



14. Wahlperiode

Drucksache **14/1902**

# HESSISCHER LANDTAG

01. 07. 96

## **Vorlage der Landesregierung**

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

Vorgelegt mit der Stellungnahme zum Vierundzwanzigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten - Drucks. 14/1418 - nach § 30 Abs. 2 des Hessischen Datenschutzgesetzes vom 11. November 1986.

Eingegangen am 1. Juli 1996 · Ausgegeben am 16. Juli 1996

Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

**Inhaltsverzeichnis**

	Seite
1. Bearbeitung von an die Behörden herangetragenen Datenschutzbeschwerden nach § 38 Abs. 1 BDSG .....	4
2. Von Amts wegen durchgeführte Überprüfungen von Stellen, die nach § 32 Abs. 1 Nr. 1 bis 3 BDSG geschäftsmäßig personenbezogenen Daten verarbeiten oder nutzen .....	5
2.1 Register .....	5
2.2 Prüfungsübersicht .....	5
2.3 Meldepflicht Ingenieurbüros .....	6
3. Bearbeitung von Anfragen zu Problemen des Datenschutzes.....	6
4. Wirtschaftsauskunfteien .....	7
5. SCHUFA .....	7
5.1 Auskünfte an Serviceprovider im Bereich Funktelefon .....	7
5.2 Die Gefälligkeitsauskunft .....	8
5.3 Verwechslungen .....	8
6. Kreditkartenunternehmen .....	8
7. Versicherungen .....	9
8. Datenverarbeitung im medizinischen Bereich .....	9
8.1 Datenverarbeitung in Alten- und Pflegeheimen .....	9
8.2 Mängel in der Datensicherheit bei Daten, die der ärztlichen Schweigepflicht unterliegen .....	10
9. Arbeitnehmerdatenschutz .....	10
9.1 Nutzung des unternehmensinternen Telefonverzeichnisses für Zwecke Dritter .....	10
9.2 Behandlung von Mitarbeiterpost .....	11
9.3 Leitsätze und Verpflichtungen für Bankmitarbeiter zur Verhinderung von Insidergeschäften .....	12
10. Auslandsdatenverarbeitung .....	12
11. Werbewirtschaft .....	13
11.1 Adreßhandel mit Auslandsbezug .....	13
11.2 Adreßhandel mit Partnerschaftsadressen .....	13
12. Banken .....	13
12.1 Offenlegung der finanziellen Verhältnisse bei Wertpapiergeschäften .....	13
12.2 Geldausgabeautomaten .....	14
13. Der betriebliche Datenschutzbeauftragte .....	14
13.1 Prüfungserfahrungen .....	14

---

13.2	Inkompatibilität von Datenschutzbeauftragtem und Geldwäschebeauftragtem .....	15
14.	Datensicherheit .....	16
14.1	Einsatz von Personalcomputern (PC) .....	16
14.2	Die digital gespeicherte Unterschrift .....	16
14.3	Der PC als Heimarbeitsplatz .....	17
15.	Ordnungswidrigkeitenverfahren .....	17

### 1. Bearbeitung von an die Behörde herangetragenen Datenschutzbeschwerden nach § 38 Abs. 1 BDSG

Die Regierungspräsidien überprüfen als Aufsichtsbehörde nach § 38 Abs. 1 BDSG im Einzelfall die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien regeln, wenn hinreichende Anhaltspunkte dafür vorliegen, daß eine dieser Vorschriften durch eine nicht-öffentliche Stelle verletzt ist, insbesondere wenn es Betroffene selbst begründet darlegen.

Im Berichtsjahr gingen bei den Aufsichtsbehörden 150 Beschwerden gegen Stellen ein, die Datenverarbeitung nach § 28 BDSG für die Erfüllung eigener Geschäftszwecke betreiben oder personenbezogene Daten nach §§ 29, 30 BDSG zur personenbezogenen oder anonymisierten Übermittlung speichern und nutzen.

Alle Beschwerden führten zur Überprüfung der datenverarbeitenden Stellen durch die Aufsichtsbehörden. In 11 Beschwerdefällen wurden Überprüfungen "vor Ort" durchgeführt.

Die Beschwerden betrafen:

- Kreditinformationsdienste (Wirtschaftsauskunfteien, SCHUFA) in 26 Fällen,
- Kreditinstitute in 23 Fällen,
- Versicherungen in 16 Fällen,
- Vereine in 8 Fällen,
- Kreditkartenunternehmen in 5 Fällen,
- das Gesundheitswesen (Ärzte und Krankenhäuser) in 4 Fällen,
- den Einzelhandel in 3 Fällen,
- Markt- und Meinungsforschungsunternehmen in 3 Fällen,
- Adreßverlage in 3 Fällen,
- Fluglinien in 3 Fällen,
- Verlage in 3 Fällen,
- den Versandhandel in 3 Fällen,
- Vermieter in 2 Fällen,
- Kurierdienste in 2 Fällen,
- Reiseveranstalter in 2 Fällen,
- sonstige Unternehmen in 44 Fällen.

In 26 Fällen waren die Beschwerden begründet, davon in je drei Fällen gegen Kreditinstitute in je zwei Fällen gegen speichernde Stellen aus dem Gesundheitswesen, gegen einen Verein, einen Kreditinformationsdienst und eine Versicherung sowie in je einem Fall gegen den Einzelhandel, einen Vermieter, ein Kreditkartenunternehmen, eine Fluglinie, ein Unternehmen aus der Markt- und Meinungsforschung sowie einen Versandhandel. Zehn weitere begründete Beschwerden richteten sich gegen sonstige Unternehmen.

Bei acht 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 64 Fällen sind die Ermittlungen der Aufsichtsbehörde noch nicht abgeschlossen.

Aus den Vorjahren wurden 41 Beschwerdefälle abgeschlossen. Die Beurteilung der Aufsichtsbehörden ergab, daß davon 14 Beschwerden begründet waren. Gerade in diesen Fällen gestaltet sich die Aufklärung oft schwierig und zeitaufwendig. Dabei hatten in drei Fällen Kreditinformationsdienste, in zwei Fällen Vermieter, sowie in je einem Fall ein Kreditinstitut, ein Verein, eine Versicherung, ein Arzt, ein Kreditkartenunternehmen, ein Inkassounternehmen, ein Datenvernichter, ein Markt- und Meinungsforscher und ein sonstiges Unternehmen 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 unzulässi-

ger Weise erfolgt war, mangels eindeutigen Sachverhaltes nicht getroffen werden.

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

### 2.1 Register

Die Aufsichtsbehörden führen nach § 38 Abs. 2 BDSG das Register der 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 1996 waren im Register der meldepflichtigen Stellen bei den Aufsichtsbehörden 631 Unternehmen eingetragen. Die nach § 32 Abs. 1 Ziff. 1 BDSG meldepflichtigen Kreditinformationsdienste und Auskunftsteien haben daran den geringsten Anteil, gefolgt von - nach § 32 Abs. 1 Ziff. 2 BDSG - meldepflichtigen Unternehmen der Markt- und Meinungsforschung. Die nach § 32 Abs. 1 Ziff. 3 BDSG meldepflichtigen Unternehmen, die im Auftrag Dritter Datenverarbeitung als Dienstleistung betreiben, stellen den Hauptanteil des Meldebestands bei den Aufsichtsbehörden.

Innerhalb dieser Gruppe von Dienstleistungsunternehmen sind die Dienstleistungsrechenzentren am stärksten vertreten, was auch der am Markt zu beobachtenden Outsourcingtendenz im Datenverarbeitungsbereich entspricht. Als weitere relevante Branchen sind die Schreibservices und Datenerfasser zu verzeichnen, gefolgt Konzernrechenzentren, Datenträgervernichtern, Adreßhändlern und Lettershops.

### 2.2 Prüfungsübersicht

Im Berichtsjahr wurden 66 Prüfungen nach § 38 Abs. 2 BDSG durchgeführt. Davon betrafen Datenverarbeiter nach § 32 Abs. 1 Ziff. 3 BDSG insgesamt 51, nämlich

- Servicerechenzentren 9
- Konzerndatenverarbeiter 12
- Datenerfasser und Schreibbüros mit Dateiverwaltung 17
- Adreßhändler 4
- Mikroverfilmer 1
- Datenträgervernichter 6
- Telemarketing 3.

Des weiteren wurden 6 Kreditinformationsdienste und 8 Unternehmen aus dem Bereich der Markt- und Meinungsforschung geprüft.

Die Prüfungen brachten folgendes Ergebnis:

- Beanstandungen 27
- Empfehlungen 22
- ohne wesentliche Beanstandungen 17

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 unvollständige Weisungen nach § 11 BDSG vom Auftraggeber
4. mangelhafter Einsatz von Paßworten (Zugriffskontrolle)
5. kein Datenschutzbeauftragter, Mängel in der Tätigkeit,
6. mangelhafte bzw. fehlende Datenträgerverwaltung
7. fehlende Verpflichtung auf das Datengeheimnis (§ 5 BDSG)
8. mangelhafte Dokumentation

Im übrigen wurde bei einer Prüfung im Regierungsbezirk Neustadt an der Weinstraße Amtshilfe geleistet.

### 2.3 Meldepflicht Ingenieurbüros

Ingenieurleistungen, z.B. in den Bereichen Stadtplanung/Stadtentwicklung, Verkehrsplanung und Umweltschutz können in der Regel nur auf der Grundlage einer soliden Datenbasis erbracht werden. Beispielsweise ist es bei der Sanierung von Stadtteilen wichtig zu wissen, welche Bewohner auf welche Art und Weise und zu welchem Zweck den zu untersuchenden Stadtteil nutzen. Eine Straßenplanung ist ohne Ermittlung der zu erwartenden Verkehrsbe-/entlastung nicht sinnvoll. Im Umweltschutz müssen Altlasten sowie die betroffenen ehemaligen und heutigen Grundstückseigentümer ermittelt werden.

Bei diesen Tätigkeiten sind Befragungen - also personenbezogene Datenerhebungen -, Datenspeicherungen und analytische Auswertungen erforderlich. Erst als Abschluß wird die Ingenieurleistung im engeren Sinne erbracht, wobei die gewonnenen Erkenntnisse über den Ist-Zustand in eine Planung übergeleitet werden und die Planung gegebenenfalls durch Bau-/Sanierungsmaßnahmen umgesetzt wird.

Je nach Auftrag kommt es aus den unterschiedlichsten Gründen - Kosten, räumliche Nähe zu dem zu untersuchenden Objekt, Erfahrungen - zu den verschiedensten Auftragskonstellationen.

Solange ein Ingenieurbüro alle Phasen eines der kurz skizzierten Projekte verwirklicht, wird dies insgesamt als Ingenieurleistung bewertet, bei der die Datenverarbeitung nicht als eigenständige Leistung im Vordergrund steht.

Im Einzelfall werden jedoch durchaus Nebentätigkeiten wie die Datenerhebung auch als isolierter Auftrag ausgeführt und die weiteren höherwertigen Tätigkeiten bei einem anderen Ingenieurbüro erledigt.

Diese Konstellation hat datenschutzrechtliche Konsequenzen. Eine Meldepflicht nach § 32 Abs. 1 Ziff. 2 bzw. 3 BDSG ist immer dann zu bejahen, wenn derartige isolierte Datenverarbeitungstätigkeiten auf Dauer geschäftsmäßig angeboten und nicht nur gelegentlich angenommen werden. Diese Unternehmen sind dann gegenüber der jeweils zuständigen Aufsichtsbehörde meldepflichtig. Oft kann die Klärung des jeweiligen Sachverhaltes nur in Zusammenarbeit mit der Aufsichtsbehörde erfolgen und muß eine Analyse der Aufträge in der Vergangenheit und eventuell zukünftige Veränderungen dieser Auftragsstruktur einbeziehen.

### 3. Bearbeitung von Anfragen zu Problemen des Datenschutzes

Ein weiterer Bereich der Tätigkeit der Aufsichtsbehörden ist die Beantwortung von Anfragen zu verschiedensten datenschutzrechtlichen Problemstellungen, die nur zum Teil schriftlich abgewickelt wurden.

Im Berichtszeitraum wurden zahlreiche Anfragen an die Aufsichtsbehörden herangetragen. Das Spektrum reichte von der Bitte um Erteilung allgemeiner Informationen zum Datenschutz bis zur Bitte um Beurteilung komplexer technischer und juristischer Sachverhalte, um eventuelle datenschutzrechtliche Bedenken bereits im Vorfeld einer geplanten Maßnahme ausräumen zu können. Allerdings ist darauf hinzuweisen, daß ein Rechtsanspruch auf Beratung durch die Aufsichtsbehörde nur für betriebliche Datenschutzbeauftragte nach § 37 Abs.1 BDSG gegeben ist, wenn sie sich in Zweifelsfällen an die Behörde wenden. Soweit die Aufsichtsbehörden dazu in der Lage waren, wurden allerdings im Berichtszeitraum auch noch Eingaben durch Unternehmensleitungen und Rechtsvertreter bearbeitet, da eine Abklärung von Datenschutzproblemen im Planungsstadium von Maßnahmen sicherlich sinnvoller ist als die Befassung der Aufsichtsbehörde, wenn Maßnahmen bereits in die Tat umgesetzt worden sind.

Schwerpunkt war hierbei mit ca. 18 v.H. der Fälle die Tätigkeit des betrieblichen Datenschutzbeauftragten, gefolgt von Anfragen zur Datenverarbeitung in Vereinen und zur Meldepflicht nach § 32 BDSG mit je ca. 7 v.H. der Fälle.

Die Anfrager waren zu je ca. 30 v.H. betroffene Bürger und Unternehmen. Der Anteil anfragender Verbände und Vereine belief sich auf ca. 19 v.H. gefolgt von Behörden und betrieblichen Datenschutzbeauftragten mit nur je ca. 6 v.H. der eingegangenen Anfragen.

#### 4. Wirtschaftsauskunfteien

Im letzten Tätigkeitsbericht wurde bereits die Praxis von Wirtschaftsauskunfteien dargestellt, Aussagen zum "zulässigen Höchstkredit" zu treffen. Solche Festlegungen basierten und basieren in der Regel nicht auf konkreten Fakten über das jeweilige Unternehmen, sondern werden nach bestimmten Verfahren aus den der Wirtschaftsauskunftei vorliegenden Zahlen, z.B. der veröffentlichten Gesellschaftereinlagen, errechnet. Der Aufsichtsbehörde war in Einzelfällen vorgetragen worden, daß die dabei zustande gekommenen Empfehlungen zu einer falschen, negativen Einschätzung des Unternehmens geführt hätten.

Diese und ähnliche Probleme der Methodik bei der Erstellung von Aussagen und Einschätzungen haben in der Regel eine langwierige Diskussion zwischen Aufsichtsbehörde und Wirtschaftsauskunftei zur Folge. Auch in der oben geschilderten Frage ist bisher eine Abänderung des Verfahrens nicht erreicht worden.

Generell ist zu beobachten, daß die Methoden der Erkenntnisgewinnung durch die Wirtschaftsauskunfteien zunehmend verfeinert werden. So wird versucht, mittels einer immer größeren Zahlenbasis die einzelnen Unternehmen in eine fein abgestufte Bewertungsskala zu bringen. Dabei spielen z.B. die einzelnen Zahlungserfahrungen, die in einer bestimmten Anzahl von Unternehmen einer Branche an die Wirtschaftsauskunftei übermittelt werden eine Rolle und dienen dazu, die wirtschaftliche Zuverlässigkeit des einzelnen Unternehmens auf dem Hintergrund der Kenntnis von Branchengrößen genauer einschätzen zu können. Dabei werden keine unternehmens- oder personenbezogene Daten anderer Unternehmen übermittelt, sondern lediglich aggregierte Zahlen. Dem Anfrager wird damit das Werkzeug in die Hand gegeben, selbst mit Hilfe der mitgeteilten Daten seine Schlüsse zu ziehen.

Da mit solchen Branchenkennzahlen keine personen- bzw. unternehmensbezogenen Daten des angefragten Unternehmens übermittelt werden, muß sich eine datenschutzrechtliche Bewertung darauf beschränken, daß nicht durch eine auf einer ungenügenden Zahlenbasis beruhenden Branchendarstellung ein falscher Eindruck über die mögliche Einordnung des angefragten Unternehmens entstehen kann. In den der Aufsichtsbehörde vorliegenden Fällen konnten solche auf mangelhaften, d.h. zu geringen Zahlen beruhenden Fehleinschätzungen nicht entstehen.

#### 5. SCHUFA

Als Gemeinschaftseinrichtung der kreditgebenden deutschen Wirtschaft speichert die SCHUFA in einem sehr bedeutenden Umfang Daten von Personen, die in irgendeiner Weise, z.B. als Bankkunde, Versandhauskunde, Leasingnehmer unter anderem, in kreditorisch relevanten Rechtsbeziehungen stehen. Nach dem Eigenverständnis der SCHUFA soll ihre Tätigkeit die kreditgebende Wirtschaft schützen und gleichzeitig den Schuldner vor einer Überschuldung bewahren.

In jedem Berichtszeitraum kamen bisher Fälle vor die Aufsichtsbehörden, in denen Betroffene sich durch Speicherungen bzw. Auskünfte der SCHUFA in ihren Persönlichkeitsrechten beeinträchtigt sahen. Diese Fallzahlen sind allerdings angesichts des gesamten Tätigkeitsumfangs der SCHUFA minimal.

##### 5.1 Auskünfte an Serviceprovider im Bereich Funktelefon

In einem Fall hatte eine Rentnerin mehrfach neue Kreditkarten beantragt und auch erhalten und sich dann jeweils umgehend an Geldautomaten mit Bargeld versorgt. Auf diese Weise war ein erheblicher Schuldenberg angewachsen. Als die Betroffene einen Vertrag über einen Funktelefonanschluß abschließen wollte, scheiterte dies an den dem Serviceprovider mitgeteilten erheblichen Negativdaten der Betroffenen. Da mit der Aushändigung von Telefonkarte und Gerät die sofortige Möglichkeit der Nutzung eingeräumt wird

und sehr schnell hohe Beträge zustandekommen können, haben Serviceprovider im Funktelefonbereich von der SCHUFA die Möglichkeit erhalten, sich über die Negativdaten der potentiellen Kunden Kenntnis zu verschaffen. Diese für die SCHUFA neuen Vertragsverhältnisse sind datenschutzrechtlich allerdings nicht unproblematisch, da diese Vertragspartner der SCHUFA im Wege der Nachmeldung eine gewisse Zeitlang auch mit weiteren Auskünften versorgt werden, wenn sie diese gar nicht benötigen. Im gegebenen Fall diene allerdings die SCHUFA-Auskunft tatsächlich dazu, die Betroffene vor weiterer Verschuldung, die sie nicht mehr übersehen konnte, zu bewahren.

## 5.2 Die Gefälligkeitsauskunft

Von der SCHUFA und Auskunfteien dürfen Auskünfte nur erteilt werden, wenn der Empfänger ein berechtigtes Interesse glaubhaft darlegt. SCHUFA-Auskünfte sind wegen ihrer Aktualität und ihres detaillierten Informationsgehaltes besonders beliebt. Der Kreis der Unternehmen, die als SCHUFA-Anschlußpartner zur Datenabfrage berechtigt sind, ist durch das oben dargestellte Merkmal der Absicherung eines kreditorischen Risikos begrenzt. Andere oder Privatpersonen erhalten von der SCHUFA (außer über sich selbst) keinerlei Auskünfte. Dennoch wurden der Aufsichtsbehörde immer wieder Fälle dargestellt, in denen sich insbesondere Rechtsanwälte gerühmt haben sollen, Zugang zu SCHUFA-Daten zu haben. Erklärlich wird dies dadurch, daß in Einzelfällen auch Unternehmen, die zur SCHUFA-Abfrage berechtigt sind, von Unberechtigten als Anfrager vorgeschoben werden. So hatte in einem konkreten Fall die Mitarbeiterin eines Versandhandelsunternehmens bei einer Anfrage als berechtigtes Auskunftsinteresse "Warenkredit" angegeben, obwohl der Betroffene kein Kunde des Unternehmens war. Die Auskunft wurde vielmehr für einen privaten Bekannten benötigt, der sonst keine SCHUFA-Auskunft erhalten hätte.

## 5.3 Verwechslungen

Immer wieder passiert es, daß Schuldnerdaten von der SCHUFA nicht richtig zugeordnet werden können, sei es, weil Meldungen aus dem Schuldnerregister der Amtsgerichte ohne Angabe des Geburtsdatums erfolgen, oder weil Daten nicht eindeutig zugeordnet werden können, jedoch trotzdem übermittelt werden.

Auch wenn durch die SCHUFA in der Beauskunftung darauf hingewiesen wird, daß die Negativdaten "ohne Geburtsdatum bekannt geworden" seien, wie in einem der Aufsichtsbehörde vorgelegten Fall, trägt die SCHUFA die Verantwortung für die Übermittlung eventuell nicht zutreffender Daten. Im aktuellen Fall führten zwei eine andere Person betreffende Haftbefehle dazu, daß der potentielle Vertragspartner ohne weitere eigene Prüfung einen Vertragsabschluß verweigerte. Der Betroffene fand sich dadurch in der Situation nachweisen zu müssen, daß die Negativdaten nicht bei ihm vorlagen. Eine derartige "Beweislastumkehr" ist nicht akzeptabel. Die Datenschutzaufsichtsbehörden haben hierzu stets die Meinung vertreten, daß bei Zweifeln aufgrund von Datendifferenzen eine Beauskunftung dieser Daten zu unterbleiben hat.

Leider ist diese Situation auch durch die Novellierung der Vorschriften der Zivilprozeßordnung zum Schuldnerverzeichnis (§ 915) nicht verbessert worden. Noch immer ist nicht vorgesehen, daß bei Eintragungen ins Schuldnerregister das Geburtsdatum des Betroffenen mit zu erheben und zu speichern ist.

## 6. Kreditkartenunternehmen

Die etwas erhöhte Anzahl von Eingaben gegen Kreditkartenunternehmen zeigte keinen deutlichen Schwerpunkt.

Nur eine Beschwerde war begründet.

Eine in den Vorjahren akut gewordene Problematik, die Speicherung von Kundendaten weit über die Beendigung des Kreditkartenverhältnisses hinaus, konnte einer positiven Klärung zugeführt werden. Es kann damit nicht mehr vorkommen, daß Kartenumsätze, die erst nach Ablauf des Kartenvertrages an das Kreditkartenunternehmen gemeldet werden, noch ohne weiteres dem



früheren Kunden angelastet werden. In solchen Fällen wird die Rechnung dem früheren Kunden geschickt mit der Bitte um eigenständigen Ausgleich nach Überprüfung, ob die Umsätze von ihm auch tatsächlich getätigt wurden.

Eine größere Anzahl meist fernmündlicher Anfragen wurde verursacht durch die in der Presse breit geführte Diskussion im Zusammenhang mit der neuen Bahncard der Deutschen Bahn AG.

Der Bahnkunde erhielt ab Mitte des Jahres 1995 die Wahl zwischen der alten Bahncard, der Elektroncard - eine auf Guthabenbasis geführte Karte - und einer echten Kreditkarte mit der Zusatzfunktion Bahncard. Das Antragsformular verlangte allerdings für alle drei verschiedenen Versionen auf den ersten Blick die Angabe derselben Daten, unter anderem zur Bonität, wie sie sonst nur im Kreditkartenbereich üblich waren.

Nachdem zunächst unklar war, welche Aufsichtsbehörde in dieser Angelegenheit zuständig ist, übernahm im Einvernehmen der Berliner Datenschutzbeauftragte als Aufsichtsbehörde im nicht-öffentlichen Bereich und damit zuständig für den Unternehmenssitz der Deutschen Bahn AG die Federführung und konnte eine datenschutzgerechte und kundenfreundliche Gestaltung des Verfahrens durchsetzen. Im Ergebnis werden nunmehr für jede der drei Kartenversionen gesonderte Anträge verwendet, bei denen sich die Datenerhebung auf diejenigen Daten beschränkt, die für das jeweilige Verfahren auch tatsächlich benötigt werden. Darüber hinaus wird der Kunde darüber informiert, durch welche Unternehmen und wo, beispielsweise im Wege des Outsourcing auch in den USA, seine Daten verarbeitet werden.

## 7. Versicherungen

Obwohl gegen Versicherungen mit 14 Beschwerden deutlich mehr als im Vorjahr (7) eingingen, zeigen sich auch hier keine deutlichen Schwerpunkte oder besondere Probleme über die bereits bekannten hinaus. Nur zwei der im Berichtszeitraum eingegangenen Beschwerden waren berechtigt.

Im Bereich der Kraftfahrzeugversicherung hatte die große Differenzierung in dieser Branche infolge der Deregulierung der Tarifgestaltung zur Folge, daß zur Bestimmung des zu zahlenden Versicherungsbeitrags deutlich mehr personenbezogene Daten als früher vom Betroffenen an den Versicherer abzugeben waren. Auch Interessenten, die sich lediglich unverbindlich per Telefon nach der zu erwartenden Beitragshöhe erkundigen wollten, wurden so mit Fragen z.B. nach jährlicher Fahrleistung, Familienstand, Kinderzahl und Beruf konfrontiert, da bei bestimmten Versicherern jedes dieser Daten Einfluß auf die Höhe des Versicherungsbeitrags hat.

## 8. Datenverarbeitung im medizinischen Bereich

### 8.1 Datenverarbeitung in Alten- und Pflegeheimen

Eine Eingabe befaßte sich mit der Verarbeitung personenbezogener Daten in Alten-/Pflegeheimen. Ein Angehöriger eines Pflegeheimbewohners hatte bemerkt, daß bei der Pflegeleitung nicht nur persönliche Daten des Heimbewohners, sondern auch Daten zu ihm als Angehörigen gespeichert waren.

Nach § 8 des Heimgesetzes müssen in entsprechenden Einrichtungen Buchhaltungsdaten geführt werden. Ein Heimvertrag ist mit dem Betroffenen oder seinem Vertreter abzuschließen. Weitere Regelungen zur Verarbeitung personenbezogener Daten sind nicht vorhanden.

Dementsprechend werden allgemeine Daten zu Person, Krankenkasse und Pflegegruppe für die Erfüllung der Verwaltungsaufgaben geführt. Darüber hinaus wird in der Regel eine sogenannte Pflegedokumentation geführt. Sie enthielt in dem vorliegenden Fall folgende Daten:

- Allgemeine Angaben über Lebensgewohnheiten und Hobbys
- Vorlieben und Abneigungen
- Kontaktadressen
- Kostformen
- Diagnosen, Allergien, Einschränkungen
- Körperhilfsmittel

- Familiäre Situation
- Betreuung
- Krankenkasse
- Behandelnde Ärzte
- Medikation
- Durchführungsnachweise
- Pflegegruppe.

Diese Daten sollen von allen in der Pflege, Betreuung und Therapie der Bewohner/-innen tätigen Personen, unter Einbeziehung der behandelnden Ärzte/-innen, regelmäßig und fortlaufend geführt und eingesehen werden. Die Dokumentation wurde auf Stammblätttern und Berichtsblättern handschriftlich geführt, soll jedoch auf automatische Datenverarbeitung umgestellt werden, da die nach dem Pflegeversicherungsgesetz erforderlichen Nachweise nur mit Hilfe eines automatisierten Verfahrens zu erstellen seien.

Die Datenverarbeitung ist im Rahmen des Vertragsverhältnisses zwischen Heim und Bewohner zulässig (§ 28 Abs. 1 Ziff. 1 BDSG). Angaben zu Vorlieben und Abneigungen sowie zur familiären Situation müssen allerdings kritisch betrachtet werden. Die Gefahr ist hier groß, daß Daten Dritter, mit denen kein Vertragsverhältnis besteht, in nicht mehr zulässiger Weise verarbeitet werden. Die Speicherung der Krankenkasse ist lediglich für die Verwaltung zum Zweck der Abrechnung, nicht jedoch im Rahmen der Pflege sinnvoll und erforderlich.

Klargestellt werden mußte, daß jeder Betroffene, eventuell über seinen Vertreter, Auskunft über die zu seiner Person gespeicherten Daten verlangen kann. Dies betrifft auch Dritte, soweit ihre Daten verarbeitet werden.

## **8.2 Mängel in der Datensicherheit bei Daten, die der ärztlichen Schweigepflicht unterliegen**

Ein Beschwerdeführer übersandte der Aufsichtsbehörde die Kopien von Schriftstücken, die er im Müllcontainer eines Mehrfamilienhauses entdeckt hatte. Sie enthielten Angaben zu Diagnosen und Medikationen von Patientinnen einer gynäkologischen Praxis. Es stellte sich heraus, daß es sich um Tagesprotokolle aus der EDV einer gynäkologischen Praxis handelte. Die Ärztin hatte das Tagesprotokoll regelmäßig zur weiteren Bearbeitung mit in die Privatwohnung genommen. Dabei sind nicht mehr benötigte Ausdrücke in den Müllcontainer gelangt.

Ähnliche Fälle wurden auch in der Vergangenheit immer wieder an die Aufsichtsbehörde herangetragen. Sie zeigen, daß die leichte Verfügbarkeit von Daten, die automatisiert verarbeitet werden, manchmal auch zu einem leichtsinnigen Umgang mit ihnen führt.

Es ist hervorzuheben, daß die von der Aufsichtsbehörde angesprochenen Verantwortlichen in der Regel einsichtig und zu Änderungen ihrer Verarbeitungs- und Arbeitsweise bereit sind. Es wird allerdings auch beklagt, daß die alltägliche Arbeitsbelastung oft keine Zeit für Datensicherungsmaßnahmen lasse, eine Behauptung, die nur zum Teil akzeptiert werden kann. In allen Fällen wurden jedoch bisher Ratschläge zur Verbesserung des Datenschutzes und Aufklärung allgemein dankbar angenommen.

## **9. Arbeitnehmerdatenschutz**

### **9.1 Nutzung des unternehmensinternen Telefonverzeichnisses für Zwecke Dritter**

In jedem größeren Unternehmen gibt es interne Telefonverzeichnisse, die mit großem Aufwand in regelmäßigen Abständen aktualisiert werden. Eines der größten Unternehmen in Hessen beabsichtigte, in diesem internen Telefonverzeichnis Dritten Raum für Werbezwecke zur Verfügung zu stellen. Darüber hinaus sollte das Telefonverzeichnis auch von Nichtteilnehmern zu Marketing- und anderen Zwecken käuflich erworben werden können.

Ziel war, zumindest einen Teil der Herstellungskosten durch die damit erhofften Einnahmen zu kompensieren. Gängige Praxis ist es bereits bisher, im Fall von Werbeeinschüben den werbenden Unternehmen komplette Belegexemplare des Verzeichnisses zur Verfügung zu stellen.

Auf der anderen Seite wird in den Unternehmen über massive Telefonwerbung am Arbeitsplatz geklagt, die fast ausschließlich aus der Nutzung von firmeninternen Telefonverzeichnissen durch Dritte resultieren dürfte (vgl. dazu der im letzten Tätigkeitsbericht, Ziff. 12.1 geschilderte Fall eines Kapitalanlageberatungsunternehmens). Solche Werbung ist auch im Fall des Anrufs am Arbeitsplatz von der wettbewerbsrechtlichen Rechtsprechung zunehmend als rechtswidrig beurteilt worden.

Selbstverständlich dürfen Telefonverzeichnisse innerhalb des Teilnehmerkreises unbedenklich verbreitet werden. In der Kommunikation der Mitarbeiter untereinander besteht ja der wesentliche Zweck solcher Verzeichnisse. Gegenüber Dritten bedeutet die Herausgabe des Telefonverzeichnisses jedoch die Übermittlung von Arbeitnehmerdaten, die nach § 28 Abs. 2 Ziff. 1 a BDSG restriktiv geregelt ist. Es gilt bei Daten aus dem Arbeitsverhältnis die Vermutung, daß der Betroffene ein überwiegendes, schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.

Im Falle der Plazierung von Werbung ist daher von der Aufsichtsbehörde empfohlen worden, dem werbenden Unternehmen zum Nachweis des Abdrucks entweder Einsicht in das komplette Verzeichnis zu gewähren oder nur die entsprechenden Teile (Seiten) als Beleg gegebenenfalls unter Hinweis auf die strikte Zweckbindung der Verwendung herauszugeben.

Unternehmen, die das Telefonverzeichnis für (Telefon-)Marketingzwecke nutzen wollen, können dagegen aus wettbewerbsrechtlichen Gründen kein berechtigtes Interesse an der Übermittlung kompletter Verzeichnisse geltend machen.

Das Unternehmen hat sich dieser auch von der Datenschutzbeauftragten von Anfang an vertretenen Meinung angeschlossen.

## 9.2 Behandlung von Mitarbeiterpost

In mehreren Fällen, zum Teil auch fernmündlich, wurde von Arbeitnehmern Kritik an der Praxis der Behandlung von persönlicher Post durch den Arbeitgeber geübt.

In den meisten Fällen ist hier jedoch keine Zuständigkeit der Aufsichtsbehörde gegeben, da es an einer Verarbeitung von personenbezogenen Daten in oder aus einer Datei fehlt. Es kommt damit auf den erkennbaren Inhalt der Poststücke an. Enthalten die Poststücke personenbezogene Daten, die offensichtlich aus einer Datei entnommen sind (§ 27 Abs. 2 BDSG), so gelten die Vorschriften des Bundesdatenschutzgesetzes für die Datenverarbeitung nicht-öffentlicher Stellen (§§ 27 ff. BDSG), damit auch die Sicherheitsanforderungen (§ 9 BDSG und gegebenenfalls Anlage) und § 38 mit den Befugnissen der Aufsichtsbehörde.

Es liegt auf der Hand, daß diese Einschränkung nicht nur höchst unpraktikabel sondern auch für Betroffene kaum nachvollziehbar ist. Auf diesem Hintergrund sind Arbeitnehmer z.B. darauf verwiesen, ihre Datenschutzbelange mittels individueller Klage vor dem Arbeitsgericht selbst zu vertreten, wenn ihre persönlichen Daten durch den Arbeitgeber in Briefform unzulässig offen behandelt werden. Nur wenn die verwendeten Dokumente offensichtlich aus einer Datei stammen (z.B. Ausdruck aus der Gehaltsabrechnungsdatei), können die Regelungen des Bundesdatenschutzgesetzes in Anspruch genommen werden.

Eine solche Gestaltung lag in einem Fall vor, in dem innerbetriebliche persönliche Post, z.B. Mitteilungen des Arbeitgebers, private Post zwischen Mitarbeitern, aber auch Gehaltsabrechnungen und Schreiben des Arbeitgebers anderer Art aus Dateien, für die abwesenden Mitarbeiter bis zur Abholung in betrieblich offen zugängliche Postmappen gelegt wurden, von denen mehrere Tausend in einem großen Raum konzentriert aufbewahrt werden. Nachdem von den Mitarbeitern öfters über Abhandenkommen von Schreiben geklagt wurde, wandte sich die Personalvertretung an die Aufsichtsbehörde. Nach einer Ortsbesichtigung und Gesprächen mit den Verantwortlichen durch die Aufsichtsbehörde wurde ein Kompromiß gefunden, der zum einen den Arbeitnehmerinteressen entgegenkommen soll, zum anderen das Unternehmen nicht sofort mit ganz erheblichen Investitionskosten für die Einrichtung von Schließfächern belastet: Da bisher das Abhandenkommen von Poststücken auch damit zusammenhing, daß der Inhalt (Art der Abrechnung) bereits von außen erkennbar war, wurden die Umschläge und Ausdrücke im

Bereich der Kuvertfenster so umgestaltet, daß ein Erkennen nicht mehr möglich war. Sollte sich mit dieser Maßnahme keine Besserung erzielen lassen, so wird allerdings der Arbeitgeber eventuell auch unter erheblichen Investitionskosten eine andere Lösung finden müssen, die seine Verpflichtung hinsichtlich Transport- und Organisationskontrolle (vgl. Anlage 9 zu § 9 BDSG, Ziff. 9 und 10) abdeckt.

### **9.3 Leitsätze und Verpflichtungen für Bankenmitarbeiter zur Verhinderung von Insidergeschäften**

Ende 1994 erhielten in vielen Kreditinstituten die Mitarbeiter Schreiben und Fragebögen der Unternehmensleitungen, in denen die Mitarbeiter darauf hingewiesen wurden, daß ihnen die Nutzung interner Kenntnisse aus dem Bereich Wertpapiergeschäfte für private eigene Zwecke oder Zwecke Dritter untersagt sei. Zunächst auf der Grundlage einer Richtlinie des Bundesaufsichtsamtes für die Kreditwirtschaft wurden Mitarbeiter aufgefordert, zum Teil umfangreiche Fragebögen zur eigenen finanziellen Situation, aber auch zu Verhältnissen Dritter, z.B. Angehöriger, deren Bankgeschäfte durch den Mitarbeiter geführt werden, zu beantworten.

Diese Richtlinie wurde später durch das Wertpapierhandelsgesetz ersetzt, womit eine als Grundlage für den Eingriff in das informationelle Selbstbestimmungsrecht taugliche Rechtsnorm geschaffen war.

Sowohl im öffentlichen Bereich (öffentlich-rechtliche Sparkassen) als auch im privatwirtschaftlichen Bereich der anderen Kreditinstitute wurde in ähnlicher Weise verfahren.

Während sich die Landesdatenschutzbeauftragten für den Bereich der öffentlichen Sparkassen zum Beispiel mit der zu breiten Streuung sehr umfassender Fragebögen (vgl. 24. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten für das Jahr 1995) befassen konnten, waren den Aufsichtsbehörden im nicht-öffentlichen Bereich die Hände gebunden: Die besagten Fragebögen wurden nämlich in aller Regel lediglich in Akten abgelegt, so daß keine Dateiverarbeitung in Dateien vorlag und das Bundesdatenschutzgesetz damit nicht anwendbar war. Die Aufsichtsbehörde mußte sich daher darauf beschränken, den Betroffenen in dieser Weise allgemein Auskunft zu geben.

## **10. Auslandsdatenverarbeitung**

Bereits im letzten Tätigkeitsbericht wurde dargestellt, daß grenzüberschreitende Datenverarbeitungen immer selbstverständlicher werden. Dieser Trend hat sich zumindest im europäischen Bereich verstärkt, gefördert sicherlich auch durch die Verabschiedung der europäischen Richtlinie zum Datenschutz im Jahr 1995. Dennoch dürfte es der Praxis entsprechen, daß auch Übermittlungen ins nichteuropäische Ausland und von dort eine erhebliche Rolle spielen. Beispiele dafür finden sich immer wieder in Presseberichten über die Datenverarbeitung für deutsche Unternehmen z.B. in asiatischen Ländern. Die damit verbundenen datenschutzrechtlichen Probleme werden den Aufsichtsbehörden nur selten zur Beurteilung vorgelegt. Eine Melde- oder gar eine Genehmigungspflicht gibt es bisher nicht; sie wird erst durch die infolge der europäischen Datenschutzrichtlinie notwendigen Anpassung deutschen Rechts auf deutsche Datenverarbeiter und Aufsichtsbehörden zukommen.

Im Fall UPS (vgl. dazu Ziff. 14), zu dem im letzten Tätigkeitsbericht kein abschließendes Ergebnis berichtet werden konnte, wurde hinsichtlich der Übermittlungen von Daten in die USA ein akzeptabler Abschluß gefunden. Dabei ist zu unterstreichen, daß das Unternehmen stets bemüht war, Anregungen der Aufsichtsbehörde zur Gestaltung der vertraglichen Beziehung mit den amerikanischen Rechenzentren des Mutterunternehmens aufzunehmen und umzusetzen. Da Kundendaten und Daten der Empfänger von Paketsendungen wie weiter unten ausgeführt zur weiteren Verarbeitung in Rechenzentren in die USA übermittelt werden, und es sich bei den betroffenen Staaten der USA zumindest bislang um Länder handelt ohne ein angemessenes Datenschutzniveau, war eine diesen Mangel ausgleichende Vereinbarung zwischen den beteiligten Unternehmen erforderlich, um die Übermittlung rechtlich zu ermöglichen. Eine solche Vereinbarung wurde der Aufsichtsbehörde im Berichtsjahr im Entwurf vorgelegt und soll 1996 wirk-

sam werden. Inwieweit allerdings solche Vereinbarungen in der Praxis der ausländischen Partnerunternehmen tatsächlich umgesetzt werden, muß abgewartet werden, sofern eine Beurteilung von hier aus überhaupt möglich ist. Es muß zunächst darauf vertraut werden, daß Wettbewerber sich ähnlichen Bedingungen unterwerfen werden und ein gegenseitiges Interesse an der Einhaltung von Standards entsteht.

## **11. Werbewirtschaft**

### **11.1 Adreßhandel mit Auslandsbezug**

Direktmarketingadressen befinden sich im Regelfall im Eigentum von Unternehmen (z.B. Versandhandel) und werden über spezielle Marketingunternehmen (Adreßbroker) an bestimmte werbewillige Unternehmen zur Nutzung angeboten. Die Bestimmungen des § 28 Abs. 2 Ziff. 1b BDSG geben für derartige Aktionen einen ausreichenden Spielraum.

Probleme entstehen, wenn sich entweder die speichernde Stelle ("Eigentümer" der Adressen) oder der Adreßbroker im Ausland befinden. In einem der Aufsichtsbehörde vorgelegten Fall befand sich der Adreßbroker in Italien. Von dort wurden Adressenkollektionen angeboten, die in Deutschland aus datenschutzrechtlichen Gründen unverkäuflich wären, da sie vorwiegend aus dem politisch-religiösen Bereich kamen. Die Nutzung solcher Adreßbestände durch deutsche Unternehmen zu Werbezwecken widerspricht zwar auch dem Datenschutz, ist aber, da die Kontrolle über den "Verteiler" fehlt, kaum zu verhindern.

Solange in Italien ein angemessener Datenschutz und die Überwachung seiner Einhaltung rechtlich nicht garantiert ist, wird dieser Adreßhandel weiter funktionieren. Zur Zeit kann lediglich spekuliert werden, wie die deutschen Adressen nach Italien verkauft werden. Sicher ist lediglich, daß sie zuvor bereits mit datenschutzrechtlich unzulässigen Zuordnungskriterien aus dem Bereich des Bundesdatenschutzgesetzes exportiert worden sind.

### **11.2 Adreßhandel mit Partnerschaftsadressen**

Ein Unternehmen verkaufte ausschließlich private Kontaktadressen an interessierte Männer. Die Adressen der kontaktsuchenden Männer wurden wiederum über einen Adreßbroker angeboten. Die genannte Adreßpersonengruppe ist offensichtlich als Käufersegment besonders interessant. Bereits der Wunsch nach Adressen zur Erreichung partnerschaftlicher Kontakte und damit verknüpfte sexuelle Wunschvorstellungen gehen weit in den persönlichen Intimbereich und lassen auch Schlüsse auf sonstige Verhaltensweisen der Interessenten zu.

Die Europarats-Konvention zum Datenschutz von 1981 untersagte bereits eine Vermarktung von derartigen Adressen. Es werden ohne eine gesonderte Einwilligung der Betroffenen auch nach dem BDSG schutzwürdige Interessen der Betroffenen am Ausschluß der Adreßübermittlung überwiegen.

Im geprüften Fall verfügte der Adreßeigentümer über keine Einwilligung der Betroffenen. Der geprüfte Adreßbroker stellte daraufhin die Vermarktung der Adressen ein. Die für den Adreßeigentümer zuständige Aufsichtsbehörde stellte sicher, daß die Adressen auf anderen Wegen nicht weiter vermarktet werden.

## **12. Banken**

### **12.1 Offenlegung der finanziellen Verhältnisse bei Wertpapiergeschäften**

Aufgrund vorangegangener Schadensersatzklagen von Kunden verlangten verschiedene Banken von ihren Privatkunden nach § 31 Abs. 2 Ziff. 1 Wertpapierhandelsgesetz (WpHG) Angaben über Erfahrungen oder Kenntnisse in Wertpapiergeschäften, über die verfolgten Ziele und über die finanziellen Verhältnisse. Die Bank ist verpflichtet, die Angaben des Kunden zu dokumentieren; bei Prüfungen der Bank wird das Vorhandensein der Dokumentationen kontrolliert.

In mehreren Fällen schrieben die Banken alle Depotkonteninhaber(innen) an und baten mittels eines Formulars um nähere Angaben, obwohl die Kunden keine Absicht geäußert hatten, Wertpapiere zu erwerben. Für eine echte Vermögensverwaltung sind eine detaillierte Klärung und ein Beratungsgespräch sicher stets erforderlich. Die generelle und detaillierte Befragung aller Kunden berücksichtigt jedoch nicht, daß sich die Verpflichtung des Wertpapierdienstleistungsunternehmens nach § 31 Abs. 2 letzter Halbsatz WpHG an den Interessen des Kunden und Art und Umfang der beabsichtigten Geschäfte orientieren soll. Die betroffenen Kunden befürchteten - wahrscheinlich nicht zu Unrecht -, daß ihre detaillierten Vermögensangaben eventuell unerwünschte Kaufangebote der Banken nach sich ziehen werde.

## 12.2 Geldausgabeautomaten

Ein Bargeldabheber stellte fest, daß er auf der Rückseite des frei aufgestellten Bargeldautomaten durch die Lüftungsschlitze auf einem Protokolldruck die Bargeldtransaktionen vorheriger Geldabheber erkennen konnte.

Bargeldabhebungen von Automaten werden zur Sicherheit für den Kunden auf Magnetspeicher (am Geldautomaten und gegebenenfalls zusätzlich beim Zentralrechner) und auf Papier protokolliert. Fehler wegen Stromausfalls, wegen defekter Magnetspeicher oder wegen Datenfernübertragungsstörungen lassen sich mit der Protokollierung auf Papier im Fehlerfall in der Regel aufklären. Manipulationen werden durch die mehrfache Protokollierung zusätzlich erschwert. Aus den vorgenannten Gründen wird zur Zeit nicht auf den Papierausdruck verzichtet, obwohl ein zweites Speichermedium - z.B. eine nur einmal beschreibbare CD-ROM - den gleichen Zweck erfüllen könnte.

Da elektrische Geräte Hitze entwickeln, sind Lüftungsschlitze für den Geldausgabeautomaten unverzichtbar. Bei älteren Geldausgabeautomaten eines bestimmten Herstellers sind die Lüftungsschlitze jedoch so unglücklich angebracht, daß die jeweils fünf Transaktionen zurückliegende Bargeldabhebung erkennbar ist. Einem Laien ist zwar die Interpretation der Protokolldaten nicht möglich; es kann aber abgelesen werden, von welcher Kontonummer zu welcher Uhrzeit Geld abgehoben wurde. Sobald sich die beschriebene Papierrolle weiter aufspulte, war die Transaktion neugierigen Blicken entzogen.

Die betroffene Bank hat erfreulicherweise sofort reagiert und nach Rücksprache mit dem Geldautomatenhersteller einen Teil der Lüftungsschlitze von innen mit einer Blende abgedeckt. Die Arbeiten konnten von der Bank problemlos selbst ausgeführt werden. Bei neueren Geldausgabeautomaten bzw. wenn die Geldausgabeautomaten anders aufgestellt sind, tritt das geschilderte Problem nicht auf.

## 13. Der betriebliche Datenschutzbeauftragte

### 13.1 Prüfungserfahrungen

Im Prüfungszeitraum wurden mit den Prüfungen einhergehend systematisch Erkenntnisse über die Bestellung von betrieblichen Datenschutzbeauftragten und die Erfüllung der gesetzlichen Anforderungen zusammengetragen. Sie sind, auch wenn sie nur einen kleinen Ausschnitt zeigen, leider als sehr unbefriedigend zu bezeichnen.

Von 56 geprüften Unternehmen hatten 7 keinen Beauftragten für den Datenschutz bestellt, obwohl sie der Pflicht zur Bestellung nach § 36 BDSG unterlagen.

Bei 6 Unternehmen war nur eine mangelhafte Tätigkeit, zum Teil Untätigkeit festzustellen. Bei 2 Unternehmen fehlte "nur" eine ordentliche Fortbildung des Datenschutzbeauftragten.

Bei der Gruppe der nicht meldepflichtigen Unternehmen, die im Rahmen einer Anlaßkontrolle überprüft wurden, ist das Bild noch negativer:

Von 8 überprüften Unternehmen bestand bei 7 die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten. Dieser Pflicht waren 5 Unternehmen nicht nachgekommen.

Das Bundesdatenschutzgesetz mißt der Eigenverantwortung der nicht-öffentlichen Stellen für die Beachtung datenschutzrechtlicher Vorschriften eine hohe Bedeutung zu. Um dieser Eigenverantwortung gerecht zu werden, muß ab einer bestimmten Betriebsgröße ein Datenschutzbeauftragter bestellt werden. Die im November letzten Jahres in Kraft getretene europäische Richtlinie zum Datenschutz bestätigt die Bedeutung der Einrichtung des betrieblichen Datenschutzbeauftragten, indem sie akzeptiert, daß die Bestellung zur Ablösung sehr umfangreicher Meldepflichten gegenüber der Aufsichtsbehörde führen kann. Auch im Hinblick auf die hier zu erwartenden Anpassungen des deutschen Datenschutzrechts halten die Datenschutzaufsichtsbehörden eine verstärkte Beobachtung der Erfüllung der Bestellungspflicht nach § 36 BDSG für notwendig.

Wie weiter unten ausgeführt wird (vgl. Ziff.15), ist im Berichtszeitraum nur in einem Fall ein Ordnungswidrigkeitenverfahren wegen Nichtbestellung eines Datenschutzbeauftragten eingeleitet worden. Dies ist darauf zurückzuführen, daß die Forderung der Aufsichtsbehörde die Bestellung vorzunehmen, lediglich von einem der geprüften Unternehmen nicht unmittelbar erfüllt wurde. Ob der in diesen Fällen Bestellte die erforderlichen Qualifikationen tatsächlich besaß oder zumindest in überschaubarer Frist erworben hat und ob er eine Tätigkeit in dem notwendigen Umfang entfaltet, kann die Aufsichtsbehörde nicht immer nachprüfen. Zumindest wird jedoch die Vorlage von Fortbildungsnachweisen innerhalb angemessener Frist von der Aufsichtsbehörde verlangt.

### **13.2 Inkompatibilität von Datenschutzbeauftragtem und Geldwäschebeauftragtem**

Im Rahmen der Überprüfung der Geeignetheit eines betrieblichen Datenschutzbeauftragten wurde festgestellt, daß die Position des Datenschutzbeauftragten und des Geldwäschebeauftragten nach § 14 Abs. 2 Ziff.1 Geldwäschegesetz vom 25. Oktober 1993 in einer Person vereint waren.

Das Zusammentreffen beider Funktionen ist unter bestimmten Voraussetzungen jedoch nicht zulässig.

Nach § 36 Abs.2 BDSG darf zum betrieblichen Datenschutzbeauftragten nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. An der erforderlichen Zuverlässigkeit fehlt es jedoch, wenn der Datenschutzbeauftragte auch andere Aufgaben zu erfüllen hat, die mit seiner Kontrollfunktion nach dem BDSG nicht zu vereinbaren sind und die ihn deshalb in Interessenkonflikte bringen könnten. Der Geldwäschebeauftragte, der von den in § 14 Abs.1 Geldwäschegesetz genannten Unternehmen und Personen zu bestimmen ist, hat nach Abs. 2 dieser Vorschrift eine leitende Person zu sein, die Ansprechpartner für die Strafverfolgungsbehörden bei der Verfolgung der Geldwäsche nach § 261 StGB ist. Weitere Ausführungen zu dieser Person macht das Geldwäschegesetz nicht. In der Verlautbarung des Bundesaufsichtsamtes für das Kreditwesen über Maßnahmen der Kreditinstitute zur Bekämpfung und Verhinderung der Geldwäsche vom 15. Oktober 1993 werden dazu jedoch folgende Ausführungen gemacht:

"Die "leitende Person" muß mit sämtlichen Angelegenheiten zur Einhaltung des Geldwäschegesetzes innerhalb des Kreditinstitutes befaßt sein. Sie soll auch für den Kontakt zum Bundesaufsichtsamte für das Kreditwesen zuständig sein... Leitende Personen müssen zur Wahrnehmung ihrer Tätigkeit berechtigt sein, für alle Angelegenheiten im Zusammenhang mit der Verhinderung der Geldwäsche unternehmensintern Weisungen zu erteilen... Mit der Funktion der "leitenden Person" dürfen nicht Mitarbeiter der Innenrevision betraut werden, da der "leitenden Person" vor allem bei der Erstattung von Verdachtsanzeigen nach § 11 Geldwäschegesetz Handlungspflichten zugewiesen sind und die Innenrevision grundsätzlich nicht ihre eigene Tätigkeit überprüfen soll."

Der Geldwäschebeauftragte ist damit eine Person, die, falls sie selbst über die Erstattung der Verdachtsanzeigen nach dem Geldwäschegesetz entschei-

det und dementsprechend auch sämtliche Informationen über Verdachtsfälle in ihrem Bereich erhält, in einem sehr sensiblen Bereich verantwortlich für die Speicherung und Übermittlung von personenbezogenen Daten ist. Die Verlautbarung des Bundesaufsichtsamtes für das Kreditwesen geht deswegen zu Recht davon aus, daß Mitarbeiter der Innenrevision nicht zum Geldwäschebeauftragten bestimmt werden dürfen, da ansonsten Handelnder und Kontrollierender identisch wären. Aus den gleichen Gründen muß auch eine Funktionsverbindung von Geldwäschebeauftragtem und Datenschutzbeauftragtem dann für unzulässig angesehen werden, wenn der Geldwäschebeauftragte selbst über die Weiterleitung der Verdachtsfälle an die zuständigen Strafverfolgungsbehörden entscheidet und sie in Gang setzt.

## **14. Datensicherheit**

### **14.1 Einsatz von Personalcomputern (PC)**

Bereits seit mehreren Berichtsperioden spielt die Datensicherheit beim Einsatz von Arbeitsplatzrechnern (PC) eine immer größere Rolle. Auch in diesem Berichtszeitraum konnte festgestellt werden, daß hier deutliche Mängel vorhanden sind. Sehr zögerlich werden die ersten Richtlinien zum Einsatz und zu Sicherheitsmaßnahmen erstellt. Lediglich in größeren Unternehmen gibt es hier hervorhebenswerte Beispiele.

Auch die Dokumentation der Datenverarbeitung weist beim Arbeitsplatzrechner große Mängel auf bzw. ist gar nicht vorhanden. Demgegenüber verlangt Ziff. 7 der Anlage zu § 9 BDSG, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit vom wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle). Zumindest bei personenbezogenen Daten in sensibleren Bereichen muß auch bei Arbeitsplatzrechnern darauf bestanden werden, daß diese Forderung eingehalten wird, wobei klar ist, daß der Gesetzgeber bei Schaffung dieser Vorschrift die Möglichkeiten der individuellen Datenverarbeitung per PC noch nicht kannte. Dieser Dokumentationspflicht kann auf verschiedene Weise manuell z.B. durch Abzeichnung der erfaßten Dokumente oder automatisiert entsprochen werden.

Grundsätzlich sollte in jedem Unternehmen eine genaue, aktuelle Übersicht über alle installierten Datenverarbeitungsgeräte vorliegen. § 37 Abs. 2 BDSG, der zum Inhalt einer solchen Übersicht genauere Angaben macht, spricht von einer solchen Verpflichtung zwar nur in bezug auf den Datenschutzbeauftragten. Sinnvoll ist aber ein Geräte- und Dateienkataster sicher auch in Unternehmen, die keinen Datenschutzbeauftragten bestellen müssen. Hierzu gehören aktuelle Verzeichnisse der installierten Software und der Netzzugehörigkeit (intern wie auch extern). Daneben ist festzulegen, welche Mitarbeiter mit welchen Funktionen an welchen Geräten tätig sind. Es muß nachvollziehbar sein, welche individuellen Dateien auf dem Gerät gehalten werden bzw. welche Zugriffe für den jeweiligen Aufgabenbereich erforderlich und erlaubt sind.

Im Rahmen von allgemeinen Regelungen zur PC-Nutzung ist es sinnvoll festzulegen, wer verantwortlich für den Sicherheitszustand des Geräts ist, wenn mehrere Mitarbeiter an einem Gerät tätig sind. Zu regeln ist weiterhin die Nutzung und Aufbewahrung interner und externer Datenträger, wozu eine ordentliche Katalogisierung und Erstellung von Sicherungskopien sowie deren Aufbewahrung zählt.

### **14.2 Die digital gespeicherte Unterschrift**

Ein Unternehmen, dessen Geschäftszweck Beförderung und Zustellung von Paketen weltweit ist, hatte bereits 1994 ein neues elektronisches Verfahren der Überwachung der Zustellvorgänge eingeführt. Zum Nachweis der Zustellung der ausgelieferten Pakete wurde ein spezielles Gerät entwickelt, das der Zusteller mit den gespeicherten aktuellen Auftragsdaten des Tages versehen mit sich führt. Auf dem Gerät ist ein Schreibfeld angebracht, auf dem der Empfänger einer Sendung den Erhalt mit Hilfe eines Spezialstiftes quittiert. Die Unterschrift wird als Graphik zunächst im Gerät gespeichert und bei Einkoppelung des Geräts in die dafür vorgesehene Bucht im Zustellfahrzeug zusammen mit einem Teil der anderen zum Auftrag gespeicherten Daten drahtlos in den Zentralrechner des Unternehmens übertragen.



Betroffene in ganz Deutschland wandten sich an die Aufsichtsbehörden, da sie dem neuen Verfahren der elektronisch erfaßten Unterschrift mißtrauisch gegenüberstanden und besorgt waren, ob so ihre Unterschrift nicht mißbräuchlich verwendet werden könnte.

Da das Unternehmen seinen Hauptsitz in Hessen hat, hatte sich die zuständige hessische Aufsichtsbehörde mit der Problematik zu befassen. Die Überprüfung, die sich aufgrund der Schwierigkeit, die dem deutschen Unternehmen bis dahin nicht bekannten amerikanischen Verfahrensdokumentationen zu beschaffen, langwierig gestaltete, führte zu dem Ergebnis, daß gegen eine mißbräuchliche Verwendung der elektronisch erfaßten Unterschrift ausreichende Sicherheiten im Verfahren vorhanden sind. Dabei war zu erkennen, daß die elektronisch gespeicherte Unterschrift nach den vorgelegten Dokumentationen und nach der praktischen Überprüfung der Arbeitsweise zumindest bis zur Speicherung im Rechenzentrum nicht isoliert, d.h. von den anderen Daten getrennt verarbeitbar ist. Der Weg bis zum Rechenzentrum genügt mit den Sicherheiten, die das genutzte Funkverfahren bietet, den Datenschutzanforderungen. Zu berücksichtigen war dabei, daß es sich bis auf die Unterschrift nicht um besonders sensible Daten handelte. Die Unterschrift ist in einzelne große Bildpunkte zerlegt gespeichert und bereits von daher kaum mit einer original auf Papier geleisteten Unterschrift zu verwechseln. Mit hochwertigen Scannern und einer entsprechenden Auflösung bei Erfassung und Speicherung kann heute auch eine normal z.B. auf einem beliebigen Dokument gegebene Unterschrift isoliert und - mißbräuchlich - verwendet werden.

In diesem Prüfungsverfahren wurde allerdings deutlich, wie begrenzt die Möglichkeiten der Aufsichtsbehörden bei solcherart hochkomplexen Datenverarbeitungssystemen sind. Die komplette bis ins Einzelne gehende Überprüfung sämtlicher Dokumentationen, die zum überwiegenden Teil nur in englischer Sprache vorgelegt werden konnten, hätte die Kapazitäten der Aufsichtsbehörde bei weitem überschritten. Insofern mußte die Überprüfung auf ein Stichprobenverfahren beschränkt werden, und das Ergebnis kann natürlich in keiner Weise als irgendwie geartete Unbedenklichkeitsbescheinigung verstanden werden.

### 14.3 Der PC als Heimarbeitsplatz

Insbesondere im Bereich der Datenerfassung wird in zunehmendem Maße von den Aufsichtsbehörden eine Verlagerung in Heimarbeitsplätze beobachtet. Hier geben gemeldete Unternehmen ihre Aufträge im Rahmen von Dienst- oder Werkverträgen weiter. Mit Blick auf die Datensicherheit hält eine solche Arbeitsweise besondere Probleme bereit.

Zu fordern ist eine geregelte und dokumentierte An- und Ablieferung der zu erfassenden Daten bzw. der Datenträger nach Erfassung. Bei Online-Verbindung müssen Sicherheitseinrichtungen vorhanden sein, die verhindern, daß sich Unbefugte über diesen Weg in die Verarbeitung personenbezogener Daten einklinken können.

Der Arbeitsplatz in der Wohnung sollte in einem separaten, abschließbaren Raum liegen.

Schließlich ist darauf hinzuweisen, daß - obwohl es sich in den meisten Fällen nicht um Arbeitnehmer des Betriebs im arbeitsrechtlichen Sinn handelt - diese Arbeitsplätze im Rahmen der Organisationskontrolle auch der Kontrolle durch den betrieblichen Datenschutzbeauftragten des "Mutter"-Unternehmens unterliegen sollten. Bei Prüfungen der Aufsichtsbehörde konnte erst in einem Fall festgestellt werden, daß eine derartige Kontrolle auch tatsächlich durchgeführt worden war.

### 15. Ordnungswidrigkeitenverfahren

Von den bereits in den letzten Berichten der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden erwähnten Bußgeldverfahren konnten im Berichtsjahr 1995 drei Verfahren gegen einen Adreßverlag mit einer Bußgeldsumme in Höhe von 5000,- DM rechtskräftig abgeschlossen werden. 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 1995 wurden von der Aufsichtsbehörde gegen 7 Unternehmen Ordnungswidrigkeitenverfahren nach dem BDSG eingeleitet. So hat die Aufsichtsbehörde gegen 4 Unternehmen Ordnungswidrigkeitenverfahren wegen der nicht erfolgten Erteilung von Auskünften entgegen § 38 Abs. 3 Satz 1 BDSG eingeleitet (Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 6, 1. Alternative BDSG). In zwei Fällen wurden Ordnungswidrigkeitenverfahren wegen der entgegen § 33 Abs. 1 BDSG unvollständigen bzw. unterlassenen Benachrichtigung von Betroffenen eingeleitet (Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 3 BDSG).

Bei einem weiteren Unternehmen hat die Aufsichtsbehörde wegen der verspäteten Abgabe der nach § 32 Abs. 1 BDSG erforderlichen Mitteilung über die Aufnahme einer meldepflichtigen geschäftsmäßigen Datenverarbeitungstätigkeit ein Ordnungswidrigkeitenverfahren nach § 44 Abs. 1 Nr. 2 BDSG eingeleitet. Das Unternehmen hatte - ohne seiner Meldepflicht nachgekommen zu sein - bereits mehrere Jahre lang personenbezogene Daten geschäftsmäßig zum Zwecke der anonymisierten Übermittlung im Bereich der Markt- und Meinungsforschung gespeichert.

In den sieben neu eingeleiteten Verfahren hat die Aufsichtsbehörde im Berichtsjahr drei Bußgeldbescheide mit einer Bußgeldsumme in Höhe von 10.250,-- DM erlassen. Zwei dieser Bußgeldbescheide haben im Berichtsjahr Rechtskraft erlangt.

Wiesbaden, den 27. Juni 1996

Der Hessische Ministerpräsident  
Eichel

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