe der "reinen" Daten, wie sie in Datenbanken zu finden sind, kann hier das Medienprivileg für sich in Anspruch nehmen mit der Konsequenz, daß die Meldepflicht für diese Verlage entfällt.

Die Frage der Meldepflicht kann sich auch bei Umorganisationen im Unternehmen stellen.

So entsteht eine Meldepflicht oft, wenn die ursprünglich integrierte Datenverarbeitung ausgegliedert und verselbständigt wird.

4.3 Prüfungsübersicht

Im Berichtsjahr 1992 wurden 64 Prüfungen nach § 38 Abs. 2 BDSG durchgeführt. Davon betrafen Datenverarbeiter nach § 32 Abs. 1 Ziff.3 BDSG insgesamt 42, nämlich

- Servicerechenzentren 12
- Konzerndatenverarbeiter 5
- Datenerfasser und Schreibbüros mit Dateienverwaltung 15
- Adreßhändler 2
- Mikroverfilmer 1
- Datenträgervernichter 4
- Telemarketing 3

Des weiteren wurden sieben Kreditinformationsdienste und zwei Brancheninformationsdienste, fünf Unternehmen aus dem Bereich der Markt- und Meinungsforschung und acht sonstige Unternehmen geprüft.

Die Prüfungen brachten folgendes Ergebnis:

- Beanstandungen 21
- Empfehlungen 32
- ohne wesentliche Beanstandungen 11

Folgende wesentliche Mängel wurden am häufigsten festgestellt:

1. keine bzw. verspätete oder unvollständige Registermeldung nach § 32 BDSG
2. kein Datenschutzbeauftragter oder Mängel in Fachkunde und/oder Aufgabenerfüllung
3. keine oder mangelhafte Zugangskontrolle
4. Mängel in der Datenträgerkontrolle
5. keine oder mangelhafte Zugriffskontrolle
6. keine Maßnahmen zur Eingabekontrolle
7. fehlende Verpflichtung auf das Datengeheimnis (§ 5 BDSG).

Darüber hinaus wurde nach § 38 Abs. 1 BDSG vor Ort wegen acht Beschwerden und fünf mal aus gegebenem Anlaß (Presseveröffentlichungen u.ä.) geprüft.

5. Wirtschaftsauskunfteien

5.1. Fehlende Angabe des berechtigten Interesses

Das BDSG erlaubt Wirtschaftsauskunfteien - auch ohne die Kenntnis und ohne die Einwilligung des Betroffenen -, personenbezogene Daten zu speichern und an Dritte zu übermitteln, wenn diese ein berechtigtes Interesse an der Kenntnis dieser Daten glaubhaft dargelegt haben. Als berechtigtes Interesse sind wirtschaftliche Interessen anerkannt. So fällt hierunter die Anbahnung und Erweiterung geschäftlicher Beziehungen wie die Einräumung von Krediten, der Abschluß von Raten- und Leasingverträgen, der Kauf oder die Bestellung auf Rechnung und anderes.

Wirtschaftsauskunfteien geben an die bei ihnen anfragenden Unternehmen im Regelfall zur Vereinfachung des Anfrageverfahrens Anfragegutscheine heraus. Auf diesen Gutscheinen hat der Anfrager das berechtigte Interesse anzugeben oder bereits vorgegebene Rubriken dafür anzukreuzen.

Anläßlich der Beschwerde eines Betroffenen stellte sich heraus, daß eine im Aufsichtsbereich tätige Auskunftei Anfragezettel benutzt, auf denen vermerkt ist, daß als berechtigtes Interesse eine Kreditentscheidung angenommen wird, wenn der Anfrager kein berechtigtes Interesse angekreuzt oder angegeben hat.

Diese Verfahrensweise läßt die Möglichkeit des Übersehens bzw. Vergessens der Angabe des berechtigten Interesses unberücksichtigt. Eine Rechtmäßigkeitskontrolle ist in diesen Fällen nicht mehr möglich.

Darüber hinaus wird durch ein solches Verfahren auch das Erschleichen von Auskünften erleichtert, da ein unredlicher Anfrager nicht aktiv eine Falschangabe machen muß, sondern sich durch passives Verhalten einer Verantwortungsübernahme entzieht.

In den Fällen des Nichtangebens eines berechtigten Interesses ist das berechtigte Interesse nicht glaubhaft dargelegt. Damit ist in diesen Fällen das Erteilen einer Auskunft unzulässig.

Auch im Hinblick auf die Strafvorschrift des § 43 Abs. 2 Nr. 1 BDSG ist es erforderlich, daß derartige Anfragegutscheine geändert werden. Nach der Strafvorschrift wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer die Übermittlung von geschützten personenbezogenen Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht.

Es ist ungewiß, ob im Fall des Nichtvorliegens eines berechtigten Interesses ein unredlicher Anfrager, der absichtlich kein berechtigtes Interesse angegeben hat, wegen des Erschleichens personenbezogener Daten durch unrichtigte Angaben bestraft werden kann.

Die Aufsichtsbehörde hat deshalb die Änderung der Anfragegutscheine dahingehend gefordert, daß jeder Anfrager bei der Angabe des berechtigten Interesses aktiv tätig werden muß.

5.2. Zusammenarbeit mit Inkasso-Unternehmen

Anläßlich der Beschwerde einer Betroffenen über ein Inkasso-Unternehmen stellte sich heraus, daß dieses Unternehmen Daten, die eine - strittige - Inkasso-Angelegenheit der Beschwerdeführerin betrafen, unaufgefordert an eine Auskunftei übermittelt hatte.

Wie die Ermittlungen der Aufsichtsbehörde ergaben, handelte es sich dabei um keinen Einzelfall. Vielmehr übermittelt das betroffene Inkasso-Unternehmen, wenn es von Dritten mit der Einziehung fälliger Forderungen beauftragt wird, regelmäßig Daten zu den jeweiligen Inkasso-Angelegenheiten Betroffener an Wirtschaftsauskunfteien, ohne daß von diesen Auskunfteien Anfragen zur Person der Betroffenen vorgelegen haben. Bei den empfangenden Auskunfteien werden diese Daten dann sozusagen "auf Vorrat" gespeichert.

Eine solche Vorgehensweise ist unzulässig, da der Empfänger der übermittelten Daten an deren Kenntnis kein berechtigtes Interesse hat. Außerdem ist davon auszugehen, daß das Inkasso-Büro - wie im Beschwerdefall - nicht vor der Datenübermittlung prüft, ob die Betroffenen ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung haben, z.B. weil die Forderung strittig ist. Im Beschwerdefall war aus diesen Gründen sowohl die Übermittlung der Daten zur Inkasso-Angelegenheit der Betroffenen an die Auskunftei als auch die dortige Speicherung unzulässig.

6. SCHUFA

Die Datenspeicherung durch die SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung) ist für jeden Bürger spätestens dann von Bedeutung, wenn er sich um einen Bank- oder Warenkredit bemüht. Die Vertragspartner der SCHUFA gewähren einen Kredit grundsätzlich nur, wenn der Betroffene aufgrund der Mitteilung seiner bei der SCHUFA gespeicherten Daten als kreditwürdig angesehen wird.

Es ist deshalb äußerst wichtig, daß nur solche Daten gespeichert und übermittelt werden, bei denen die Identität der betroffenen Person unzweifelhaft feststeht. Darauf sind die jeweiligen SCHUFA-Geschäftsstellen wiederholt hingewiesen worden. Im Berichtszeitraum ist es gleichwohl wiederum vorgekommen, daß Angaben zu einem Betroffenen gespeichert und übermittelt wurden, die in Wahrheit nicht ihn, sondern eine andere namensgleiche Person betrafen.

So wollte ein Betroffener einen Pkw leasen. Die Leasing-Bank lehnte den Vertrag unter Hinweis auf die SCHUFA-Auskunft ab, die für den Betroffenen unter anderem die Angabe enthielt: "Ohne Geburtsdatum sind uns folgende Informationen bekanntgeworden: Aus öffentlichem Verzeichnis: Eidesstattliche Versicherung". Die Nachprüfung der Angelegenheit ergab, daß ein Verwandter des Betroffenen mit weitgehend gleichem Namen die eidesstattliche Versicherung abgegeben hatte, die im Schuldnerverzeichnis des Amtsgerichts eingetragen war. Die SCHUFA hatte das Merkmal von dort übernommen und aufgrund der weitgehenden Identität der Namen dem Betroffenen zugeordnet. Da das Schuldnerverzeichnis die Geburtsdaten nicht speichert, kommt es hier immer wieder zu Verwechslungen. Die negativen Auswirkungen für den Betroffenen sind auch nicht stets dadurch zu vermeiden, daß die SCHUFA zur eigenen Entlastung bereits auf das nicht überprüfte Geburtsdatum hinweist.

Auf Betreiben der Aufsichtsbehörde wurde das Merkmal bei der SCHUFA gelöscht und die SCHUFA nochmals darauf hingewiesen, daß nicht eindeutig zuzuordnende Daten im Zweifel nicht verwendet werden dürfen.

7. Kreditkartenunternehmen

Kreditkartenunternehmen bieten, aufgrund der großen Menge personenbezogener Daten, die sie verarbeiten, immer wieder Anlaß für Anfragen und Beschwerden Betroffener bei den Aufsichtsbehörden. Im Berichtszeitraum führte ein Unternehmen eine sogenannte Haushaltsbefragung durch, die eine größere Anzahl von Anfragen und Beschwerden nach sich

zog. Das Kreditkartenunternehmen mietete Adressen bei einem Listbroker (Adressenhändler) an und schickte an jede Anschrift einen Fragebogen. Dieser enthielt Fragen nach dem Besitz von Kapitalanlagen (Sparbuch, Sparvertrag, Wertpapiere, Aktien usw.), Kredit- oder Hypothekenarten (Ratenkredit, Hypothekenkredit), Eurocheque, Warenhauskarten oder Kreditkarten. Auf der zweiten, "Statistik" überschriebenen Seite, wurde unter anderem nach Geschlecht, Familienstand, Kinderzahl, Schulbildung, Einkommenshöhe, Wohnverhältnissen, Reisezielen, Anzahl wöchentlicher Restaurantbesuche sowie kontoführenden Banken gefragt. Schließlich sollte der Befragte sein Einverständnis damit erklären, daß die erfragten Angaben zum Zweck der "Auswertung und dem Angebot von Finanzdienstleistungen" gespeichert werden. Dem beigefügten Schreiben konnten die Betroffenen entnehmen, daß sie im Rahmen einer jährlich durchgeführten repräsentativen Haushaltsbefragung angeschrieben wurden, um die "Wünsche und Gepflogenheiten im Bereich der privaten finanziellen Angelegenheiten festzustellen". Unter allen Einsendern sollte ein Wochenendaufenthalt in einem Hotel verlost werden.

Viele Bürger wollten wissen, ob eine solche Datenerhebung überhaupt erlaubt sei und ob die erfragten Daten nicht zu anderweitigen Zwecken Verwendung finden würden.

Die Erhebung von Daten wird durch das Bundesdatenschutzgesetz nur insoweit geregelt, als sie nicht gegen Treu und Glauben oder unter Täuschung des Betroffenen erfolgen darf. Danach war die Datenerhebung hier noch zulässig. Ein Verstoß hätte allerdings festgestellt werden müssen, wenn die Angaben über den Zweck der Erhebung und die Verwendung der Daten zwar nicht falsch, aber so allgemein gewesen wären, daß sie bei den Betroffenen leicht eine falsche Vorstellung hätten erzeugen können. Zu berücksichtigen war auch, daß die Teilnahme an der Befragung deutlich freigestellt war und auch nicht durch die Auslobung eines höherwertigen Gewinns ein faktischer Zwang zur Teilnahme bestand. Dennoch zeigte die doch breite negative Reaktion von Betroffenen, daß nicht ausreichend über Sinn und Zweck der Erhebung informiert worden war.

Ein Kreditkartenunternehmen fragte bei der Aufsichtsbehörde an, ob es zulässig sei, Kreditkarten aufgrund einer telefonischen Bestellung auszugeben. Der Antrag sollte wie üblich bearbeitet werden, d.h. im Rahmen der Bonitätsprüfung sollte eine SCHUFA-Anfrage erfolgen. Noch während die Anfrage von der Aufsichtsbehörde geprüft wurde, warb ein anderes Kreditkartenunternehmen in der Presse damit, daß aus Anlaß des die Post betreffenden Streiks im öffentlichen Dienst Kreditkarten auch per Telefon beantragt werden könnten. Die Aufsichtsbehörde bezog das zweite Unternehmen in die datenschutzrechtliche Prüfung ein und stellt dabei fest, daß die Möglichkeit der telefonischen Kartenbestellung durchaus über die Dauer des Streiks hinaus angeboten werden sollte. Es war daran gedacht, bei der telefonischen Bestellung gleichzeitig die Einwilligung des Betroffenen zur SCHUFA-Anfrage einzuholen. Mit der Kreditkarte wollte das Unternehmen die üblichen Antragsunterlagen mit der Bitte um Unterzeichnung - darunter auch die SCHUFA-Klausel - und Rückgabe versenden.

Die Aufsichtsbehörde konnte hierin keine wirksame Einwilligung des Betroffenen zur Einholung der SCHUFA-Auskunft, also zur Übermittlung des Merkmals "Kreditkarte angefragt" an die SCHUFA und die Übermittlung der gesamten Betroffenendaten von der SCHUFA an das Kreditkartenunternehmen, erkennen. Aufgrund des Bundesdatenschutzgesetzes muß für solche Übermittlungen ausdrücklich eine schriftliche, vorherige Einwilligung des Betroffenen vorliegen, auf die nur verzichtet werden kann, wenn "wegen besonderer Umstände eine andere Form angemessen ist". Das Kreditkartenunternehmen sah diesen Ausnahmetatbestand aufgrund der telefonischen Bestellung und der geringen Anzahl solcher Bestellungen als gegeben an. Die Aufsichtsbehörde hat demgegenüber darauf hingewiesen, daß allein die Tatsache der telefonischen Bestellung noch keinen besonderen Umstand im Sinne der gesetzlichen Regelung darstellt. Der Ausweitung schneller Kommunikationswege und fernmündlicher Kontakte ist ja gerade im Sinne des Betroffenenschutzes das grundsätzliche Schriftformerfordernis entgegengestellt worden. Der Verzicht auf die Schriftform ist hier auch nicht angemessen. Der Umfang

des Datenaustausches mit der SCHUFA erfordert eine eingehende Information des Betroffenen über das Verfahren. Diese ist nur bei Unterzeichnung der ausführlichen SCHUFA-Klausel gewährleistet, die zugleich eine Einwilligung zur Datenverarbeitung beinhaltet.

Nicht zuletzt deshalb wurden von der SCHUFA in Abstimmung mit den Aufsichtsbehörden für den Datenschutz detaillierte Einwilligungsklauseln für das SCHUFA-Verfahren entwickelt, die die Vertragspartner der SCHUFA - wie Kreditkartenunternehmen - vor einer Anfrage unterzeichnen lassen müssen.

Selbstverständlich steht es jedoch den Kreditkartenunternehmen im Sinne eines schnellen Services für zukünftige Kunden frei, telefonisch bestellte Kreditkarten ohne Bonitätsprüfung durch die SCHUFA auszugeben.

8. Versicherungen

8.1. Datenerhebung

Aufgrund der Eingabe einer Betroffenen bestand der Verdacht, daß ein Versicherungsunternehmen Daten von Wöchnerinnen noch auf der Entbindungsstation des Krankenhauses in einer Art und Weise erhebt, die gegen Treu und Glauben verstößt. So sollten Mitglieder des Pflegepersonals im Auftrag der Versicherung Wöchnerinnen zur Abgabe personenbezogener Daten mit dem Ziel eines Versicherungsabschlusses gedrängt haben.

Inwieweit in Einzelfällen bzw. in bestimmten Krankenhäusern regelmäßig in dieser Art und Weise vorgegangen wurde, ließ sich letztlich nicht klären. Das Versicherungsunternehmen versicherte, daß alle Mitarbeiter im Rahmen von Schulungen darauf hingewiesen werden, daß eine Aufnahme von Daten im Krankenhaus, insbesondere am Krankenbett, unzulässig ist. Schließlich wurde eine Einigung dahin erzielt, daß Rückantwortkarten im Krankenhaus ausgelegt werden, die von den Müttern, falls gewünscht, ausgefüllt werden können. Die jungen Mütter können so selbst entscheiden, ob und gegebenenfalls wann sie - in der Regel zu Hause - Besuch von einem Versicherungsvertreter bekommen möchten.

8.2. Schweigepflichtentbindungsklauseln

Immer wieder erreichen die Aufsichtsbehörde Beschwerden von Bürgern, aber auch Eingaben von Ärzten, die gegen von Versicherern verwendete Schweigepflichtentbindungsklauseln Bedenken geltend machen. In den letzten Jahren wurden zwischen den Verbänden der Versicherungswirtschaft, dem Bundesaufsichtsamt für das Versicherungswesen und den Datenschutzaufsichtsbehörden Musterformulierungen für Schweigepflichtentbindungserklärungen entworfen, die für die verschiedenen Sparten der Versicherungen zu unterschiedlichen Zeitpunkten Geltung erlangten. Trotz dieser in wesentlichen Punkten hinsichtlich Bestimmtheit und Geltungsdauer datenschutzrechtlich aktualisierten Muster werden jedoch immer wieder bei der Geltendmachung von Leistungsansprüchen den Versicherten Erklärungen zur Unterschrift vorgelegt, die über den im Einzelfall erforderlichen Rahmen weit hinausgehen.

Die betroffenen Versicherer entschuldigten dies mit der versehentlichen Verwendung von noch vorrätigen Formularen bzw. Textbausteinen in der Textverarbeitung. Allerdings ist hier auch ein gestiegenes Datenschutzbewußtsein insofern festzustellen, als Beschwerden gegen Versicherungen sich selbst dann gegen Schweigepflichtentbindungsklauseln richteten, wenn bereits die neuen Mustertexte verwendet wurden. Die Bedenken richteten sich gegen die Erweiterung der Einwilligung um anderweitig beantragte (Versicherungs-)Verträge und um künftige Anträge auf Abschluß einer Versicherung, sowie gegen die Geltung der Einwilligung unabhängig vom Zustandekommen des Versicherungsvertrags. Diese Bedenken sind nicht gänzlich von der Hand zu weisen, da es dem Betroffenen hier kaum noch möglich ist, den Umfang seiner Einwilligungserklärung zu überblicken.

Leider ist jedoch nicht zu erwarten, daß nach den langwierigen Verhandlungen, die zu den jetzt geltenden Texten geführt haben, kurzfristig erneut Änderungen erfolgen.

8.3. Unzulässige Übermittlung durch private Krankenkassen

Angaben über gesundheitliche Verhältnisse sind immer besonders schutzwürdig. Dies beachtete eine private Krankenversicherung nicht, die die Begleichung der Rechnung eines Sanitätshauses diesem gegenüber mit der Begründung "Vorsatz oder Sucht" ablehnte. Die Betroffene fühlte sich dadurch bei dem Sanitätshaus in ein falsches Licht gesetzt. Tatsächlich war die Mitteilung des Ablehnungsgrundes gegenüber dem Sanitätshaus weder zur Erfüllung des Versicherungsvertrages mit der Betroffenen noch zur Wahrung berechtigter Interessen der Kasse erforderlich und damit datenschutzrechtlich unzulässig. Es wäre völlig ausreichend gewesen, wenn die Versicherung eine Begründung der Ablehnung nur gegenüber der Versicherten abgegeben hätte.

9. Datenverarbeitung im medizinischen Bereich

9.1. Übermittlung von medizinischen Daten Verstorbener

Im Berichtszeitraum wurde der zuständigen Aufsichtsbehörde durch eine Pressemeldung bekannt, daß der Chemiekonzern Hoechst medizinische Daten verstorbener ehemaliger Mitarbeiter des Unternehmens sammelt und hinsichtlich der Todesursache und eventuellen Zusammenhängen mit früheren Kontakten des Beschäftigten mit chemischen Stoffen im Unternehmen auswertet. Dabei tauchte der Verdacht auf, daß die Daten unter Verstoß gegen die ärztliche Schweigepflicht und eventuell datenschutzrechtliche Gebote in das Unternehmen gelangt waren. Da von dem Verdacht der rechtswidrigen Übermittlung von Gesundheitsdaten auch öffentliche Stellen des Landes bzw. von Kommunen betroffen waren, war auch der Hessische Datenschutzbeauftragte an der Überprüfung beteiligt. Die Datenverarbeitung des Werksärztlichen Dienstes der Hoechst AG wurde daraufhin im einzelnen überprüft. Es konnte jedoch nicht festgestellt werden, daß gegen Datenschutznormen verstoßen worden war. Soweit im Rahmen des Werksärztlichen Dienstes Daten von noch Beschäftigten des Unternehmens verarbeitet wurden, geschah dies auf der Grundlage des Arbeitsverhältnisses und der Vorschriften des Arbeitssicherheitsgesetzes. Im Rahmen der Vorsorgepflicht dürfen solche Daten auch für die epidemiologische Forschung verwendet werden. Hinsichtlich der Daten verstorbener ehemaliger Mitarbeiter des Unternehmens konnten keine konkreten Einzelfälle unzulässiger Übermittlung durch Ärzte oder öffentliche Stellen an das Unternehmen festgestellt werden. Ohne das Einverständnis der hinterbliebenen nächsten Angehörigen wäre darin jedenfalls ein Verstoß gegen die ärztliche Schweigepflicht zu sehen gewesen. Ein Verstoß gegen den Datenschutz wäre jedoch in einem solchen Fall nicht festzustellen, weil die Daten Verstorbener jedenfalls datenschutzrechtlich grundsätzlich nicht mehr geschützt sind. Schutzgegenstand des Datenschutzes ist nämlich das allgemeine Persönlichkeitsrecht in seiner vom Bundesverfassungsgericht anerkannten speziellen Ausprägung als informationelles Selbstbestimmungsrecht, das nur einer noch lebenden Person zugeordnet werden kann (BVefGE 30, 173, 194).

9.2. Besondere Probleme bei Wartung und Reparatur von Arztcomputern

Eine Ärztin besaß einen PC mit einer 40 MB-Festplatte, die sehr schnell mit Programmen und Daten gefüllt war. Sie bat ihren Lieferanten, die Festplatte auszubauen, den Daten-Inhalt auf eine neue größere Festplatte zu überspielen und ihr aus Sicherheitsgründen die alte 40 MB-Festplatte zusätzlich wieder auszuhändigen.

Die Betroffene glaubte, damit sämtliche Datenschutzrisiken ausgeschaltet zu haben.

Für den Kopiervorgang von der kleinen alten Festplatte auf die neue größere Festplatte mußte jedoch ein Zwischenspeicher benutzt werden. Hierfür verwendete das Serviceunternehmen einen Notebook- PC. Dieser Notebook-PC wurde später an einen anderen Kunden ausgehändigt, der dringend ein Leihgerät benötigte, welches sofort funktionsfähig sein sollte. Dieser Kunde stellte die in dem Gerät gespeicherten Arztdaten fest. Die

von ihm angesprochene Aufsichtsbehörde überprüfte daraufhin das Serviceunternehmen und forderte eine andere Arbeitsweise bei der Reparatur und dem Austausch von Festplatten. Das Serviceunternehmen sicherte zu, daß es zukünftig Zwischenspeicherungen in einer einzigen Kopierroutine umgehend physisch löschen wird. Trotzdem sollte dafür Sorge getragen werden, daß ein PC für eigene Werkstattarbeiten - hier für Zwischenspeicherungen - auch tatsächlich immer in der Werkstatt verbleibt und nicht an Kunden ausgehändigt wird.

10. Arbeitnehmerdatenschutz

10.1. Spesenabrechnungen

An die Aufsichtsbehörde wurde in einigen Fällen unter anderem auch fernmündlich die Frage herangetragen, inwieweit ein Arbeitgeber auf Dienstreisen entstandene personenbezogene Daten von Arbeitnehmern bei diesem selbst oder bei anderen Stellen erfragen und speichern darf.

Einem Beschwerdefall lag zugrunde, daß der Arbeitgeber des Betroffenen zur Kontrolle, ob der Betroffene tatsächlich das im Rahmen der Reisespesen abgerechnete Ticket benutzt hatte, sämtliche Flugdaten sowohl des Betroffenen als auch seiner Begleiterin von der in Anspruch genommenen Fluggesellschaft anforderte und sie auch bekam.

Für die in der Anfrage liegende Datenerhebung gilt als Zulässigkeitsvoraussetzung lediglich, daß die Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben werden müssen. Daten, die beispielsweise durch heimliche Beobachtung gewonnen wurden, wären danach unter Umständen nicht rechtmäßig erhoben mit der Folge, daß die Speicherung und weitere Verarbeitung dieser Daten rechtswidrig wäre. Grundsätzlich darf der Arbeitgeber jedoch auch durch Nachfrage bei Dritten prüfen, ob Spesenabrechnungen korrekt aufgestellt worden sind. Er wird dies allerdings nur dann tun, wenn er konkreten Anlaß zu Zweifeln daran hat. Eine regelmäßige Rückfrage wäre nicht nur ein unwirtschaftlicher Aufwand, sondern könnte unter Umständen auch zu einer unzulässigen Datenübermittlung des Arbeitgebers an die angefragten Unternehmen führen, da mit einer solchen Rückfrage stets auch die Information verbunden ist, daß der betroffene Arbeitnehmer zumindest im Verdacht der Unregelmäßigkeiten steht.

Im konkreten Beschwerdefall war jedoch die Übermittlung von der Fluggesellschaft an den Arbeitgeber, soweit der Beschwerdeführer selbst betroffen war, hinsichtlich des Umfangs zu bemängeln, da erheblich mehr Daten als zur Überprüfung der Spesenabrechnung erforderlich übermittelt worden waren. In den übersandten Kopien der "passenger name records" der Fluggesellschaft fanden sich nämlich neben den Buchungsdaten auch noch Angaben über Paßnummer und -gültigkeit, bevorzugte Mietwagenfirma und Autotypen, Kreditkartennummer und -gültigkeit, bevorzugte Hotels und Anzahl der Gepäckstücke. Soweit Daten der Begleiterin des Betroffenen übermittelt worden waren, war die Übermittlung in vollem Umfang rechtswidrig, da ein berechtigtes Interesse des Arbeitgebers an der Kenntnis dieser Daten auch nicht deswegen zugestanden werden konnte, weil die Begleiterin ebenfalls Arbeitnehmerin in demselben Unternehmen war.

10.2. Übermittlung zu Werbezwecken

Gelegentlich wird der Aufsichtsbehörde bekannt, daß Arbeitgeber Daten ihrer Arbeitnehmer zu Werbezwecken an Dritte - z.B. Versicherungsgesellschaften - übermitteln, ohne dabei Datenschutzbestimmungen zu beachten. Dies ist häufig dann der Fall, wenn die Möglichkeit zum Abschluß von Gruppen- oder Sammelversicherungsverträgen für die Beschäftigten besteht. So wandte sich ein Arbeitnehmer an die Aufsichtsbehörde, weil er von einer Versicherungsgesellschaft ein Werbeschreiben erhalten hatte, in dem er direkt als Mitarbeiter seines Arbeitgebers angesprochen wurde. Der Betroffene war darüber verärgert, daß seine Anschrift sowie seine Eigenschaft als Arbeitnehmer in einem bestimmten Unternehmen durch den Arbeitgeber zu Werbezwecken an die Versiche-

rung übermittelt worden war. Der Arbeitgeber, der im übrigen die Daten sämtlicher Beschäftigter weitergegeben hatte, war zunächst der Auffassung, diese Übermittlungen seien zulässigerweise erfolgt, da der Betriebsrat in der Angelegenheit vorab informiert worden war und keine Einwendungen erhoben hatte.

Zwar ist die Verarbeitung personenbezogener Daten und deren Nutzung zulässig, wenn der Betroffene eingewilligt hat. Die Einwilligung ist jedoch vom Betroffenen selbst zu erteilen. Sie kann nicht kollektiv durch den Betriebsrat für alle Beschäftigten ausgesprochen werden.

Das novellierte BDSG geht für Daten aus dem Arbeitsverhältnis von einer besonderen Schutzbedürftigkeit aus. So stellt § 28 Abs. 2 Ziff. 1 b BDSG fest, daß Arbeitnehmer in der Regel ein schutzwürdiges Interesse daran haben, daß ihre Daten durch den Arbeitgeber nicht listenmäßig - z.B. für Werbezwecke - an Dritte übermittelt werden. Damit ist es - wie im Beschwerdefall - in aller Regel unzulässig, Daten von Beschäftigten listenmäßig an Versicherungen oder Andere zu Werbezwecken zu übermitteln.

Sofern der Abschluß von Gruppenversicherungen oder Sammelversicherungsverträgen für Beschäftigte eines Unternehmens interessant sein könnte, ist es angebracht, die Beschäftigten durch Aushang oder bei Betriebsversammlungen auf entsprechende Angebote hinzuweisen und durch das Auslegen von Informationsmaterial den Mitarbeitern zu ermöglichen, sich bei Interesse mit den Anbietern selbst in Verbindung zu setzen.

11. Sicherheitsdienste

Aufgrund eines Artikels im Nachrichtenmagazin "Der Spiegel" über den hauseigenen Sicherheitsdienst der Zentrale der Deutschen Bank kam dieser und darüber hinaus generell die Datenverarbeitung von privaten Sicherheitsdiensten in das Blickfeld der Aufsichtsbehörden. Detekteien und private Sicherheitsdienste verarbeiteten bisher nach den Erkenntnissen der Aufsichtsbehörden personenbezogene Daten nahezu ausschließlich nicht in Dateien, sondern in Akten, so daß das Bundesdatenschutzgesetz auf sie nicht anwendbar war. Die Weiterentwicklung der Technik hat auch hier Änderungen mit sich gebracht. Im Falle der Deutschen Bank wurden Video-Aufnahmen auf optischen Speichern, sogenannten Bildplatten gespeichert und waren damit anders als die reine Videoaufnahme nach Bildadressen wieder auffindbar. Auswertbar ist eine solche Sammlung allerdings nur durch Verbindungen zu weiteren automatisiert oder herkömmlich geführten Dateien, die Bildadressen bestimmten personenbezogenen Merkmalen zuordnen. Gegenstand der Überprüfung waren jedoch im wesentlichen herkömmlich geführte und automatisiert auf PC geführte Dateien. Als Ergebnis der Überprüfung mußte festgestellt werden, daß personenbezogene Daten, wozu auch Kfz-Kennzeichen zählen, in aller Regel länger als erforderlich gespeichert wurden. In Gesprächen mit der Deutschen Bank, an denen der Hessische Datenschutzbeauftragte im Rahmen seiner Zuständigkeit für den polizeilichen Bereich zum Teil ebenfalls teilnahm, wurde ein Konzept erarbeitet, das unter Berücksichtigung sowohl der Sicherheitsinteressen des Unternehmens als auch der Persönlichkeitsrechte betroffener Bürger vor allem im Hinblick auf Anlaß und Dauer der Speicherung differenzierte Verfahrensregeln aufstellt. Ein Teil dieses Konzepts besteht darin, daß nach fest definierter Speicherungsdauer die Notwendigkeit der weiteren Speicherung zu überprüfen ist.

12. Auslandsdatenverarbeitung

In mehreren Fällen wurden die Aufsichtsbehörden von Unternehmen bzw. Unternehmensberatungen angesprochen, die um Klärung von Fragen der Verarbeitung von personenbezogenen Daten im Ausland bzw. Übermittlung von Daten ins Ausland baten. So wurde gefragt, ob im Falle einer Online-Verbindung zwischen dem Auftraggeber im Inland und dem ausländischen Rechenzentrum ein Stichprobenverfahren nach § 10 Abs.4 BDSG einzurichten sei. Durch Stichprobenverfahren soll bei automatisierten Abrufverfahren durch die speichernde Stelle die Zulässigkeit

einzelner Übermittlungen überprüft werden können, auch wenn die rechtliche Verantwortung für die Zulässigkeit der Übermittlungen grundsätzlich die abrufende Stelle trägt. Die Frage stellt sich nur, weil es sich rechtlich betrachtet bei jedem Datenaustausch über nationale Grenzen hinweg um eine Übermittlung im Rechtssinne und nicht lediglich um eine Weitergabe an den Auftragnehmer handelt. Ein formelles Stichprobenverfahren, wie es § 10 Abs. 4 BDSG fordert, ist allerdings zur Kontrolle hier nicht erforderlich. Die speichernde Stelle bestimmt als Auftraggeber, welche Daten der Auftragnehmer zu welchem Zeitpunkt erhält und wie er mit ihnen zu verfahren hat. Sie bindet den Auftraggeber durch möglichst genaue Weisungen (§ 11 BDSG) hinsichtlich des Umgangs mit den Daten, schon weil sie gegenüber den Betroffenen und den Behörden für die Einhaltung der Vorschriften des Datenschutzrechts verantwortlich ist. Der Auftragnehmer erhält keine rechtliche Befugnis, selbst über die Datenweitergabe zu entscheiden. Dies entbindet den Auftraggeber jedoch nicht von seiner Pflicht zu überprüfen, ob der Auftragnehmer - im Ausland - die Weisungen auch einhält. In mehreren Fällen ging es um die Zulässigkeit der Übermittlung von Daten aus dem Geltungsbereich des BDSG hinaus.

In der Praxis der Aufsichtsbehörden haben sich folgende Grundsätze entwickelt:

I. Jeder Transfer ins Ausland erfüllt den Tatbestand einer Übermittlung mit der Folge, daß die Übermittlungsgrundsätze des § 28 BDSG anzuwenden sind. Liegt weder eine Einwilligung des Betroffenen noch eine vertragliche Grundlage vor, die die Auslandsberührung voraussetzt bzw. rechtfertigt, so ist die Generalklausel des § 28 Abs. 1 Ziff. 2 BDSG anzuwenden. Je nach Datenschutzstandard des Empfängerlandes besteht jedoch Grund zu der Annahme, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Verarbeitung oder Nutzung überwiegt. Bei der folgenden grundsätzlichen Differenzierung ist jedoch auch die Art bzw. die Schutzbedürftigkeit der zu transferierenden Daten zu berücksichtigen.

II. Datenübermittlungen in ein Land, das weder die Europäische Datenschutzkonvention vom 28. Januar 1981 ratifiziert noch eine eigene Datenschutzgesetzgebung mit dem deutschen Datenschutzrecht vergleichbaren Mindeststandards geschaffen hat, sind äußerst kritisch zu bewerten. Auch die Übermittlung relativ unsensibler Daten ist grundsätzlich nur mit Einwilligung des Betroffenen oder im Rahmen eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses möglich.

III. Datenübermittlungen in ein Land, das die Europäische Datenschutzkonvention ratifiziert, jedoch bisher noch keine eigene Datenschutzgesetzgebung geschaffen hat, die Mindeststandards einhält, sind nach der Art der betroffenen Daten differenziert zu beurteilen. Zwar darf nach Art. 12 Abs. 2 der Konvention allein zum Zweck des Schutzes des Persönlichkeitsrechts kein Vertragsstaat den grenzüberschreitenden Verkehr personenbezogener Daten in das Hoheitsgebiet anderer Vertragsstaaten verbieten oder von einer besonderen Genehmigung abhängig machen. Von der Regelung des Art. 12 Abs. 2 der Konvention kann die Aufsichtsbehörde jedoch abweichen, soweit das innerstaatliche Recht für bestimmte Arten von personenbezogenen Daten/Datensammlungen wegen der Beschaffenheit dieser Datenarten besondere Vorschriften enthält, es sei denn, die Vorschriften des ausländischen Vertragsstaates sehen einen gleichwertigen Schutz vor.

Grundsätzlich kann die Zulässigkeit der Datenübermittlung ins Ausland dadurch erreicht werden, daß durch vertragliche Vereinbarungen zwischen dem deutschen Unternehmen und dem ausländischen Partnerunternehmen angemessene Datenschutzregelungen sichergestellt werden. Die obersten Aufsichtsbehörden für den Datenschutz erarbeiten zur Zeit gemeinsame Anforderungen, die an derartige Verträge zu stellen sind. Sie sollen in einer Art Checkliste zusammengefaßt werden, um eine für den jeweiligen Einzelfall angemessene Beurteilung und Bewertung zu ermöglichen.

13. Datenverarbeitung im Auftrag

13.1. Schriftform des Auftrags

Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Datenverarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind (§ 11 Abs. 2 BDSG).

Wird Datenverarbeitung im Auftrag an ein Dienstleistungsunternehmen vergeben, so wird nach den Erfahrungen der Aufsichtsbehörden das Auftragsverhältnis in nur sehr wenigen Fällen schriftlich festgelegt. Mängel waren hier insbesondere bei Datenerfassungsunternehmen und im Bereich der Datenverarbeitung zu Werbezwecken zu verzeichnen. Die Erteilung eines Auftrags in Schriftform wurde in der Regel versäumt, weil das Auftragsverhältnis bereits seit Jahrzehnten besteht oder weil dem Auftragsverhältnis keine Bedeutung zugemessen wurde.

Immer wieder wurden deshalb sowohl Auftraggeber als auch Auftragnehmer auf das Schriftformerfordernis des Auftrags hingewiesen. Beanstandungen wurden aber auch bei vorliegenden schriftlichen Regelungen öfters ausgesprochen, weil diese über den Hinweis, daß sich der Auftraggeber nach den Bestimmungen des Datenschutzgesetzes zu verhalten habe, nicht hinausgingen.

Als Beispiel ist der Fall eines Versandhandelsunternehmens zu nennen, von dem Antwortkarten der Teilnehmer eines Preisausschreibens und Bestellkarten von Katalogen kartonweise auf der Straße gefunden worden waren. Wie sich feststellen ließ, waren alle Aufträge lediglich mündlich vergeben worden. Weder das Unternehmen, das die Bearbeitung des Preisauschreibens bzw. die Katalogversendung innehatte, noch die Unternehmen, die mit der späteren Vernichtung des Altpapiers beauftragt wurden, hatten konkrete Anweisungen in datenschutzrechtlicher Hinsicht noch einen Überblick über die Ihnen zufallende Verantwortung. Das Versandhandelsunternehmen war von der Unterbeauftragung für die Papierentsorgung nicht informiert worden. Von einer sorgfältigen Auswahl des Auftragnehmers kann in solch einem Fall nicht gesprochen werden.

Seit Bekanntwerden dieses Falles erteilt das Versandhausunternehmen seine Aufträge nun in schriftlicher Form. Der Auftragnehmer seinerseits verpflichtete sich dazu, ohne Einverständnis des Auftraggebers keine Subauftragnehmer zu verpflichten.

An die Aufsichtsbehörden wird hier auch öfter die Frage nach Musterverträgen gerichtet. Die einzelnen Aufsichtsbehörden sind damit allerdings überfordert. Sinnvoller erscheint es, daß die Verbände der betroffenen Branchen Mustertexte und Hinweise entwickeln und die gesetzlichen Erfordernisse bei den angeschlossenen Unternehmen bekannt machen. Unabhängig von branchenspezifischen Besonderheiten sind aber einige wesentliche Punkte zu beachten:

a) Beschreibung des Dienstleisters

Es muß eindeutig festgelegt sein, wer die Dienstleistung tatsächlich erbringt. Die Zulässigkeit der Eingehung von Unterauftragsverhältnissen, die Person und der Verantwortungsbereich des Unterauftragnehmers sowie das Verfahren von eventuellen Wechseln ist festzulegen.

b) Beschreibung der Dienstleistung

Der Umfang der Tätigkeit, vor allem aber die Verantwortungsübergänge zwischen Auftraggeber und Auftragnehmer bzw. ev. Subunternehmen müssen klar definiert sein.

c) Maßnahmen nach der Anlage zu § 9 BDSG

Eine Wiederholung des Normtextes reicht nicht aus. Es sind vielmehr angepaßt an die konkret vorliegenden Umstände die einzelnen Maßnahmen zu beschreiben.

d) Die Datenschutzbeauftragten der beteiligten Unternehmen sollten bei der Abfassung der Weisungen einbezogen und als Ansprechpartner in

eventuellen Konfliktfällen benannt werden. Zu ihren Aufgaben gehört auch die Gewährleistung der Auftragskontrolle nach Ziff. 8 der Anlage zu § 9 BDSG.

13.2. Einzelne Datensicherungsprobleme

Auf der Grundlage der vertraglichen Weisungen muß den Transportwegen und der Übergabe der Daten bzw. Datenträger besondere Aufmerksamkeit gewidmet werden. Es finden sich in der Praxis immer noch Fälle, in denen der Auftraggeber sich die Übernahme von Daten bzw. Datenträgern durch den Auftragnehmer nicht quittieren läßt oder die Erledigung des Auftrages und die damit verbundene Rückgabe der Daten nicht bestätigt wird. Bei Verfahren der Datenfernverarbeitung sind anwählbare Verbindungen für die Verarbeitung sensibler personenbezogener Daten in aller Regel nicht geeignet. Neben der grundsätzlichen Angreifbarkeit von Wählleitungen besteht die Gefahr, daß eine versehentlich falsche Anwahl sofort zu einer unzulässigen Datenübermittlung führt. Es sollte vielmehr eine ausgetestete Übertragungsprozedur bestehen, in der die Anschlußnummer des Empfängers vorgegeben ist. Die Übertragung sollte protokolliert werden.

14. Datensicherung

14.1. Private Personalcomputer am Arbeitsplatz

Für die Anwendung des Bundesdatenschutzgesetzes ist es zunächst nicht relevant, ob die Datenverarbeitungsgeräte im Eigentum des Unternehmens stehen oder ob sie z.B. einem Beschäftigten gehören. Für die Bestimmung der speichernden Stelle und damit der Verantwortlichkeit z.B. der Aufsichtsbehörde gegenüber kommt es allerdings darauf an, in wessen Verfügungsbereich sich die Geräte befinden. Nur wenn ein Unternehmen tatsächlich und rechtlich auf die Geräte einwirken kann, ist es in der Lage, die gesetzlichen Anforderungen technischer und organisatorischer Art zu erfüllen, die insbesondere in § 9 BDSG und der dazu ergangenen Anlage genannt sind. Die grundlegenden Kontrollpflichten, wie Zugangskontrolle, Abgangskontrolle oder Speicherkontrolle sind nur zu gewährleisten, wenn die Datenverarbeitungsgeräte nicht im privaten Haushalt des Arbeitnehmers, sondern in Geschäftsräumen des Unternehmens stehen. Es ist allerdings auch denkbar, daß durch dienstliche Anweisungen und besondere organisatorische Regelungen, z.B. durch Archivierung der Datenträger und Dokumentation ihrer Verwendung, die Bearbeitung von Unternehmensdaten auch auf einem privaten PC in der Wohnung eines Beschäftigten ermöglicht wird. Grundsätzlich sollte dies aber nur gestattet sein bei weniger sensiblen Daten, wozu jedenfalls nicht Personaldaten gehören. Selbstverständlich sollte auch dann ein regelmäßiges back-up sein. In vielen Unternehmen ist die Mitnahme von Datenträgern nach Hause zur Bearbeitung am privaten PC grundsätzlich verboten. Dies hat auch seinen Sinn darin, daß andernfalls die Gefährdung der unternehmenseigenen Daten durch Viren auf dem Fremd-PC oder gar durch die ebenfalls mögliche Einschleppung von Viren von dem privaten PC auf die Datenverarbeitungsgeräte im Unternehmen erheblich ist. Private PC sind in aller Regel nicht nur Arbeitsmittel, sondern werden auch für Spiele etc. verwandt. Gerade bei Spielprogrammen ist es aber bekannt, daß viele dieser oft aus nicht besonders seriösen Quellen stammenden Spielprogramme durch Viren verseucht sind. Aus diesem Grund verbieten die meisten Unternehmen auch den Einsatz fremder ungeprüfter Disketten auf Unternehmens-Personal-computern. Im Falle des Einsatzes eines privaten PCs im Unternehmen muß aus eben diesen Gründen auch gewährleistet sein, daß keine anderen als die vom Unternehmen zur Verfügung gestellten Programme und Disketten verwendet werden. Dies sicherzustellen, ist auch die zugegebenermaßen schwierige Aufgabe des betrieblichen Datenschutzbeauftragten.

14.2. Vernichtung von Datenträgern

Bei der Vernichtung von Datenträgern aus Papier geschieht es öfter, daß ein Unternehmen nur den Transport übernimmt und ein zweites Unter-

nehmen - in der Regel ein Subunternehmen - dann die tatsächliche Datenvernichtungsleistung ausführt.

Derartige Konstellationen sind nicht unproblematisch, weil der Datenvernichter als Fachmann nicht im direkten Kontakt mit dem Kunden steht. Koordinationslücken zwischen Transporteur und Datenvernichter können zusätzliche Probleme schaffen. Vorteilhafter erscheint es deshalb, wenn die gesamte Dienstleistung vom Transport bis zur Vernichtung in einer Hand liegt.

Das Bundesdatenschutzgesetz fordert in Kenntnis solcher Probleme, daß Auftraggeber und Auftragnehmer in der notwendigen schriftlichen Auftragserteilung auch regeln, ob und welche Unterauftragsverhältnisse eingegangen werden dürfen. Insbesondere die Übergänge von einem Verantwortungsbereich in den anderen sollten klar definiert und die Übergabe geregelt sein. Das schließt ein, daß klar geregelt ist, wer welche Dienstleistung erbringt.

Entgegen den Formulierungen des § 11 BDSG, der davon ausgeht, daß der Auftraggeber dem Auftragnehmer Weisungen erteilt, wird in der Regel der Auftragnehmer die Rahmenbedingungen der Datenvernichtung gegenüber dem Kunden festlegen. Es ist ratsam, in solchen Standardverträgen die notwendigen Ausführungen zum Datenschutz gleich mit aufzunehmen.

Bei der Vernichtung von großen Magnetbändern wird nicht selten immer noch der Magnetkern manuell entfernt und erst dann das Band vernichtet. Eine Maschine, die dies in zwei Arbeitsgängen erledigt, wurde noch nicht vorgefunden.

Magnetplatten werden in der Regel wieder an den Lieferanten zurückgegeben, wenn sie nicht mehr brauchbar sind. Vom Recyclinggedanken her ist dies positiv zu bewerten; allerdings ist der Plattenhersteller ausgerechnet derjenige, der auch defekte Platten noch zum größten Teil lesen kann. Ein Serviceunternehmen, welches weder das Wissen noch die technische Einrichtung hat, alte Festplatten zu lesen, ist deshalb als Vernichter vorzuziehen. Noch besser wäre es, Platten vor der Ausmusterung möglichst physisch mehrfach mit einer Konstante zu überschreiben.

14.3. Datensicherungsprobleme mit Festplatten von Personal-Computern

Unproblematisch sind nur die Fälle, in denen die sogenannte "Festplatte" über einen Wechselrahmen vom PC getrennt und separat unter besonderen Verschluß genommen werden kann. Die Entnahme der Festplatte ist in der Regel erst nach der Betätigung eines Schlosses möglich; dadurch ist die Wechselplatte ebenso schwer zu entfernen, wie eine tatsächlich "fest" eingebaute Festplatte.

Wenn der Nutzer eines PCs aus technischen Gründen seinen PC samt Festplatte an ein EDV-Service-Unternehmen außer Haus gibt, so sollte er sich genau überlegen, welche Daten besonders schutzwürdig sind und deshalb nicht der direkten eigenen Kontrolle entzogen werden sollten. Im Zweifelsfall sollte man die Dateien mit personenbezogenen Daten und sonstige schutzwürdige Daten auf einen externen Datenträger (Diskette, Streamer) sichern und, nachdem man sich vergewissert hat, daß die Sicherung einwandfrei lesbar ist, die in Frage kommenden Bereiche auf der Festplatte physisch löschen. Für die physische Löschung sollte man die zu löschenden Plattenbereiche mehrfach überschreiben. Ein besonders prekäres Beispiel war im Berichtszeitraum mit dem Fall eines von einer Ärztin genutzten PC gegeben (s. oben 9.2.).

15. Anordnung von Maßnahmen nach § 38 Abs. 5 BDSG

Zur Gewährleistung des Datenschutzes nach diesem Gesetz und anderen Vorschriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien regeln, kann die Aufsichtsbehörde anordnen, daß im Rahmen der Anforderungen nach § 9 Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden. Von dieser seit der Novellierung zur

Verfügung stehenden Möglichkeit haben die Aufsichtsbehörden nur in sehr wenigen Fällen bisher Gebrauch machen müssen.

In einem Fall bestand das Problem, daß ein Adresshändler trotz mehrmaliger Hinweise und Aufforderungen durch die Aufsichtsbehörde bei Betroffenenbeschwerden deren Adressdaten sofort aus seinem Datenbestand löschte, so daß weder festgestellt werden konnte, aus welcher Liste bzw. aus welcher Quelle die Adresse stammte, noch für welche weiteren Werbesendungen die Adresse eventuell noch genutzt worden war. Betroffene, die von ihrem Widerspruchsrecht gegen die Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung nach § 28 Abs. 3 BDSG Gebrauch machen wollten, liefen auf diese Weise ins Leere. Beim nächsten up-date durch den Adresseneigentümer, von dem die Adresse ursprünglich stammte, fanden sich so die Betroffenen wieder im Datenbestand.

Die Aufsichtsbehörde sah darin einen organisatorischen Mangel und ordnete, um die Ausübung des Widerspruchsrechts für die Betroffenen sicherzustellen, an, daß das Unternehmen die Datensätze von Betroffenen, deren Beschwerde dort bekannt wird, noch mindestens 3 Monate gesperrt und gekennzeichnet im Bestand zu führen hat.

Die Anordnung wurde bestandskräftig und bei einer nichtangemeldeten Prüfung kontrolliert, wobei festgestellt werden konnte, daß die lange geforderte Maßnahme nun endlich getroffen worden war.

16. Ordnungswidrigkeitenverfahren

Im Berichtsjahr waren 15 Ordnungswidrigkeitenverfahren nach dem BDSG anhängig. So hat die Aufsichtsbehörde in fünf Fällen Verfahren wegen der verspäteten Abgabe der nach § 32 Abs. 1 BDSG erforderlichen Mitteilung über die Aufnahme der meldepflichtigen geschäftsmäßigen Datenverarbeitungstätigkeit eingeleitet (Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 2 BDSG), wobei die betroffenen Unternehmen die meldepflichtige Tätigkeit bereits einige Jahre ausgeübt hatten.

Bei drei dieser Unternehmen wurde gleichzeitig ein Ordnungswidrigkeitenverfahren wegen der entgegen § 36 Abs. 1 BDSG seit Aufnahme der Tätigkeit nicht erfolgten Bestellung eines Datenschutzbeauftragten eingeleitet (Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 5 BDSG). In drei 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). Acht Verfahren sind bereits durch Bußgeldbescheid bestandskräftig abgeschlossen, in den übrigen Fällen wurde noch kein Bußgeldbescheid erlassen.

Wiesbaden, den 8. September 1993

Der Hessische Ministerpräsident
Eichel

Der Hessische Minister des Innern
und für Europaangelegenheiten
Dr. Günther