

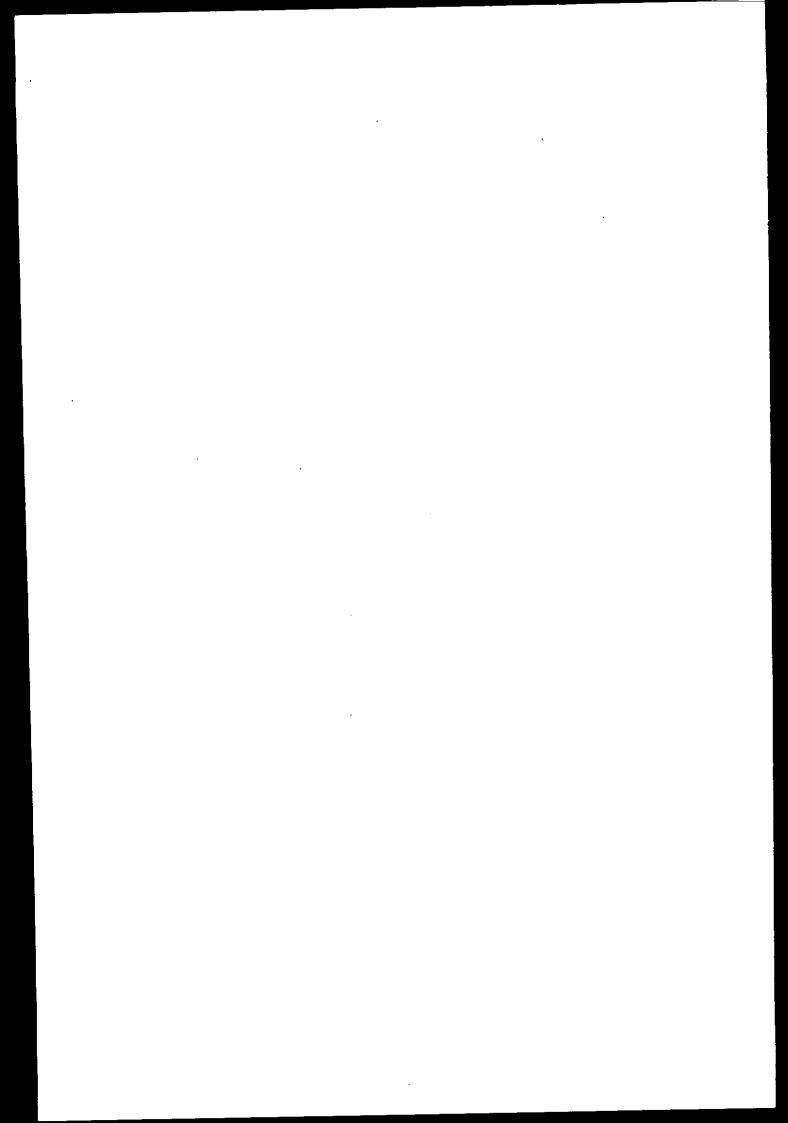
# HESSISCHER LANDTAG

15.07.94

Vorlage der Landesregierung

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

Vorgelegt mit der Stellungnahme zum Zweiundzwanzigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten - Drucks. 13/5813 - nach § 30 Abs. 2 des Hessischen Datenschutzgesetzes vom 11. November 1986.



#### Inhaltsverzeichnis

	B	Seite
1.	Bearbeitung von Beschwerden gegen Stellen, die personenbezogene Daten nach § 28 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) für die Erfüllung eigener Geschäftszwecke verarbeiten	
2.	schäftszwecke verarbeiten  Bearbeitung von Beschwerden gegen Stellen, die personenbezogene Daten nach § 32 Abs. 1 Nr. 1 bis 3 BDSG	5
	geschäftsmäßig verarbeiten oder nutzen	5
3.	Bearbeitung von Anfragen zu Problemen des Daten- schutzes	6
4.	Von Amts wegen durchgeführte Überprüfungen von Stellen, die nach § 32 Abs. 1 Nr. 1 bis 3 BDSG geschäftsmäßig personenbezogene Daten verarbeiten oder nutzen	
4.1	Register	6 6
4.2	Prüfungsübersicht	6
4.3	Registermeldungen über regelmäßige Übermittlungsempfänger	
5.	Wirtschaftsauskunfteien	7
5.1	Allgemeines und Entwicklung der Branche	7
5.2	Dokumentation der Quellen	7
5.3	Benachrichtigung nach § 33 BDSG	7
5.4	Ehegattendaten	8
5.5	Angabe des berechtigten Interesses	8
5.6	Aktualität der Online-Auskünfte	8
5.7	Der angebliche Hackgreinbruck	8
5.8	Der angebliche Hackereinbruch	9
6.	SCHUFA	9
7.	Kreditkartenunternehmen	10
8.	Kreditkartenunternehmen	11
8.1	Versicherungen Widerspruchsrecht gegen die Datenübermittlung zu Werbezwecken	11
8.2	Übermittlung von Arbeitnehmerdaten zu Werbezwecken	11
8.3	Datenverarbeitungsklauseln	12
9.	Datenverarbeitung im medizinischen Bereich	12
9.1	Krankenversichertenkarte - Einsatz der Kartentechnik im medizinischen Bereich	12
9.2	Unzulässige Übermittlung an Orthopädiegeschäft	12
10.	Arbeitnehmerdatenschutz	13
10.1	Bewerberdaten	14
10.2	Verarbeitung von Arbeitnehmerdaten für die Betriebsrats- wahl	14
11.	Auslandsdatenverarbeitung	14
11.1	Grundsätze der Aufsichtsbehörden	15
11.2	Grenzüberschreitende Direktwerbung	15
13.	Werbewirtschaft	17
13.1	Unzulässige listenmäßige Übermittlung personenberges	18
13.2	Widerspruchsrecht gegen die Nutzung oder Übermittlung	18
13.3	Nichtheachtung von Dotterer	19
14.	Datenschutz im Telefonverkehr - Erfassung und Speicherung von Verbindungsdaten durch	20
15	Invate	21
15.	Vereinsdatenverarbeitung	21

Drucksache 13/6385

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

Im Berichtsjahr gingen bei der Aufsichtsbehörde 104 Beschwerden gegen Stellen, die Datenverarbeitung für die Erfüllung eigener Geschäftszwecke betreiben, ein. Alle Beschwerden führten zu einer Überprüfung durch die Aufsichtsbehörde.

# Die Beschwerden betrafen

- Versicherungen in 14 Fällen,
- den Einzelhandel in 12 Fällen,
- Kreditkartenunternehmen in 10 Fällen,
- Kreditinstitute in 10 Fällen,
- das Gesundheitswesen (Ärzte, Krankenhäuser, Apotheken) in 6 Fällen,
- Vereine in 5 Fällen,
- den Versandhandel in 4 Fällen,
- Verlage in 4 Fällen,
- Chemieunternehmen in 4 Fällen,
- Reiseveranstalter in 3 Fällen.
- Inkassounternehmen in 3 Fällen,
- Anbieter von Fort- und Weiterbildung in 3 Fällen,
- Fluglinien in 2 Fällen,
- sonstige Unternehmen in 24 Fällen.

In 32 Fällen waren die Beschwerden begründet, davon in fünf Fällen gegen Kreditkartenunternehmen, in drei Fällen gegen den Einzelhandel, in je zwei Fällen gegen Versicherungen, Kreditinstitute, das Gesundheitswesen, Vereine, Inkassounternehmen sowie Anbieter von Fort- und Weiterbildung. In je einem Fall waren Beschwerden gegen den Versandhandel und Verlage begründet, zehn weitere begründete Beschwerden richteten sich gegen sonstige Unternehmen.

Bei zwei Beschwerden konnte nicht abschließend festgestellt werden, ob die Datenverarbeitung im zulässiger oder in unzulässiger Weise erfolgt war. In 30 Fällen sind die Ermittlungen der Aufsichtsbehörde noch nicht abgeschlossen.

Im Berichtsjahr wurden außerdem 16 bereits in den Vorjahren eingereichte Beschwerden abgeschlossen. Die Beurteilung der Aufsichtsbehörde ergab hier, daß sechs Beschwerden begründet waren. Dabei hatten in zwei Fällen Versicherungen und in je einem Fall ein Verkehrsverbund, ein Verein, eine Tankstelle und ein Arbeitgeber, der auf dem Gebiet des Personenschutzes tätig ist, personenbezogene Daten unzulässig verarbeitet oder genutzt.

Damit ist der Anteil der begründeten Beschwerden im Vergleich zu den Vorjahren erheblich angestiegen.

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

Im Berichtsjahr gingen bei der Aufsichtsbehörde 45 Beschwerden gegen Stellen, die personenbezogene Daten geschäftsmäßig verarbeiten oder nutzen, ein. Diese richteten sich fast ausschließlich gegen Kreditinformationsdienste. Alle Beschwerden führten zu einer Überprüfung durch die Aufsichtsbehörde.

#### Die Beschwerden betrafen:

- Kreditinformationsdienste (Wirtschaftsauskunfteien und SCHUFA) in 43 Fällen,
- einen Adreßverlag in einem Fall und
- einen Dienstleistungsverarbeiter in einem Fall.

Von den Beschwerden gegen Kreditinformationsdienste richteten sich 21 gegen eine einzige Wirtschaftsauskunftei, die ihren Betrieb jedoch zwischenzeitlich eingestellt hat (s. unten Ziff. 5.8).

In acht Fällen - alle gegen Kreditinformationsdienste - waren die Beschwerden begründet. Bei einer Beschwerde gegen einen Adreßverlag konnte nicht mehr abschließend festgestellt werden, ob die Datenverarbeitung in zulässiger oder unzulässiger Weise erfolgt war. In 17 Fällen sind die Ermittlungen der Aufsichtsbehörde noch nicht abgeschlossen.

Im Berichtsjahr wurden außerdem drei bereits in den Vorjahren eingegangene Beschwerden abgeschlossen. Dabei stellten sich zwei Beschwerden gegen Wirtschaftsauskunfteien als begründet heraus. Bei einer weiteren Beschwerde gegen eine Wirtschaftsauskunftei konnte nicht mehr abschließend festgestellt werden, ob die Datenverarbeitung in zulässiger oder unzulässiger Weise erfolgt war.

# 3. Bearbeitung von Anfragen zu Problemen des Datenschutzes

Ein Bereich der Tätigkeit der Aufsichtsbehörden, der nur zum Teil schriftlich abgewickelt wird, ist die Beantwortung von Anfragen verschiedenster Art. Das Spektrum reicht hier von der Bitte eines Diplomanden, Auskünfte über die Art und Weise der Prüfungstätigkeit der Aufsichtsbehörde für die Diplomarbeit zu geben, bis zu detaillierten und kenntnisreichen Anfragen zu technischen Entwicklungen wie z.B. dem Telefonbanking mit der Absicht, die Aufsichtsbehörden auf eventuelle datenschutzrechtliche Probleme aufmerksam zu machen bzw. das eigene Mißtrauen von kompetenter Seite bestätigt zu erhalten. Von den schriftlichen Anfragen betrafen die meisten das Thema "Datenschutzbeauftragter" (s. dazu unten Ziff. 15). Einen weiteren Schwerpunkt bildeten die Anfragen von Verbänden und Unternehmen, die beabsichtigte Datenverarbeitungen oder -nutzungen vor ihrer Umsetzung in die Praxis datenschutzrechtlich abklären wollten.

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

#### 4.1 Register

Die Aufsichtsbehörde führt 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, im wesentlichen aus den Branchen Auskunfteien, Adreßhändler, Markt- und Meinungsforschungsunternehmen und Unternehmen, die im Auftrag Datenverarbeitung als Dienstleistung betreiben, unterliegen nach § 32 BDSG der Meldepflicht.

Am 1. Februar 1994 waren zu diesem Register 614 Unternehmen gemeldet.

#### 4.2 Prüfungsübersicht

Im Berichtsjahr wurden 66 Prüfungen nach § 38 Abs. 2 BDSG durchgeführt. Davon betrafen Datenverarbeiter nach § 32 Abs. 1 Ziff. 3 BDSG insgesamt 53, nämlich

- Servicerechenzentren 25
- Konzerndatenverarbeiter 7
- Datenerfasser und Schreibbüros mit Dateiverwaltung 9
- Adreßhändler 2
- Mikroverfilmer 1
- Datenträgervernichter 7
- Telemarketing 2.

Desweiteren wurden 5 Kreditinformationsdienste und 6 Verbände/Vereine und 2 Unternehmen aus dem Bereich der Markt- und Meinungsforschung geprüft.

Die Prüfungen brachten folgendes Ergebnis:

- Beanstandungen 26
- Empfehlungen 17
- ohne wesentliche Beanstandungen 23

Folgende wesentliche Mängel wurden am häufigsten festgestellt:

- Keine bzw. verspätete oder unvollständige Registermeldung nach § 32 BDSG
- 2. Keine oder mangelhafte Zugangskontrolle
- 3. Keine oder mangelhafte Zugriffskontrolle
- 4. Mängel in der Datenträgerkontrolle
- 5 Kein Datenschutzbeauftragter oder Mängel in der Fachkunde
- 6. Fehlende schriftliche Verpflichtung auf das Datengeheimnis (§ 5 BDSG)

Erstaunlich ist, daß immer noch Unternehmen vorgefunden werden, die trotz jahrelangen Betreibens einer meldepflichtigen Tätigkeit keine Kenntnis der datenschutzrechtlichen Meldepflicht haben und auch sonst den Regeln des Datenschutzes eher unwissend gegenüber stehen. Die Aufsichtsbehörden bemühen sich hier, mit Öffentlichkeitsarbeit, aber auch durch Bußgeldverfahren Änderungen herbeizuführen.

Neben den Prüfungen im Bereich der Meldepflicht, die immer im Rahmen einer Betriebsbesichtigung durchgeführt werden, wurden nach § 38 Abs. 1 BDSG in sechs Beschwerdefällen und in zwei Fällen, in denen die Hinweise der Presse entnommen wurden, Überprüfungen "vor Ort" durchgeführt.

# 4.3 Registermeldungen über regelmäßige Übermittlungsempfänger

Seit 1992 wurde größeren Auskunfteien die Möglichkeit eingeräumt, regelmäßige Übermittlungsempfänger nicht mehr unmittelbar nach Vertragsaufnahme mit Namen und Anschrift, sondern nur noch branchenweise zusammengestellt nach der Anzahl und in bestimmten regelmäßigen Zeitabständen dem Register zu melden. Derartige Vereinbarungen im Einzelfall haben sich bewährt. Zu Teil hatten die laufenden Meldungen der Online-Partner sowohl dem meldenden Unternehmen als auch der Aufsichtsbehörde einen Aufwand bereitet, der in keinem Verhältnis zu dem Nutzen für die Öffentlichkeit und für die Aufsichtstätigkeit stand. Es muß allerdings gewährleistet sein, daß die vollständige namentliche Zusammenstellung der Online-Partner dem betrieblichen Datenschutzbeauftragten und der Aufsichtsbehörde jederzeit zugänglich ist.

#### 5. Wirtschaftsauskunfteien

#### 5.1 Allgemeines und Entwicklung der Branche

Im Berichtsjahr wurde überprüft, inwieweit der Aufbau einer zentralen Negativdatei unter Einbeziehung neuer branchenspezifischer Gruppen von Anschlußpartnern weiterverfolgt wurde. Die Aufsichtsbehörde hatte hier, wie im Tätigkeitsbericht fürdas Jahr 1991 dargelegt, schwerwiegende Bedenken erhoben, weil die beabsichtigte Einmeldung und Speicherung von sog. "weichen", das heißt nicht mit Tatsachen belegbaren, Daten in erheblichem Umfang die Gefahr der Speicherung und Übermittlung fehlerhafter Daten in sich barg. Die erneute Überprüfung ergab, daß eine derartige Negativdatei nicht im ursprünglich geplanten Umfang entstanden war und die als besonders problematisch eingestuften Merkmale bisher nicht oder nur in wenigen Ausnahmefällen benutzt worden waren. Das Interesse an einer solchen branchenbezogenen Auskunftstätigkeit hatte sich wohl nicht in dem erwarteten Umfang bestätigt. Die Aufsichtsbehörde wird in diesem Fall aber die weitere Entwicklung beobachten.

#### 5.2 Dokumentation der Quellen

Gegenüber einer Reihe von Forderungen der Aufsichtsbehörden wurde seitens verschiedener Unternehmen grundsätzlich die Bereitschaft zur Kooperation bekundet; jedoch mangelte es öfters an der konkreten Umsetzung im einzelnen. Beispielsweise war die Dokumentation der Quellen zum Teil nach wie vor unbefriedigend, so daß im Beschwerdefall nicht immer eindeutig nachvollzogen werden konnte, woher die Daten stammten.

#### 5.3 Benachrichtigung nach § 33 BDSG

Strittig ist zwischen den Aufsichtsbehörden und verschiedenen Auskunfteien die Formulierung der Benachrichtigungsschreiben nach § 33 Abs. 1 Satz 2 BDSG. Nach dieser Vorschrift ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen. Oft beschränken sich die Auskunfteien in ihrem Benachrichtugnstext jedoch auf Formulierungen wie, daß "vorliegende Informationen", "Daten zu wirtschaftlichen Verhältnissen und ähnliches" oder "Daten, die zur Beurteilung der Bonität erforderlich sind" übermittelt würden. Dies ist nicht ausreichend. Unter "Art der Daten" sind vielmehr Bezeichnungen wie "Adresse, Beruf, Geburtsdatum, finanzielle Verpflichtungen, Immobilien, Vermögensdaten" und ähnliches zu verstehen. Die Argumentation der Auskunfteien, daß damit bereits die Auskunft nach § 34 BDSG vorweggenommen würde, trifft nicht zu, da mit der Bezeichnung der Datenart noch nicht die individuellen zu den einzelnen Datenarten gespeicherten Daten mitgeteilt werden.

#### 5.4 Ehegattendaten

Seit Jahren ist streitig, wann eine Wirtschaftsauskunftei Daten über den Ehegatten des Betroffenen übermitteln darf. Die hessischen Aufsichtsbehörden vertreten hier eine restriktive Linie, die es als rechtswidrig betrachtet, den Ehegatten als "informatorisches Anhängsel" des Partners zu betrachten. Nur wenn sich das berechtigte Interesse des Anfragers auch auf die Person des Ehegatten bezieht, dürfen Aufskünfte zu diesem gegeben werden (vgl. Tätigkeitsbericht für das Jahr 1990, Ziff. 5.4).

Zu dieser Problematik konnte ein gemeinsamer Standpunkt zwischen den Auskunfteien in Hessen und den Aufsichtsbehörden nicht gefunden werden, da sich die betroffenen Auskunfteien nicht in Gegensatz zu anderen Auskunfteien bzw. zu ihrer Zentrale setzen wollten. Zwischenzeitlich besteht jedoch eine gewisse Erwartung, daß ein Konsens in Gesprächen zwischen dem Arbeitskreis Wirtschaftsauskunfteien der oberste Aufsichtsbehörden für den Datenschutz und den Verbänden gefunden wird.

# 5.5 Angabe des berechtigten Interesses

Erfreulicherweise konnte ein Entgegenkommen einer bundesweit vertretenen Auskunftei in bezug auf die Darlegung des berechtigten Interesses für die Anfrage seitens des Anfragers festgestellt werden. Die Wirtschaftsauskunftei hatte jahrelang Anfrageformulare verwendet, bei denen die Möglichkeit bestand, überhaupt kein "berechtigtes Interesse" anzugeben. Die Auskunftei nahm in diesen Fällen stets eine Kreditentscheidung als "berechtigtes Interesse" an und beantwortete die Anfrage (s. Tätigkeitsbericht für 1992). Dies war von den Aufsichtsbehörden beanstandet worden. Die Wirtschaftsauskunftei hat nun die Formulare so umgestaltet, daß ein spezifisches berechtigtes Interesse in jedem Fall angekreuzt werden muß. Findet sich unter den vorgegebenen häufig vorkommenden Einzelrubriken nicht die passende Angabe, so muß der Anfrager den Anfragegrund mit eigenen Worten darstellen.

#### 5.6 Aktualiät der Online-Auskünfte

Bei mehreren Wirtschaftsauskunfteien bestehen Probleme bei der Aktualiät und damit Richtigkeit der zu Unternehmen und deren Verantwortlichen gespeicherten Daten insoweit, als die Auskunfteien aus Kapazitätsgründen Änderungen der Daten tagsüber nur erfassen und sie erst am darauffolgenden Tag nach einem nächtlichen Update der Online-Datenbank für Auskunftszwecke zur Verfügung stellen.

Bei einem Unternehmen werden die Veränderungsdaten zwar in der dezentralen Datenbank sofort gespeichert, in die zentrale Online-Datenbank jedoch erst mit dem nächtlichen Update übernommen. Im Einzelfall führt diese Arbeitsweise dazu, daß der Online-Anfrager einen ganzen Tag lang falsche oder unvollständige Daten erhält. Dies ist datenschutzrechtlich nicht akzeptabel.

Ein sofortiges Update aller Datenbestände setzt mit allen erforderlichen Sicherungen eine erheblich verstärkte Rechnerleistung und umfangreiche Softwareänderungen voraus. Unter Berücksichtigung der damit einhergehenden finanziellen Auswirkungen hat die Aufsichtsbehörde vorgeschlagen, zumindest diejenigen Nummern von Betroffenen zentral abzuspeichern, für die eine aktuelle Veränderung vorliegt. Im Falle einer Online-Auskunft könnte dieses Veränderungsregister einen Stop auslösen und den Anfrager auf die Notwendigkeit der Einholung der aktualisierten Auskunft hinweisen. Dem ist bisher lediglich ein Unternehmen gefolgt.

# 5.7 Der angebliche Hackereinbruch

Ein Wochenmagazin hatte gelmeldet, daß Hackern der Zugriff zu sensiblen Unternehmensdaten, darunter auch personenbezogenen Daten, bei zwei bundesweit arbeitenden Wirtschaftsauskunfteien gelungen sei. Daraufhin schaltete sich die zuständige Aufsichtsbehörde in die bereits bei dem betroffenen Unternehmen mit Sitz in Hessen eingeleiteten Ermittlungen ein. Zunächst wurde nicht offenbart, wann der angebliche Hackereinbruch stattgefunden haben sollte, so daß sich die Überprüfungen durch das Unternehmen und entsprechend durch die Aufsichtsbehörde sehr aufwendig gestalteten. Unregelmäßigkeiten im Ablauf der Online-Auskunftstätigkeit, die hier nur betroffen sein konnte, konnten jedoch nicht festgestellt werden. Schließlich stellt sich heraus, daß aus alten Geschäftsunterlagen eines Online-Kunden dieser Auskunftei wohl durch einen Mitarbeiter dieses Unternehmens alte damals auf korrekte Anfrage erteilte Firmenauskünfte mißbraucht und - etwas aufbereitet - als aktueller Hackererfolg präsentiert worden waren. Vermutlich hätte eine genauere Überprüfung der als "Originalausdrucke" dem Magazin vorgelegten Unterlagen die Plumpheit der Fälschung aufzeigen können. Ob der durch die betroffene Wirtschaftsauskunftei gestellte Strafantrag Erfolg hatte, ist nicht bekannt.

Aus diesem Fall muß allerdings insofern eine Lehre gezogen werden, als Unterlagen mit personenbezogenen Daten in jedem Fall besser vor eventuell unbefugten Zugriff geschützt werden sollten. Die Pflicht, entsprechende technische und organisatorische Maßnahmen zu treffen (§ 9 BDSG) gilt auch für Dateienausdrucke, die personenbezogene Daten enthalten und z.B. in Geschäftsakten aufbewahrt werden.

# 5.8 Ein herausragend negativer Fall

Ein erheblichen Anteil an den Beschwerde- und Anfragezahlen in den vergangenen Jahren ist auf die Tätigkeit einer einzigen Auskunftei bzw. einem Nachfolgeunternehmen zurückzuführen. Die Geschäftstätigkeit beider Unternehmen bestand darin, für Versandhäuser Informationen über Besteller einzuholen und diese Erkenntnisse zu übermitteln. Ende 1993 wurde die Geschäftstätigkeit eingestellt und die Eröffnung des Konkursverfahrens beantragt.

Anläßlich einer Regelüberprüfung, bei der zurückliegende Auskunftsvorgänge im einzelnen überprüft wurden, stellte sich heraus, daß als Herkunft der Daten unter anderem auch Briefzusteller der Deutschen Bundespost-Postdienst - verzeichnet waren. Insbesondere in den neuen Bundesländern wurden durch Rechercheure gerne die Briefzusteller über die persönlichen Verhältnisse der Betroffenen, z.B. zur beruflichen Tätigkeit oder zu Grundbesitz, befragt. Die Briefzusteller sind jedoch nicht berechtigt, Wirtschaftsauskunfteien Auskünfte über die in ihrem Zustellbezirk ansässigen Personen zu erteilen. Eine solche Datenerhebung ist nicht auf rechtmäßige Weise erfolgt und widerspricht § 28 Abs.1 BDSG. Zudem stellte die Aufsichtsbehörde mit Hilfe der von Beschwerdeführern gegebenen Informationen fest, daß ein Gutteil der von den Briefzustellern gegebenen Informationen nicht den tatsächlichen Verhältnissen entsprach. Das gleiche galt für das auch in größerem Umfang von der Auskunftei praktizierte Verfahren, bei Nachbarn Informationen einzuholen.

Aufgrund einiger Beschwerden besteht im übrigen der Verdacht, daß Mitarbeiter der Auskunftei unter der Angabe, von einer Behörde. z.B. der Bundesversicherungsanstalt für Angestellte, anzurufen, Betroffene zur

Angabe von personenbezogenen Daten veranlaßten. So gaben Beschwerdeführer übereinstimmend an, daß sie einige Zeit vor Erhalt der Benachrichtigung nach § 33 BDSG durch die Auskunftei von einer angeblichen Mitarbeiterin der BfA angerufen worden seien. Die Anruferin habe mitgeteilt, daß die Computeranlage ausgefallen sei und man deswegen über diesen Weg Daten zu Geburtstag und derzeitigem Arbeitgeber nachfragen wolle. Solche Anrufe wurden auch von Betroffenen registriert, die in keinem Bezug zur BfA standen bzw. die durch Rückruf bei der angegebenen Behörde feststellten, daß von dort eine solche Anfrage jedenfalls nicht durchgeführt worden war.

Es liegt auf der Hand, daß solche Erhebungsmethoden unzulässig sind.

In nahezu allen Beschwerdefällen ergab die Nachprüfung, daß gespeicherte und übermittelte Daten unrichtig waren. Zum Teil waren z.B. zur beruflichen Tätigkeit sehr detaillierte Angaben gespeichert - so war bei einer Pädagogin übermittelt worden, sie sei Kassenmitarbeiterin bei der Städtischen Sparkasse -, die zu keinem Zeitpunkt, auch nicht für die Vergangenheit, zutreffend gewesen waren. Insbesondere bei den Daten zur Berufstätigkeit entstand hier der Eindruck, daß es sich um eigene Erfindungen des jeweiligen Rechercheurs handelte.

Übermittelt wurde von der Auskunftei auch eine Beurteilung der Finanzlage der Betroffenen, die entweder als "geordnet" oder als "beengt" bezeichnet wurde. Bei "beengter" Finanzlage wurde dem anfragenden Versandhaus von einer Geschäftsverbindung abgeraten. Waren die Finanzverhältnisse "geordnet", so wurde nach nicht nachvollziehbaren Kriterien entweder die Geschäftsverbindung als "zulässig" erachtet oder zur Absicherung einer eventuellen Kreditvergabe geraten. So bewertete die Auskunftei bei einem arbeitslosen Besteller, dessen Ehefrau als Hausfrau tätig war, die Kreditvergabe über DM 3000, - als "nicht zulässig"; in einem vergleichbaren Fall, in dem es um einen gleich hohen Kredit ging, wurde die Geschäftsverbindung als zulässig erachtet, obwohl die Betroffenen noch für ein Kind unterhaltspflichtig waren. Konnte die Auskunftei nichts über die wirtschaftlichen Verhältnisse ermitteln, so wurden sie als "schwer einsehbar" bezeichnet und stets zur Absicherung der Forderung geraten. Damit wurden Daten übermittelt, die im allgemeinen Sprachgebrauch eine - tatsächlich nicht begründete - Negativbewertung enthielten.

Wie jede Wirtschaftsauskunftei war die betroffene Auskunftei verpflichtet, die Betroffenen, deren personenbezogene Daten sie gespeichert und an Dritte übermittelt hatte, von der erstmaligen Übermittlung und der Art der übermittelten Daten in Kenntnis zu setzen. Diese Pflicht wurde nur sporadisch und auf Betreiben der Aufsichtsbehörde hin erfüllt. So sind schätzungsweise mindestens in 36.000 Fällen Betroffene nicht benachrichtigt worden. Wurden Benachrichtugngen versandt, so zeigte sich dies durch einen sprunghaften Anstieg der Beschwerdezahlen bei der Aufsichtsbehörde. Die Betroffenen mißtrauten dem in Stil und Gestaltung unfreundlich und undurchsichtig erscheinenden Benachrichtigungsschreiben. Auch der Inhalt der Schreiben genügte erst nach mehrmaligen Hinweisen der Aufsichtsbehörde den gesetzlichen Anforderungen. Dem gesetzlichen Auskunftsrecht der Betroffenen wurde sehr oft nur mit Verzögerung oder unvollständig Genüge getan.

Problematisch ist die gegenwärtige Situation. Nach Einstellung der Geschäftstätigkeit erklärte sich das Unternehmen außerstande, seinen Pflichten aus dem Bundesdatenschutzgesetz gegenüber Betroffenen und Aufsichtsbehörde noch nachzukommen. Nach Ansicht der Aufsichtsbehörde erlöschen jedoch diese Pflichten nach Auflösung der die Auskunftei betreibenden Gesellschaft nicht einfach, sondern sind - notfalls durch Liquidatoren - weiter zu erfüllen, solange noch Daten gespeichert sind bzw. notwendige Benachrichtigungen noch nicht durchgeführt wurden.

#### 6. SCHUFA

Im Berichtszeitraum wurden relativ wenige Beschwerden an die Aufsichtsbehörde herangetragen, die die Tätigkeit der SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung) betrafen, obgleich die Speicherung und Übermittlung von personenbezogenen Daten zur Kreditwürdigkeit als Massengeschäft abgewickelt wird.

Im Rahmen der Meldung von Negativdaten durch die Vertragspartner erweist es sich für die Betroffenen immer wieder als problematisch, wenn nicht, wie in jedem Einzelfall erforderlich, das Meldeinteresse der SCHU-FA mit den Betroffeneninteressen sorgfältig abgewogen wird.

So wurde beispielsweise das Interesse von Betroffenen nicht ausreichend berücksichtigt, bei denen die Beantragung eines Mahnbescheids gemeldet wurde, ohne daß in diesen Einzelfällen das Merkmal der Zahlungsunfähigkeit bzw. Zahlungsunwilligkeit ohne weiteres bejaht werden konnte.

Auf behördliches Betreiben wurde in diesen Fällen eine nachträgliche Interessenabwägung zugunsten der Betroffenen vorgenommen.

Positiv anzumerken ist, daß die SCHUFA im Berichtsjahr unverzüglich auf die vorgetragenen Beschwerden reagierte, so daß teilweise sogar telefonisch Abhilfe für die Betroffenen geschaffen werden konnte, wenn die Aufsichtsbehörde den Sachverhalt und die datenschutzrechtliche Bewertung unterbreitete.

#### 7. Kreditkartenunternehmen

Im Berichtszeitraum gingen wiederholt Beschwerden darüber ein, daß ehemalige Kreditkarteninhaber noch lange Zeit nach Schliessung ihres Kartenkontos von den Kreditkartenunternehmen mit Forderungen belastet wurden, die erst nach Beendigung des Kreditkartenvertrages entstanden waren. In einem Fall lagen 4 Jahre zwischen der Schließung des Kartenkontos und der Forderungsentstehung.

Eine Ursache für diese Vorfälle lag darin, daß Vertragsunternehmen im Rahmen längerfristiger Geschäftsverbindungen auf die Fortgeltung der anfänglich einmal erteilten Einwilligung in die Datenübermittlung an die Kreditkartenunternehmen vertrauten oder daß anderslautende Verfügungen des Kunden versehentlich nicht berücksichtigt wurden.

Auf diese Weise wurden den Kreditkartenunternehmen weiterhin Forderungen zur Begleichung vorgelegt. Diese wiederum zogen die Beträge per Lastschrift bei den ehemaligen Kreditkarteninhabern ein, ohne eine neuerliche Einwilligung in die Verarbeitung und Nutzung der Daten einzuholen. Begründet wurde dies damit, daß solche Belastungen üblicherweise noch längere Zeit nach Vertragsbeendigung über das Kartenkonto abgewickelt würden, was zum Teil auf verspätete Forderungseinreichungen der Vertragsunternehmen, insbesondere bei Auslandsbelastungen, zurückgehe. In einem Fall war ein vorhandener Sperrvermerk übersehen worden. Die Aufsichtsbehörde hielt in diesen Fällen eine Verarbeitung und Nutzung der Daten von ehemaligen Karteninhabern ohne erneute Einwilligung nur für zulässig, wenn die Forderung vor Schließung des Kartenkontos entstanden war und die nachträgliche Belastung des Karteninhabers innerhalb 6 Monaten nach Kontoschließung erfolgte. Diese Frist ist bei entsprechenden Vorgaben an die Vertragsunternehmen auch bei der Abwicklung von Auslandsbelastungen zumutbar. Mit Beendigung des Kreditkartenverhältnisses erlangt der ehemalige Karteninhaber ein schutzwürdiges Interesse daran, daß seine Daten nicht unbegrenzt weiterverarbeitet werden. Nach einem bestimmten angemessenen Zeitraum muß er davon ausgehen können, daß keine Daten mehr verarbeitet oder genutzt werden. Nach Ablauf dieser Frist überwiegt sein schutzwürdiges Interesse am Ausschluß der Verarbeitung und Nutzung, so daß für spätere Abrechnungsvorgänge eine erneute Einwilligung erforderlich ist.

#### Versicherungen

# 8.1 Widerspruchsrecht gegen die Datenübermittlung zu Werbezwecken

Der Aufsichtsbehörde wurde eine Beschwerde gegen die listenmäßige Übermittlung von Mitgliederadressen eines im Aufsichtsbezirk ansässigen Verbandes an ein Versicherungsunternehmen vorgelegt. Der Verbandsvorstand hatte eine Zusammenarbeit mit der Versicherung zum Angebot einer Gruppensterbegeld- und Gruppenunfallversicherung beschlossen.

Den Mitgliedern wurde vorab Gelegenheit zum Widerspruch gegen die Datenübermittlung gegeben. Ein Verbandsmitglied beschwerte sich darüber, trotz Widerspruchs gegen die Weitergabe seiner Adresse von einem Versicherungsmitarbeiter aufgesucht worden zu sein. Die Zustimmung bzw. Verweigerung der Datenweitergabe wurde vom Verband ordnungsgemäß in einer Datei erfaßt. Dementsprechend wurden nur solche Mitgliederadressen listenmäßig übermittelt, bei denen kein Widerspruch vorlag.

Der Grund, warum der Beschwerdeführer trotz seines Widerspruchs von einem Versicherungsmitarbeiter aufgesucht wurde, lag darin, daß er in seiner Eigenschaft als Vorstandsmitglied einer Ortsgruppe seines Verbandes angesprochen werden sollte und seine Personalien aufgrund dieser Funktion öffentlich bekannt waren.

Das Widerspruchsrecht gegen die Übermittlung von Daten zu Werbezwecken schützt den Betroffenen nur in seinen höchstpersönlichen Rechten auf informationelle Selbstbestimmung, nicht jedoch vor der Inanspruchnahme seiner Person als öffentlich bekannter Funktionsträger.

#### 8.2 Übermittlung von Arbeitnehmerdaten zu Werbezwecken

Als unzulässig sah die Aufsichtsbehörde die geplante Übermittlung von Arbeitnehmeradressen durch den Arbeitgeber an einen Versicherungsvertreter an, der persönliche Kontakte zum Anbieter einer betrieblichen Altersversorgung herstellen wollte. Dies gilt auch für den Fall, daß der Arbeitgeber den Versicherungsvertreter befristet als Arbeitnehmer einstellt, damit dieser die Adressen als "Interner" nutzen kann.

Die Übermittlung und Nutzung von Arbeitnehmerdaten, die anläßlich und im Rahmen von arbeitsrechtlichen Verhältnissen gespeichert sind, zu anderen als arbeitsvertraglichen Zwecken, ist grundsätzlich nur mit Einwilligung der Betroffenen zulässig, auch wenn dies listenmäßig geschehen soll.

Als Lösung wurde von der Aufsichtsbehörde vorgeschlagen, den Arbeitnehmern mit der Gehaltsabrechnung ein Informationsschreiben mit Antwortkärtchen zukommen zu lassen, was dem Arbeitnehmer die Möglichkeit eröffnet, selbst über die Weitergabe seiner Daten an den Versicherungsvertreter zu entscheiden.

#### 8.3 Datenverarbeitungsklauseln

Eine Reihe von Beschwerden richtete sich gegen die Meldung von Vertragsbeendigungen an Versicherungsverbände oder gleichartige Versicherungen, wovon verschiedene Versicherungsungssparten betroffen waren. Da diese Übermittlungen jedoch durchweg von schriftlichen Einwilligungen unter Verwendung der von den obersten Aufsichtsbehörden für den Datenschutz mit dem Bundesaufsichtsamt für das Versicherungswesen abgestimmten Klauseln gedeckt waren, mußte die Aufsichtsbehörde immer wieder auf diese Datenverarbeitungsklauseln verweisen und insbesondere Sinn und Zweck dieser Meldeverfahren erläutern.

Dabei wurde deutlich, daß in vielen Fällen den Betroffenen die Großzügigkeit dieser Klauseln bei Vertragsschluß überhaupt nicht klar gewesen war und sie auch nun nur wenig Verständnis dafür aufbrachten.

#### 9. Datenverarbeitung im medizinischen Bereich

#### 9.1 Krankenversichertenkarte - Einsatz der Kartentechnik im medizinischen Bereich

Seit 1993 wurde in Hessen eine Chipkarte für Krankenversicherte als Ersatz für Krankenscheine zunächst probeweise eingeführt. Seit 1. Januar 1994 ist die Karte bundesweit eingeführt. Die Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich hielten hier engen Kontakt zum Hessischen Datenschutzbeauftragten, der in seinen letzten beiden Tätigkeitsberichten (21. und 22. Tätigkeitsbericht) ausführlich diese Thematik angesprochen hat.

Auf der Krankenversichertenkarte werden zur Zeit nach der Festlegung in § 291 Sozialgesetzbuch V lediglich die ausstellende Krankenkasse, Name, Geburtsdatum und Anschrift des Versicherten, Krankenversichertennummer, Versichertenstatus und die Zeit des Versicherungsschutzes gespeichert. Der Versicherte gibt bei seinem Arzt die Karte ab, sie wird in speziellen Lesegeräten gelesen und die Daten werden für Abrechnungszwecke gespeichert. Diese neue Art der Patientendatenverarbeitung hat trotz des sensiblen Verwendungszusammenhangs eine hohe Akzeptanz bei den Betroffenen, Patienten und Ärzten gefunden. Aus diesem Bereich kam im Berichtszeitraum keine einzige Beschwerde oder Anfrage. Insofern lagen den Aufsichtsbehörden auch keine Hinweise irgendwelcher Art vor, die eine konkrete Überprüfung des Datenschutzes im Zusammenhang mit diesem Verfahren in ärztlichen Praxen veranlaßt hätten. Von den Beteiligten dieses Verfahrens bewegen sich allein die niedergelassenen Ärzte als datenverarbeitende Stellen im Zuständigkeitsbereich der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich.

Es gibt allerdings im privaten Bereich weitere Projekte im Zusammenhang mit kartengestützter Patientendatenverarbeitung. So bestehen zwischenzeitlich auch in der Presse angekündigte Bestrebungen, eine "APO-Card" herauszubringen, auf der Diagnosen und ärztliche Verschreibungen gespeichert werden sollen. Die Karte, deren Inanspruchnahme freiwillig sein soll, soll dem Apotheker, an den sich der Patient wendet, einen besseren Informationsstand über den Patienten vermitteln. Damit sollen eventuelle Verschreibungsunstimmigkeiten aufgeklärt und Unvereinbarkeiten zwischen verschiedenen Medikamenten vermieden werden.

In die Ausgestaltung dieses Verfahrens in datenschutzrechtlicher Hinsicht ist die Aufsichtsbehörde einbezogen worden. Dabei ist die Problematik zu berücksichtigen, daß auch bei freiwilligen Projekten dieser Art Gefahren für das informationelle Selbstbestimmungsrecht des Bürgers bestehen (vgl. im einzelnen 22. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Ziff. 9.1.). Der betroffene Bürger muß wirklich umfassend informiert sein, wo welche Daten über ihn gespeichert sind, und er muß grundsätzlich darüber bestimmen können, wem er welche Daten über sich offenbart.

# 9.2 Unzulässige Übermittlung an Orthopädiegeschäft

Eine Betroffene beschwerte sich darüber, daß ein Rezept für ein orthopädisches Hilfsmittel, das ihr auf telefonische Bitte hin in der Praxis des sie behandelnden Orthopäden bereitgelegt werden sollte, ohne ihr Zutun dem im selben Haus gelegenen Sanitätsfachhandel zur Ausführung übergeben wurde.

Diese Übermittlung von ihren personenbezogenen Daten war bereits deshalb rechtswidrig, weil sie gegen die Strafvorschrift des § 203 Abs. 1 Ziff. 1 StGB (Arzt/Patientengeheimnis) verstieß. Bei dieser Vorschrift handelt es sich um eine spezielle Datenschutzregelung, deren Einhaltung allerdings durch die Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich nur insoweit überprüfbar ist, als es sich um Daten aus Dateien handelt. Im gegebenen Fall war das Rezept durch eine Praxisgehilfin mittels der Praxis-EDV und der darin gespeicherten Adresse der Betroffenen erstellt worden. Wäre das Rezept wie in früheren Zeiten per Hand vom Arzt ausgeschrieben worden, so hätte die Datenschutzaufsichtsbehörde keine Überprüfung vornehmen können.

Ergebnis der Überprüfung war, daß nicht sorgfältig genug mit den über den Tag hin ausgestellten Rezepten umgegangen worden war. In Fällen, in denen der Orthopäde bereits bei der Behandlung von Akutpatienten Hilfsmittel aus dem ihm von dem Sanitätsfachgeschäft für diese Zwecke zur Verfügung gestellten Vorrat verwendete, wurde mit Wissen des Patienten ein Rezept dafür ausgestellt und zum Zwecke der Abrechnung des Hilfsmittels an das Sanitätsfachgeschäft gegeben. Insofern waren die Patienten informiert und hatten ihre Einwilligung in die damit verbundene Datenübermittlung gegeben. Weil das telefonisch estellte Rezept jedoch entgegen der Ankündigung bis Praxisende nicht abgeholt worden war, gingen die Praxismitarbeiter davon aus, daß es sich auch bei diesem Fall um ein Rezept für ein akut verwendetes Hilfsmittel handeln würde, und gaben das Rezept weiter.

#### 10. Arbeitnehmerdatenschutz

Der Arbeitnehmerdatenschutz hat einen nicht unerheblichen Anteil an den an die Datenschutzaufsichtsbehörden herangetragenen Fällen. Oft sind es die Betriebsräte, die das Thema Datenschutz ansprechen, sei es weil sie betroffene Arbeitnehmer vertreten und beraten wollen, sei es weil Datenschutz als ein Argument in sonstigen Auseinandersetzungen mit dem Arbeitgeber gerade recht kommt. Allerdings kommen auch Unternehmens- bzw. Personalverantwortliche und betriebliche Datenschutzbeauftragte zur Abklärung von datenschutzrechtlich eventuell problematischen Fällen auf die Aufsichtsbehörden zu.

#### 10.1 Bewerberdaten

In mehreren Einzelfällen ging es um die Zulässigkeit der Verarbeitung von Daten von Bewerbern.

Oft werden in Betrieben ein und dieselben Fragebögen sowohl als erstes Mittel benutzt, die Bewerber um eine Stelle kennenzulernen, als auch als Grundlage für die mit der Einstellung erfolgende Einspeicherung der Daten des eingestellten Arbeitnehmers. Die Zielrichtung ist jedoch eine sehr unterschiedliche. Der Bewerber soll möglichst schon vor dem ersten Vorstellungsgespräch angeben, ob er überhaupt nach Ausbildung und Erfahrung für die freie Stelle in Frage kommt. Von dem eingestellten Arbeitnehmer muß der Arbeitgeber bereits zur Berechnung des Entgelts bzw. eventueller Nebenleistungen oder Abzüge mehr zu seiner Familiensituation und z.B. zu seinem Glaubensbekenntnis erfahren, dies zumeist jedoch durch die Vorlage der Lohnsteuerkarte. Dem entspricht auch die Rechtsprechung des Bundesarbeitsgericht, wonach ein Arbeitgeber von einem Bewerber nur insoweit Daten erfragen - und danach auch speichern darf, als er ein berechtigtes billigenswertes und schutzwürdiges Interesse an der Beantwortung der Fragen im Hinblick auf das konkret angestrebte Arbeitsverhältnis hat (vgl. BAG vom 6. Juni 1984, DB 1984, S. 2626).

Fragen, die den Ehepartner des Bewerbers bzw. des Arbeitnehmers betreffen, sind allerdings stets problematisch. Dies gilt für den Geburtsnamen, Geburtstag, Beruf und Glaubensbekenntnis des Ehepartners. Auch das Glaubensbekenntnis des Bewerbers darf nicht quasi automatisch erhoben und gespeichert werden, es sei denn in bestimmten kirchlichen Bereichen. Auch Daten zu Kindern sind nicht stets und im einzelnen anzugeben.

Einen krassen Fall stellte ein Bewerberfragebogen dar, in dem nach persönlichen Vorlieben, der Art und Dauer der gelebten Zweierbeziehung und dem benutzten Kraftfahrzeug gefragt wurde. In diesem wie in anderen Fällen auch konnte der informierte Arbeitgeber jedoch darauf verweisen, daß die so erhobenen Daten nicht in einer Datei gespeichert würden; somit mußte die Datenschutzaufsichtsbehörde an dieser Stelle die Überprüfung abbrechen.

# 10.2 Verarbeitung von Arbeitnehmerdaten für die Betriebsratswahl

Zum Zwecke der Vorbereitung der Betriebsratswahl hat der nach § 16 BetrVG durch den noch amtierenden Betriebsrat bestellte Wahlvorstand eine Liste der Wahlberechtigten (Wählerliste) aufzustellen. § 2 Abs. 1 der Ersten Verordnung zur Durchführung des Betriebsverfassungsgesetzes (Wahlordnung) in der Fassung vom 28. September 1989 regelt das Verfahren sowie den Inhalt der Wählerliste. Danach "sollen" die Wahlberechtigten mit Famliennamen, Vornamen und Geburtsdatum aufgeführt werden, getrennt nach den Gruppen der Arbeiter und der Angestellten. Es kam jedoch vor, daß außer diesen Daten auch noch Angaben zu Beruf, Datum des Betriebseintritts und private Adresse in die Wählerliste aufgenommen wurden. Begründet wurde dies damit, daß § 2 Abs. 1 Satz 2 eine Sollvorschrift sei, die nicht ausschließe, daß noch weitere Daten außer den dort genannten aufgenommen würden. Dem konnte die Aufsichtsbehörde nicht zustimmen.

Bei der Erstellung der Wählerliste handelt es sich offensichtlich um eine Nutzung personenbezogener Daten im Sinne von § 3 Abs. 6 BDSG. Die Daten werden zwar nach § 2 Abs. 2 der Wahlordnung vom Arbeitgeber

dem Wahlvorstand zur Verfügung gestellt, eine Übermittlung ist darin jedoch nicht zu sehen, da weder Betriebsrat noch Wahlvorstand "Dritter" im Sinne von § 3 Abs. 5 Ziff. 3 BDSG ist. Nun gehen zwar spezielle Rechtsvorschriften, die Regeln für den Umgang mit personenbezogenen Daten beinhalten, den Vorschriften des Bundesdatenschutzgesetzes vor (§ 1 Abs. 4 BDG). Dies gilt jedoch nur, soweit die speziellen Regeln reichen. § 2 Abs. 1 Wahlordnung ist eine solche spezielle Rechtsvorschrift, die auf den ersten Erlaß der Wahlordnung am 16. Januar 1972 zurückgeht. Damals, mehr als 10 Jahre vor Inkrafttreten des ersten Bundesdatenschutzgesetzes und vor dem Volkszählungsurteil des Bundesverfassungsgerichts, fanden die heute anerkannten datenschutzrechtlichen Prinzipien noch keinen Eingang in die Rechtsetzung. Von daher ist zu erklären, daß § 2 Abs. 1 Satz 2 Wahlordnung als Soll-Vorschrift formuliert ist, die Anlaß zu Unklarheiten geben kann. Sie ist daher verfassungskonform, d.h. einschränkend auszulegen. Dies bereitet hier keine Schwierigkeiten, da auch nach allgemeinem juristischen Verständnis diese Formulierung nicht zwingend bedeuten muß, daß der Wahlvorstand bei der Erstellung der Wählerliste über die in der Aufzählung enthaltenen Daten hinaus Daten der Beschäftigten darin aufnehmen darf. Im Gegenteil muß die Formulierung als Sollvorschrift dazu führen, daß der Wahlvorstand z.B. das Geburtsdatum in der Wählerliste auch entfallen lassen kann. Aus der Sicht der neueren Verfassungsrechtsprechung muß jedoch die abschließende Aufzählung der genannten Daten dahin verstanden werden, daß jede darüber hinausgehende Datenaufnahme ausgeschlossen sein soll.

Sofern man dem nicht folgt, führt jedoch auch die Anwendung allgemeiner datenschutzrechtlicher Grundsätze zum gleichen Ergebnis. Nach § 4 Abs. 1 BDSG bedarf jede Verarbeitung oder Nutzung personenbezogener Daten einer besonderen Erlaubnis entweder durch Gesetz, hier durch das Bundesdatenschutzgesetz, oder durch Einwilligung der Betroffenen. Eine solche Erlaubnis wird jedoch nach den Grundsätzen, die für die Verarbeitung und Nutzung von Arbeitnehmerdaten gelten, hier kaum zu finden sein. Voraussetzung wäre nämlich, daß die Nutzung im Rahmen der Zweckbestimmung des Arbeitsverhältnisses erforderlich ist und den einzelnen Arbeitnehmer nicht unangemessen in seinen Persönlichkeitsrechten beeinträchtigt. Da weder die Bezeichnung des Berufs bzw. der Tätigkeit noch des Eintrittsdatums oder der privaten Anschrift erforderlich ist, um die aktive oder passive Wählbarkeit festzustellen, scheitert die Aufnahme dieser Daten in die Wählerliste bereits an dem ersten Kriterium.

#### 11. Auslandsdatenverarbeitung

Die Zahl der an die Aufsichtsbehörden herangetragenen Fragen nach der Zulässigkeit von Datenübermittlungen ins Ausland und den dafür geltenden Rahmenbedingungen sowie mehrere Fälle, in denen sich ausländische Staatsbürger über ihre eigenen Datenschutzinstanzen an die deutschen Behörden mit Beschwerden wegen der Verarbeitung ihrer Daten insbesondere zu Werbezwecken in Deutschland wandten, zeigen, daß den Problemen des Datenschutzes im Datenverkehr innerhalb und außerhalb Europas wachsende Bedeutung zukommt.

#### 11.1 Grundsätze der Aufsichtsbehörden

Mit dem letzten Tätigkeitsbericht der hessischen Aufsichtsbehörden waren Grundsätze veröffentlicht worden, nach denen die Aufsichtsbehörden Übermittlungen ins Ausland beurteilen (vgl. 6. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Landtags-Drs. 13/4809, S. 15 f). Darin angekündigt war die Erarbeitung einer Checkliste durch die obersten Aufsichtsbehörden, durch die der Wirtschaft Hinweise gegeben werden sollten, wie der Datenschutz durch vertragliche Vereinbarungen zwischen dem inländischen Unternehmen und dem ausländischen Datenempfänger abgesichert underforderlichenfalls gegenüber der ausländischen Gesetzeslage verstärkt werden kann. Diese Hinweise sowohl der hessischen Aufsichtsbehörden als auch der nun veröffentlichten Checkliste haben große Beachtung gefunden. Da sie, solange keine Regelungen der

Europäischen Union vorliegen, wichtige Richtschnur des behördlichen Handelns sind, sollen sie hier dargestellt werden:

I. Rechtliche Ausgangslage

Rechtsgrundlagen auch für Datenübermittlungen ins Ausland sind derzeit die §§ 28 Abs. 1 und 2 sowie § 29 Abs. 2 BDSG, soweit nicht bereichsspezifische Regelungen vorgehen. Der Tatsache, daß Datenübermittlungen in Länder stattfinden, die kein ausreichendes Datenschutzniveau haben, ist dabei bei sämtlichen Alternativen der genannten Vorschriften durch eine Abwägung mit den schutzwürdigen Interessen des Betroffenen Rechnung zu tragen; lediglich § 28 Abs. 1 Satz 1 Nr. 1 BDSG sieht eine solche Abwägung nicht ausdrücklich vor, da hier von einer jedenfalls konkludenten Einwilligung des Betroffenen ausgegangen werden kann. Vereinbarungen zwischen inländischen Datenübermittlern und ausländischen Datenempfängern mit dem Ziel, die Rechte der Betroffenen zu sichern, haben zum jetzigen Zeitpunkt also insofern Bedeutung, als sie als ein Abwägungselement in diese allgemein formulierten Abwägungsklauseln eingestellt werden können. Solche Vereinbarungen kommen vor allem dann in Betracht, wenn Datenübermittlungen durchgeführt werden sollen, für die keine entsprechende Einwilligung vorliegt und die auch nicht zur Erfüllung eines Vertrages mit dem Betroffenen erforderlich sind.

Für die Beurteilung der Zulässigkeit einer derartigen Datenübermittlung kann die nachfolgende flexibel zu handhabende Checkliste herangezogen werden, durch die der Wirtschaft ein Instrumentarium zur eigenständigen Beurteilung von Datenübermittlungen an die Hand gegeben werden soll. Eine derartige Checkliste, aus der nach den Umständen des Einzelfalls die Vertragsbestandteile eigenverantwortlich zusammengesetzt werden können, kann dazu beitragen, in einigen Bereichen den Schutz der inländischen Betroffenen zu verstärken. Dies ist vor allem erforderlich, wenn Datenschutzdefizite im Land des Datenempfängers bestehen. Mit der Checkliste soll kein Modellvertrag entworfen werden. Es geht vielmehr darum, durch zusätzliche Datenschutzmaßnahmen das Risiko für den Betroffenen bei grenzüberschreitenden Datenübermittlungen zu mindern.

#### II. Inhalt der Checkliste

1. Kooperation der Beteiligten

Die übermittlelnde Stelle soll die den Datenschutz betreffende Rechtslage im Empfängerland ermitteln, dabei bieten sich Kontaktaufnahmen zu den zuständigen Behörden im Empfängerland und zum Datenempfänger an. Ob ein Land ein ausreichendes Datenschutzniveau hat, beurteilt sich dabei anhand sämtlicher Umstände des Einzelfalls (Art der Daten, Zweckbestimmung, Verwendungszusammenhang, Dauer der geplanten Verarbeitung, allgemeine oder sektorale gesetzliche Bestimmungen im Empfängerland, Standesregeln im Empfängerland). Führt die übermittelnde Stelle trotz unklarer Datenschutzlage im Empfängerland keine Recherchen durch oder bleibt die Datenschutzlage im Empfängerland trotz derartiger Recherchen unklar, so ist im Zweifel davon auszugehen, daß das Empfängerland kein angemessenes Datenschutzniveau bietet.

2. Verwendungszusammenhang

Der Zweck der Datenverwendung solte im Vertrag möglichst präzise und verbindlich fixiert sein. Übermittelnde Stelle und Datenempfänger sollten im Vertrag ein Verbot zweckwidriger Verwendung der Daten vereinbaren. Gegebenenfalls können bestimmte unzulässige Verwendungen beispielhaft zur Klarstellung verboten werden.

#### 3. Auskunftsrechte

Im Interesse einer größtmöglichen Transparenz sollte der Betroffene Auskunftsansprüche sowohl gegen den ausländischen Datenempfänger, als auch gegen den inländischen Übermittler haben. Dieses Ziel ist effektiv jedoch nur dann zu erreichen, wenn der Datenempfänger vertraglich verpflichtet wird, der übermittelnden Stelle entsprechende Auskünfte zu erteilen, da letztere anderenfalls kaum in der Lage wäre, dem Betroffenen die verlangten Informationen zu geben.

4. Berichtigtung, Sperrung, Löschung

Auch diese Rechte sollte der Betroffene in bezug auf den ausländischen Datenbestand wahlweise gegenüber dem ausländischen Empfänger wie auch gegenüber dem inländischen Übermittler geltend machen können.

Soweit der Anspruch des Betroffenen gegenüber der übermittelnden Stelle geltend gemacht wird, richtet sich dieser Anspruch auf deren Mitwirkung bei der Erfüllung der Pflichten des Datenempfängers. Dies setzt voraus, daß sich der Datenübermittler gegenüber dem Datenempfänger einen Anspruch auf Berichtigung, Sperrung und Löschung einräumen läßt.

#### 5. Benachrichtigungspflicht

Von besonderer Bedeutung ist, daß sich die übermittelnde Stelle verpflichtet, den Betroffenen - über die gesetzliche Regelung des § 33 DSG hinausgehend - über die Datenübermittlung ins Ausland zu benachrichtigen. Dabei ist der Betroffene insbesondere auch über die ihm durch die vertragliche Vereinbarung zwischen übermittelnder Stelle und Datenempfänger eingeräumten Rechte zu informieren.

# 6. Datensicherung

Maßnahmen zur Datensicherung sollten dem Datenempfänger vertraglich auferlegt werden. Als Grundsatz sollte gelten, daß sich das Sicherheitsniveau vorrangig an der Sensibilität der Daten orientiert. Als Anhaltspunkt kann insoweit § 9 BDSG einschließlich Anlage gelten.

# 7. Vereinbarungen zur Verminderung bestehender Kontrolldefizite im

Die Umsetzung unter anderem auch der o.g. vertraglichen Vereinbarungen muß durch die übermittelnde Stelle überwacht werden können. Zu denken ist hier insbesondere an Auskunfts- und Einsichtsrechte sowie gegebenenfalls Besichtigungsrechte der übermittelnden Stelle. Auch die Einsetzung eines Beauftragten kommt in Betracht.

#### 8. Vertragsstrafe

Der Datenempfänger sollte zur Zahlung einer Vertragsstrafe an die übermittelnde Stelle für den Fall verpflichtet werden, daß er seine vertraglichen Verpflichtungen nicht einhält. Auch dadurch kann beim Datenempfänger die Bereitschaft zur Wahrung der Rechte des Betroffenen gestärkt werden.

#### 9. Haftung

Die Interessen des Betroffenen würden eine gesteigerte Berücksichtigung erfahren, wenn übermittelnde Stelle und Datenempfänger dem Betroffenen gegenüber gesamtschuldnerisch haften würden. Zu denken wäre an eine gemeinsame Verpflichtungserklärung zwischen übermittelnder Stelle und Datenempfänger, wobei der Betroffene über diesen Vertragsinhalt zu informieren wäre, da er sonst aus Unkenntnis seine erworbenen Ansprüche nicht geltend machen könnte. Im Falle der Übermittlung besonders sensibler Daten kann auch die Vereinbarung einer verschuldensunabhängigen Haftung erwogen werden.

Diese Grundsätze sind von den hessischen Aufsichtsbehörden, soweit sie bei geplanten Projekten von Unternehmensleitungen bzw. Datenschutzbeauftragten beratend in Anspruch genommen wurden, bereits als Empfehlungen angewandt worden. Die durch die Bekanntgabe der Checkliste angestoßene Diskussion sowie erste Erfahrungen mit ihrer Umsetzung in die Praxis sollen den Aufsichtsbehörden die Entscheidung ermöglichen, in welchen Punkten eine Abänderung oder Ergänzung erforderlich ist.

# 11.2 Grenzüberschreitende Direktwerbung

In mehreren Fällen wurde die Aufsichtsbehörde durch Datenschutzbeauftragte bzw. Aufsichtsinstanzen anderer europäischer Staaten um Unterstützung gebeten. So hatten sich mehrere finnische und französische Staatsangehörige an ihren Ombudsmann bzw. ihre Datenschutzaufsichtsbehörde gewandt, die von deutschen Lotterieeinnehmern mit Werbung beschickt worden waren. Sie wollten in Erfahrung bringen lassen, wie ihre Adressen zu den Lotterieeinnehmern gelangt waren und ob diese Art Datenverarbeitung nach deutschem Recht zulässig sei.

Das deutsche Datenschutzrecht schützt auch die Daten ausländischer Staatsangehöriger, die zwar nicht im Inland leben, deren Daten jedoch im Inland verarbeitet werden. Im Falle der Daten der finnischen Staatsangehörigen stammten die Adressen, die nur in der eigenen Interessentendatei des Lotterieeinnehmers gespeichert waren, nach nicht widerlegbarer Einlassung des betroffenen Lotterieeinnehmers aus Kundenhinweisen. Die

Daten wurden auf Verlangen der Betroffenen gelöscht. Im übrigen ist die Verarbeitung von Daten ausländischer Staatsbürger denselben Regeln unterworfen wie die Verarbeitung von Daten deutscher Staatsangehöriger. Auch listenmäßig zusammengefaßte Daten ausländischer potentieller Interessenten nehmen an den erleichterten Übermittlungs- und Nutzungsvoraussetzungen des § 28 Abs. 2 Ziff. 1 b BDSG teil.

Beschwerden gab es auch von deutschen Betroffenen, deren Daten von ausländischen Unternehmen für Werbezwecke genutzt wurden. In diesen Fällen nahm die Aufsichtsbehörde die Hilfe der jeweils zuständigen Datenschutzaufsichtsbehörden in Anspruch.

#### 13. Werbewirtschaft

# 13.1 Unzulässige listenmäßige Übermittlung personenbezogener Daten

Ein Großteil der in der Bundesrepublik ansässigen Wirtschaftsunternehmen, Verbände und Vereine verkauft personenbezogene Daten seiner Kunden, Interessenten und Mitglieder an Unternehmen der Werbewirt-

Diese Vorgehensweise ist aus datenschutzrechtlicher Sicht dann zulässig, wenn die personenbezogenen Daten der Kunden, Interessenten und Mitglieder listenmäßig oder sonst zusammengefaßt sind und sich auf eine Angabe über die Zugehörigkeit des Betroffenen zu einer Personengruppe (z.B. Versandhausbesteller, Zeitschriftenabonnent, Interessent für ein bestimmtes Produkt, Mitglied im Sportverein XY) sowie die Berufs-, Branchen- und Geschäftsbezeichnung, Name, Titel, akademische Grade und das Geburtsjahr des Betroffenen beschränken. Gleichzeitig darf kein Grund zu der Annahme bestehen, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat. Das Gesetz gibt jedoch selbst vor, daß ein solches Gegeninteresse des Betroffenen in der Regel besteht, wenn Daten genutzt oder übermittelt werden sollen, die im Rahmen eines vertraglichen oder quasivertraglichen Verhältnisses gespeichert worden sind und sich auf bestimmte "sensiblen" Fakten beziehen, wie Gesundheit, religiöse und politische Anschauungen usw. Im Sinne eines Regel-Ausnahme-Verhältnisses kann daher bei Daten, die sich nicht auf solche "sensible" Fakten beziehen, zunächst davon ausgegangen werden, daß ein Gegeninteresse des Betroffenen nicht besteht, sofern es nicht anderweitige Hinweise dafür gibt. Diese Zulässigkeitsvoraussetzungen werden jedoch sowohl von den Stellen, die personenbezogene Daten an Adreßhändler verkaufen, als auch von den Unternehmen der Werbewirtschaft häufig nicht beachtet.

So hatte sich ein betroffener Bürger, der ein unverlangtes Werbeschreiben eines Vereins erhalten hatte, mit der Bitte um Überprüfung dieser Angelegenheit an die Aufsichtsbehörde gewandt. Wie die Ermittlungen der Aufsichtsbehörde ergaben, hatte der Verein mit der Durchführung seiner Werbeaktion ein Direktmarketingunternehmen beauftragt. Dieses Unternehmen hatte - um an die Anschriften von Personen zu gelangen, die an dem sehr konservativen Vereinszweck Interesse zeigen könnten - bei einem Adreßverlag eine Adreßliste angemietet, auf der Personen verzeichnet waren, die einem "rechtskonservativen Verteilerkreis" zugerechnet werden. Es war aus datenschutzrechtlicher Sicht weder zulässig, daß der Adreßverlag diese Daten in seinen Datenbestand übernahm noch, daß er diese Daten an das Direktmarketingunternehmen übermittelte. Außerdem hätte das Direktmarketingunternehmen diese Daten nicht nutzen dürfen. Es besteht hier nämlich Grund zu der Annahme, daß die einem "rechtskonservativem Verteilerkreis" zugerechneten Betroffenen ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung dieser Angabe haben. Die Aufsichtsbehörde hat sowohl den Verein als auch das beauftragte Direktmarketingunternehmen auf den Verstoß gegen die Datenschutzbestimmungen hingewiesen und aufgefordert, zukünftig nur noch solche Adreßlisten zu nutzen bzw. zu verarbeiten, die die Zulässigkeitsvoraussetzungen nach dem BDSG erfüllen. Die für den außerhalb des Aufsichtsbezirks ansässigen Listeninhaber (den Adreßverlag) örtlich zuständige Datenschutzaufsichtsbehörde wurde über die Angelegenheit in Kenntnis gesetzt.

In einem anderen Fall hatte die Überprüfung bei einem Adreßverlag ergeben, daß sich ein Teil der dort gespeicherten und an werbende Unternehmen übermittelten Adreßlisten entgegen der gesetzlichen Bestimmung nicht auf die Zuordnung der Betroffenen zu einer Personengruppe beschränkte. Vielmehr beinhalteten die Adreßlisten jeweils mehrere Merkmale nebeneinander zu den darin verzeichneten Personen. So wird z.B. in einer Liste angegeben, daß die dort aufgeführten Betroffenen ein bestimmtes Produkt bestellt, per Verrechnungsscheck bezahlt und außerdem eine Schutzgebühr für den Katalog, aus dem die Bestellung erfolgt ist, entrichtet haben. Damit werden anstelle eines einzigen Merkmales zu den auf dieser Liste verzeichneten Personen gleich drei Angaben gemacht. Hierbei wurden noch nicht einmal die Einschätzungen dieser Personengruppe ("großzügig, gibt auch gerne für andere Dinge des angenehmen Lebens Geld aus") durch den Adreßverlag als eigene weitere Merkmale gewertet, da es sich hierbei um reine Spekulation handelte. Bei eben diesem Unternehmen wurden daneben auch Listen vorgefunden, die unter unzulässigen Gruppenmerkmalen liefen, z.B. als Kunden eines Spezialversenders für Erotikartikel, die dort bestimmte Dessous bestellt hatten. oder Menschen mit tatsächlichen oder vermeintlichen Schönheitsfehlern. Gerade bei der Verwendung von Gesundheitsdaten oder von aus dem Intimbereich stammenden Daten liegen hier massive Verletzungen des Persönlichkeitsrechts auf der Hand.

Wie die Ermittlungen der Aufsichtsbehörde ergeben haben, bezieht ein großer Teil der in der Bundesrepublik ansässigen Adreßverlage, die personenbezogene Daten von Wirtschaftsunternehmen, Verbänden und Vereinen anmieten, auch solche Daten, die nach den Datenschutzbestimmungen nicht verarbeitet oder genutzt werden dürfen. Da es sich hierbei um ein branchenweites Problem handelt, wurden die anderen betroffenen Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich entsprechend informiert.

#### 13.2 Widerspruchsrecht gegen die Nutzung oder Übermittlung personenbezogener Daten für Werbezwecke

Das BDSG räumt dem Betroffenen in § 28 Abs. 3 bzw. § 29 Abs. 3 ein Widerspruchsrecht gegen die Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- und Meinungsforschung ein. Widerspricht der Betroffene bei einer Stelle, die seine Daten speichert, der Nutzung oder Übermittlung seiner Daten für diese Zwecke, so ist eine weitere Nutzung oder Übermittlung für diese Zwecke unzulässig. Wenn der Betroffene sein Widerspruchsrecht bei einer Stelle einlegt, die seine Daten für die Durchführung von Werbeaktionen von einem Dritten bezogen hatte, so darf diese Stelle die angemieteten oder angekauften Daten für Werbezwecke nicht mehr nutzen.

In der Praxis berücksichtigen die Unternehmen der Werbewirtschaft sowie die für ihre Produkte werbenden Stellen jedoch das Widerspruchsrecht der Betroffenen häufig erst dann, wenn diese nach erfolglosen Versuchen, ihr Recht geltend zu machen, die Aufsichtsbehörde einschalten.

Bereits im Fünften Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden wurde dargelegt, daß die wirksame Geltendmachung des Widerspruches gegen die Nutzung oder Übermittlung personenbezogener Daten zu Werbezwecken durch die Praxis im Marketing-Bereich weitgehend verhindert wird.

Im Berichtsjahr hat sich dies anhand verschiedener Beschwerdefälle erneut bestätigt.

In einem Fall erhielt ein Betroffener in einem Zeitraum von wenigen Monaten mehrere Dutzend von unverlangten Werbezusendungen eines Unternehmens. Zunächst schickte er diese kommentarlos, ungeöffnet und für das werbende Unternehmen kostenpflichtig an dieses zurück. Da ihn die Überflutung seines Briefkastens durch diese unverlangten Werbebriefe zunehmend störte, änderte er sein Verhalten gegenüber dem Absender der unverlangten Sendungen. Nun brachte er auf den Umschlägen, die er weiterhin ungeöffnet kostenpflichtig per Post zurückgehen ließ, den Hinweis an, daß er nach § 28 Abs. 3 BDSG von seinem Widerspruchsrecht

gegen die Nutzung oder Übermittlung seiner Daten zu Werbezwecken Gebrauch mache. Dennoch erhielt er weiterhin unverlangte Zusendungen des Unternehmens, an einem Tag sogar vier Sendungen gleichzeitig.

Wie die Ermittlungen der Aufsichtsbehörde in diesem Fall ergaben, hatte das Unternehmen den Widerspruch des Betroffenen bereits zur Kenntnis genommen. Der Widerspruch blieb jedoch zunächst wirkungslos, da bereits vor diesem Zeitpunkt zahlreiche weitere Sendungen bei Subunternehmen in Auftrag gegeben worden waren. Dabei konnten die Absendungen an den Beschwerdeführer nicht mehr verhindert werden. Erst nach Ablauf mehrerer Monate erhielt der Beschwerdeführer keine unverlangten Werbezusendungen mehr.

Für viele Bürger ist es unverständlich und ärgerlich, wenn sie - obwohl sie einem bestimmten Unternehmen gegenüber ihren Widerspruch gegen die Nutzung oder Übermittlung ihrer Daten zu Werbezwecken geltend gemacht haben - dennoch von diesem Unternehmen weiterhin unverlangte Werbezusendungen erhalten. Dies ist dann nicht zu beanstanden, wenn die betroffenen Unternehmen mit der Durchführung ihrer Werbeaktionen Direktmarketingunternehmen beauftragen, welche für die Aktionen bei Dritten Adreßlisten anmieten, auf denen der Betroffene geführt wird, weil er dort - mangels der Kenntnis, daß seine Daten auch dort verarbeitet werden - seinen Widerspruch gegen die Nutzung oder Übermittlung seiner Daten zu Werbezwecken nicht geltend gemacht hat.

Sofern die Werbeaktion jedoch von der werbenden Stelle selbst durchgeführt wird, ist sie verpflichtet, auch von Dritten angekaufte Adreßbestände daraufhin zu überprüfen, ob darin Personen verzeichnet sind, die der werbenden Stelle gegenüber von ihrem Widerspruchsrecht nach § 28 Abs. 3/§ 29 Abs. 3 BDSG Gebrauch gemacht haben. Die Nutzung der Daten eines Betroffenen, der seinen Widerspruch gegen die Nutzung seiner Daten zu Werbezwecken geltend gemacht hat, ist unzulässig.

Wie die Erfahrungen der Aufsichtsbehörde gezeigt haben, ist es vielen Unternehmen der Werbewirtschaft unbekannt, daß die entgegen dem Widerspruch des Betroffenen erfolgte - unzulässige - Übermittlung seiner Daten daneben sogar strafbar ist, da hierbei unbefugt geschützte personenbezogene Daten übermittelt werden (§ 43 Abs. 1 Ziff. 1 BDSG).

#### 13.3 Nichtbeachtung von Betroffenenrechten

Die im Berichtsjahr bei den Aufsichtsbehörden insbesondere gegen Direktwerbung eingegangenen Beschwerdefälle haben gezeigt, daß viele Unternehmen ihren Pflichten gegenüber den Betroffenen, insbesondere der Auskunftspflicht, nicht oder nur zögerlich nachkommen.

Oft wurde den Betroffenen erst auf mehrmaliges Nachfragen Auskunft gegeben, vollständige Auskunft auch manchmal erst, nachdem diese die Aufsichtsbehörde eingeschaltet hatten.

So erhielt der Vorsitzende eines Betriebsrates regelmäßig unverlangte Angebote über Fortbildungssminare. Die Angebote waren unter der Anschrift seines Arbeitgebers an ihn persönlich gerichtet, allerdings unter dem unzutreffenden Zusatz "Leiter des Finanz- und Rechnungswesens". Nachdem eigene Bemühungen, die Herkunft dieses Datums zu erfahren, nichts fruchteten, wandte er sich an die Auskunftsbehörde. Erst auf deren Anfrage teilte der Seminarveranstalter mit, von welchem Direktmarketingunternehmen die Daten stammten. Damit wurde es dem Betroffenen möglich, sich zwecks Berichtigung seiner Daten mit dem Listeninhaber in Verbindung zu setzen.

In einem anderen Fall wurde einem Betroffenen von dem werbenden Unternehmen erst auf das vierte Schreiben hin geantwortet, allerdings lediglich mit der - falschen - Mitteilung, daß er keinen Anspruch auf Auskunftserteilung habe, da seine Daten dort nicht gespeichert würden. Die Ermittlungen der Aufsichtsbehörde ergaben, daß die Daten des Beschwerdeführers im Auftrag der werbenden Stelle durch ein drittes Unternehmen gespeichert wurden. Auch dann ist allerdings der Auftraggeber weiter für die Einhaltung der Datenschutzbestimmungen, also auch für die Erfüllung der Auskunftspflichten verantwortlich. Der Betroffene

hat schließlich etwa ein Jahr nach seinem erstmaligen Auskunftsersuchen die gewünschte Auskunft erhalten.

#### 14. Datenschutz im Telefonverkehr -Erfassung und Speicherung von Verbindungsdaten durch Private

In mehreren Einzelfällen wurde die Aufsichtsbehörde durch Betroffene gebeten, zur Frage der Zulässigkeit der Erhebung und Speicherung von Telefonverbindungsdaten durch Private Stellung zu nehmen.

Telefonverbindungsdaten werden in sehr großem Umfang in Hotels und Krankenhäusern für Gäste bzw. Patienten sowie in Unternehmen in bezug auf die Gespräche ihrer Mitarbeiter erhoben und gespeichert. In der Regel wird dabei die Apparate-Nummer des Anrufers, die genaue Zeit des Anrufs, die anfallenden Gebühreneinheiten sowie die angewählte Nummer gespeichert. Sofern die Zielnummer auf eine bestimmte natürliche Person angemeldet ist, werden damit - bei vollständiger Speicherung dieser Zielnummer - auch Angaben zu eben dieser Person gespeichert. Für alle speichernden Stellen, die in einem vertraglichen Verhältnis zu dem Anrufer stehen und auf dieser Grundlage die Erstattung von Gesprächsgebühren verlangen können, z.B. Hotels für die durch Gäste geführten Gespräche, Arbeitgeber in der Regel für private Gespräche der Arbeitnehmer, ist die Speicherung der drei erstgenannten Datenarten durch dieses vertragliche Verhältnis gedeckt, jedenfalls solange, wie die angefallenen Gesprächskosten noch nicht abgerechnet und bezahlt worden sind. Gegenüber dem Angerufenen gilt dies jedoch nicht. Die Speicherung seiner Rufnummer ist durch kein vertragliches Verhältnis gedeckt, sie beurteilt sich ausschließlich nach § 28 Abs. 1 Ziff. 2 BDSG. Hier ist eine Abwägung zwischen den Interessen der speichernden Stelle und eventuellen Gegeninteressen des Angerufenen zu treffen, die berücksichtigen muß, daß dem Angerufenen bereits auf der Grundlage von Art.10 Grundgesetz (Fernmeldegeheimnis) eine sehr starke Position zukommt - rechtlich betrachtet allerdings allein als Abwehrrecht gegenüber dem Staat. Durch das Fernmeldegeheimnis werden nicht nur der eigentliche Inhalt von Ferngesprächen, sondern auch bereits die Verbindungsdaten umfaßt. Auf Seiten der speichernden Stelle ist das Interesse festzustellen, die geführten Gespräche gegenüber dem Zahlungspflichtigen abzurechnen. Datum, Zeit und Dauer der Leistung sowie eine Bezeichnung der Leistung, die dem Zahlungspflichtigen die Überprüfung seiner Zahlungspflicht ermöglicht, dürfen daher ohne weiteres gespeichert werden. In der Regel muß für diesen Zweck jedoch nicht die volle Rufnummer des Angerufenen gespeichert werden. Der Zahlungspflichtige wird auf der Grundlage der Zeitdaten allein schon oft in der Lage sein zu beurteilen, ob er die Gespräche geführt hat oder nicht. In jedem Fall dürfte es ihm jedoch möglich sein, bei verkürzter Speicherung und Angabe der Zielnummer in der Abrechnung seine Zahlungspflicht zu erkennen. Nur so werden auch die Belange des Angerufenen gewahrt.

Die hessischen Aufsichtsbehörden sind daher in diesen Fällen immer dafür eingetreten, daß Zielnummern nur verkürzt gespeichert werden. Eine von einer Beschwerde eines Patienten betroffene Klinik ist dieser Auffassung gefolgt. Diskussionen mit dem Hotel- und Gaststättenverband Hessen e.V. hinsichtlich der Telefondatenspeicherung in Hotels sind dagegen leider ergebnislos geblieben. Hier konnte bisher nur erreicht werden, daß die Verbindungsdaten nicht über den Abrechnungszeitpunkt hinaus gespeichert bleiben.

#### 15. Vereinsdatenverarbeitung

In einem Fitnessclub wurde ein Zugangskontrollsystem eingeführt. Die Vereinsmitglieder bekamen auf sie persönlich ausgestellte Magnetstreifenkarten. Bei jedem Zugang muß die Karte in einen Leser eingeführt werden. Der Zugang zum Kraftraum ist ebenfalls überwacht und mit einem Sondercode abgesichert.

Nachdem ein betroffenes Vereinsmitglied um datenschutzrechtliche Bewertung dieses Sachverhalts gebeten hatte, gestaltete sich die weitere Aufklärung etwas schwierig. Nachdem der Vereinsvorstand, zu dem auch

ein Rechtsanwalt gehört, zunächst jede Datenverarbeitung bestritten hatte, wurde folgendes klar: Gespeichert werden Kartennummer, Datum, Uhrzeit und Ort des Zugangs, Tür 1 oder 2 (Kraftraum). Die Daten werden nach 1000 Eintragungen neu überschrieben, d.h. ungefähr in einem Rhythmus von 3-4 Wochen. Der Vereinsvorstand hatte dieses System auf Empfehlung eines ehemaligen Vorstandsmitglieds eingeführt, der als Unternehmer dieses System vertreibt und bereits erfolgreich unter anderem bei Banken installiert hatte. Mit Hilfe dieser Zugangskontrolle sollte gewährleistet werden, daß nur Berechtigte Zugang haben und bei Unfällen in den Trainingsräumen den durch den Verein vereinbarten Versicherungsschutz in Anspruch nehmen können.

Dieses Interesse mußte die Aufsichtsbehörde als berechtigt anerkennen, wenn man auch andererseits durchaus die Meinung hätte vertreten können, daß eine derart minutiöse Datenerhebung bereits in erheblichem Maße die Persönlichkeitsrechte der Betroffenen tangiert. Lediglich die Tatsache, daß die Speicherung relativ kurzfristig ist, führte dazu, daß die Datenverarbeitung ohne Einwilligung der einzelnen Vereinsmitglieder bzw. Nutzer nicht beanstandet wurde.

# 16. Datenverarbeitung im Wohnungseigentum

Bei der Datenverarbeitung im Zusammenhang mit der Verwaltung von Wohnungseigentum scheint ein erhebliches Defizit an datenschutzrechtlichen Kenntnissen zu bestehen.

Das Wohnungseigentumsgesetz vom 15. März 1951, das die Verhältnisse der Wohnungeigentümer untereinander und die Rollen von Verwaltung und Verwaltungsbeirat regelt, ist bei der Beurteilung der Zulässigkeit der Verarbeitung von Eigentümer- und Mieterdaten nicht sonderlich hilfreich. Nachdem auch hier Klarheit darüber besteht, daß es sich bei z.B. Verbrauchsdaten für Wasser oder Überweisungen an die Hausverwaltung um personenbezogene Daten handelt, sollte geklärt werden, unter welchen Voraussetzungen einzelne Eigentümer einer Gemeinschaft beim Verwalter Einsicht in die Einzelbelege der anderen Eigentümer nehmen dürfen. Eigentümer einer Wohnungseigentumsanlage sowie Mieter haben grundsätzlich das Recht, Abrechnungen zu überprüfen und dafür die Belege einzusehen, soweit es für die Überprüfung erforderlich ist. Dies ist in jedem Einzelfall, z.B. je nach Abrechnungsmodus, zu entscheiden. Eigentümer bilden allerdings auch noch eine selbständige rechtliche Gemeinschaft mit eigenen Rechten und Pflichten. Diese Eigentümergemeinschaft haftet gesamtschuldnerisch für Fehlbeträge und muß gegebenenfalls darüber entscheiden, ob rechtliche Schritte gegen z.B. säumige Eigentümer eingeleitet werden. Eine Bekanntgabe der säumigen Eigentümer an die Gemeinschaft, d.h. an alle Miteigentümer, ist dafür erforderlich und bewegt sich auch im Rahmen des Zwecks dieser Gemeinschaft. Eine solche Mitteilung muß jedoch die schutzwürdigen Interessen der Betroffenen so weit möglich beachten. Die Bekanntgabe sollte daher nicht in Einladungen zur Versammlung der Wohnungseigentümer oder in anderen Rundschreiben erfolgen, sondern erst in der beschlußfassenden Versammlung und mündlich. Sie als Druckmittel gegen den bzw. die Säumigen bereits vor der Versammlung einzusetzen, ist unzulässig.

#### 17. Der betriebliche Beauftragte für den Datenschutz

Erfreulich ist die Entwicklung bei der Beratung von Datenschutzbeauftragten. Die anfänglich aufgrund der Erweiterung der Anlaßaufsicht geäußerten Befürchtungen, daß nun ein Datenschutzbeauftragter auf eine Beratung durch seine zuständige Aufsichtsbehörde besser verzichten sollte, weil er damit eventuell eine Prüfung vor Ort durch die Aufsichtsbehörde riskiere, mußten wohl revidiert werden. Im Gegenteil hat sich sowohl die Zahl der Anrufe und Besuche von Datenschutzbeauftragten als auch der schriftlichen Anfragen erhöht. Die Aufsichtsbehörden sehen hier einen deutlichen Bedarf an Unterstützung insbesondere bei den Neubenennungen von unerfahrenen Datenschutzbeauftragten, die nun häufiger zu beobachten sind. Ziel ist es hier, zunächst beratend die eigenen Möglichkeiten des Tätigwerdens dem Datenschutzbeauftragten aufzuzeigen.

In einigen Fällen haben sich Datenschutzbeauftragte mit der Frage an die Aufsichtsbehörde gewandt, inwieweit sie die Belastung mit anderen Aufgaben im Unternehmen aus zeitlicher Sicht hinnehmen müssen.

Durch das BDSG wird in keiner Weise geregelt, ob und unter welchen Voraussetzungen der betriebliche Datenschutzbeauftragte haupt- oder nebenamtlich und mit welchem Anteil seiner gesamten Arbeitszeit seine Tätigkeit ausüben kann bzw. muß. Es gibt keine Richtzahlen, die sich z.B. an der Größe des Unternehmens oder an der Zahl der eingesetzten Datenverarbeitungsgeräte oder an der Zahl der mit der Verarbeitung von personenbezogenen Daten betrauten Mitarbeitern orientieren könnte (zu einem Versuch in diese Richtung siehe jedoch das Urteil des Arbeitsgerichts Offenbach vom 19. Februar 1992, RdV 1993, S. 83). Das Unternehmen muß lediglich gewährleisten, daß der betriebliche Datenschutzbeauftragte die ihm durch das Gesetz zugewiesenen Aufgaben erfüllen kann. Es muß ihm dafür genügend Zeit zur Verfügung stellen. Die Aufsichtsbehörde muß jedoch die Möglichkeit haben nachzuprüfen, inwieweit der Datenschutzbeauftragte zeitlich in der Lage ist, seine Aufgaben zu erfüllen. Nur wenn alle in § 37 BDSG genannten Aufgaben erfüllt werden (können), wird die Zeitzuweisung nicht zu beanstanden sein. Das benötigte Zeitvolumen richtet sich dabei sowohl nach der Größe des zu betreuenden Unternehmens als auch nach Art und Bedeutung der dort verarbeiteten personenbezogenen Daten und nicht zuletzt nach den Strukturen des Unternehmens. Eine Betreuung eines Unternehmens mit mehreren dezentralen Einheiten erfordert mehr Reisetätigkeit und damit auch ein größeres zur Verfügung stehenden Zeitvolumen für den Datenschutzbeauftragten.

Die Praxis zeigt leider, daß besonders in den mittleren Unternehmen sehr oft eine Überbelastung des betrieblichen Datenschutzbeauftragten mit anderen Aufgaben vorliegt. Andererseits kommt es in großen Unternehmen, die sich einen hauptamtlichen Datenschutzbeauftragten "leisten", so gut wie nie zu Beanstandungen wegen unzulänglicher Sicherstellung des Datenschutzes durch den Datenschutzbeauftragten. Dies gilt in ähnlicher Weise für die Unternehmen, die einen externen Datenschutzbeauftragten bestellt haben.

Ein anderes Problem ist die Vereinbarkeit von anderen dem nebenamtlichen Datenschutzbeauftragten zugewiesenen Aufgaben mit den vom BDSG an ihn gestellten Anforderungen. Auch wenn sich bestimmte Aufgaben anbieten, so sollten sie in der Regel nicht verantwortlich vom Datenschutzbeauftragten ausgeführt werden. Als Beispiel sei die Vergabe von Zugriffsberechtigungen erwähnt. Relativ häufig ist die Situation in Unternehmen anzutreffen, daß die Vergabe und Zuteilung von Berechtigungen zur Aufgabe des Datenschutzbeauftragten gehört. Der Datenschutzbeauftragte ist jedoch derjenige, der die Vergabe kontrollieren soll, der beratend zum korrekten Einsatz beitragen soll. Selbstverständlich ist er bei der Schaffung von Richtlinien hinzuzuziehen und sollte letztendlich das Verfahren freigeben, aber er sollte die Vergabe nicht selbständig durchführen. Er ist die Instanz, die später die Einhaltung der Richtlinie und den Einsatz zu kontrollieren hat.

Allgemein ist festzustellen, daß die Aufgabenwahrnehmung durch einen hauptamtlichen Datenschutzbeauftragten von der Aufsichtsbehörde positiver bewertet werden konnte, als wenn es sich nur um eine Nebentätigkeit handelte.

Zur Bestellung externer Datenschutzbeauftragter ist anzuführen, daß insgesamt ein positiver Trend festzustellen ist. In den der Aufsichtsbehörde bekannt gewordenen Bereichen waren selten Mängel bei dem Einsatz externer Datenschutzbeauftragter festzustellen.

Problematisch ist die Bestellpflicht, wenn ein Unternehmen, wie es insbesondere in den Bereichen Datenerfassung und Markt- und Meinungsforschung verbreitet ist, fast ausschließlich Heimarbeitskräfte unter der Bezeichnung "freier Mitarbeiter" beschäftigt. Das BDSG spricht von "Arbeitnehmern", deren Zahl für die Pflicht zur Bestellung eines Datenschutzbeauftragten maßgeblich ist.

Die Aufsichtsbehörde ist hier der Auffassung, daß diese sogenannten freien Mitarbeiter tatsächlich als Arbeitnehmer zählen, wenn ihnen Geräte und Material für die Arbeit zu Hause zur Verfügung gestellt werden und sie festumrissene Arbeitsaufträge mit im Großen und Ganzen feststehenden zeitlichen Rahmenbedingungen haben. Die von der Rechtsprechung der Arbeitsgerichte geforderte persönliche Abhängigkeit als maßgebliches Abgrenzungskriterium selbständiger Tätigkeit von der nicht selbständigen, abhängigen Tätigkeit kommt hier am stärksten in der Weisungsgebundenheit solcher Arbeitskräfte in sachlicher und zeitlicher Hinsicht zum Ausdruck. Sind die Verträge mit ihnen so ausgelegt, daß sie z.B. neben ihrer Tätigkeit als Hausfrau für kein anderes Unternehmen tätig sein können, so liegt in der Regel auch eine wirtschaftliche Abhängigkeit vor. Dies kann von der Aufsichtsbehörde allerdings nur kursorisch überprüft werden. Streitfälle hat es jedoch hierbei noch nicht gegeben. Im übrigen wäre als Alternative nur die Feststellung der Meldepflicht jedes einzelnen "freien Mitarbeiters" nach § 32 Abs. 1 Ziff. 3 BDSG möglich mit den Konsequenzen, daß zwischen Auftraggeber und "freiem Mitarbeiter" schriftliche Aufträge und Weisungen nach § 11 Abs. 2 BDSG vorliegen müßten und der Auftraggeber wiederum gegenüber seinen Auftraggebern diese Unterauftragsverhältnisses bekanntgeben und die Einwilligung dazu einholen müßte. Diese Konsequenzen sind in aller Regel nicht im Sinne der Unternehmen.

#### 18. Datenverarbeitung im Auftrag

Der Auftraggeber ist nach § 11 Abs. 2 Satz 2 BDSG verpflichtet, dem Auftragnehmer für die Verarbeitung personenbezogener Daten schriftliche Weisungen zu erteilen. Liegen keine schriftlichen Weisungen vor, können sich Schwierigkeiten bei der Ausführung eines Auftrags ergeben. Unklar kann sein, welche Plausibilitätskontrollen der Auftragnehmer gewährleisten kann. Gehören Maßnahmen zur Datensicherung zum Umfang des Auftrags? Auch die Fragen nach Verantwortungsübergängen, Aufbewahrung von Datensicherungen und die Inanspruchnahme von weiteren Subunternehmen bleiben oft offen.

Die Auftragnehmer als meldepflichtige Unternehmen sind oft besser über diese Verpflichtung aus § 11 BDG informiert als die Auftraggeber. Sie scheuen jedoch in der Regel davor zurück, den Auftraggeber darauf aufmerksam zu machen, daß "Weisungen" fehlen. Es ist jedoch auch durchaus üblich, daß die Auftragnehmer selbst die notwendigen Regelungen in (Form-) Verträgen den Auftraggebern vorgeben.

In einem Fall beauftragte ein Kreditkartenunternehmen ein euopäisches Service-Rechenzentrum mit der Verarbeitung sehr sensibler personenbezogener Daten. Dieses Rechenzentrum beauftragte wiederum ein deutsches Dienstleistungsunternehmen mit Teilen des betreffenden Auftrages. Soweit es das deutsche Dienstleistungsunternehmen betraf, war die Datenverarbeitung ordnungsgemäß. Man arbeitete jedoch in beiden Auftragsbeziehungen ohne einen schriftlichen Vertrag, ohne Weisungen durch den Auftraggeber. Es widerspricht hier offensichtlich der Verantwortlichkeit der speichernden Stelle, des Kreditkartenunternehmens, daß dieses nicht einmal wußte, wo und durch wen letztlich seine Daten verarbeitet wurden. Hier attestierte die Aufsichtsbehörde erhebliche Mängel hinsichtlich der Auftragskontrolle.

#### 19. Datensicherheit

#### 19.1 Zugangskontrolle bei der Gebäudenutzung durch mehrere Parteien

Oft werden Grundstücke und noch häufiger Gebäude von unterschiedlichen Unternehmen genutzt. Die Sicherung der jeweiligen Bereiche ist immer dann unproblematisch, wenn ganze Gebäude oder vollständige Etagen in sich abgeschlossen gesichert werden können. Die gegenseitige Abschottung ist jedoch unumgänglich. Eine Zugangsbeschränkung dergestalt, daß die nicht abgeschlossene Türe mit der Aufschrift "Kein Zutritt für Unbefugte" versehen ist, ist nicht akzeptabel. In einem anderen Fall

waren alle Türen alarmgesichert bis auf eine Tür, auf deren dem Nachbarunternehmen zugewandter Seite eine sehr große, schwere Schneidemaschine dieses Unternehmens stehen sollte. Die Besichtigung ergab, daß die Schneidemaschine längst entfernt worden war.

Zugangssicherungen sollten daher von jeder verantwortlichen Stelle eigenständig geplant, verwirklicht und kontrolliert werden. Soweit gemeinsame Sicherungen - z.B. ein gemeinsamer Pförtner - genutzt werden, muß durch Stichproben die Zuverlässigkeit dieser Einrichtungen immer wieder überprüft werden. Kontrollgänge durch betriebsfremde Hausmeister oder Wachpersonal sollten dokumentiert werden.

#### 19.2 Zugriffskontrolle

Von vielen nicht nur im Bereich der Datenverarbeitung Beschäftigten wird heute verlangt, daß sie über die eigenen privaten PINs, Kennwörter und Sicherheitscodes hinaus immer mehr geheime "Schlüssel" regelmäßig neu erfinden und im Gedächtnis behalten. Als Ausweg werden dann sprechende Paßwörter gewählt, die keine echte Sicherung mehr darstellen. Das Problem wird inzwischen bereits in den Tageszeitungen diskutiert.

Werden jedoch "sichere" Paßworte gewählt, so kann es akzeptabel sein, lediglich zwei Paßworte pro Mitarbeiter zu verwenden, beispielsweise eines für den Netzzugang und eines für die zulässigen Anwendungen.

Werden Gruppenberechtigungen vergeben, ist darauf zu achten, daß die zugrundeliegende Funktionendifferenzierung ordnungsgemäß durchgeführt wurde. In keinem Fall dürfen in diesen Fällen jedoch auch Gruppenpaßwörter benutzt werden, weil sonst die Eingabekontrolle nicht mehr gewährleistet ist. Es kann nicht mehr überprüft werden, wer aus der zum Zugang berechtigten Gruppe die jeweilige Aktion an den Daten durchgeführt hat.

#### 19.3 Datenträgerkontrolle

Werden Datenträger zwischen Auftraggeber und Auftragnehmer ausgetauscht, so sollten sie besonders gekennzeichnet sein. Auch innerhalb der speichernden Stelle sollten Datenträger immer einen - erforderlichenfalls verschlüsselten - Hinweis auf den "Eigentümer", d.h. die Stelle haben, die für die Daten verantwortlich ist.

Selbstverständlich sollten alle Datenträger, die intern oder an Dritte weitergegeben werden, nur die zur Weitergabe bestimmten Daten enthalten. Es ist sorgfältig darauf zu achten, daß Speicherungen personenbezogener Daten aus früheren Verwendungen des Datenträgers nicht nur - teilweise - überschrieben, sondern komplett und am besten durch Neuformatierung physisch gelöscht werden.

#### 20. Ordnungswidrigkeitenverfahren

Im Berichtsjahr wurden von der Aufsichtsbehörde acht Ordnungswidrigkeitenverfahren nach dem BDSG eingeleitet. Sieben dieser Verfahren betrafen zwei Unternehmen. Gegen den Geschäftsführer eines dieser Unternehmen wurden bereits in den zurückliegenden Jahren verschiedene Ordnungswidrigkeitenverfahren eingeleitet, die inzwischen durch Bußgeldbescheid bestandskräftig abgeschlossen sind.

Im Berichtsjahr hat die Aufsichtsbehörde gegen eine Wirtschaftsauskunftei Verfahren eingeleitet wegen

- der entgegen § 32 Abs. 1 BDSG verspäteten Abgabe der Meldung über die Aufnahme der geschäftsmäßigen Speicherung personenbezogener Daten zum Zwecke der Übermittlung (Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 2 BDSG),
- der entgegen § 33 Abs. 1 BDSG nicht in allen Fällen vorgenommenen Benachrichtigung der Betroffenen über die erstmalige Übermittlung ihrer personenbezogenen Daten und die Art der gespeicherten Daten (Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 3 BDSG),

- der entgegen § 29 Abs. 2 Satz 3 BDSG nicht vorgenommenen Aufzeichnung des berechtigten Interesses der Anfrager an Auskünften über Betroffene und der Nichtaufzeichnung der Art und Weise ihrer glaubhaften Darlegung bei telefonischen Auskunftsersuchen (Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 1 BDSG) sowie
- der entgegen § 38 Abs. 4 Satz 4 BDSG nicht erfolgten Duldung der Einsichtnahme in geschäftliche Unterlagen durch die von der Aufsichtsbehörde mit der Überprüfung des Unternehmens beauftragten Personen (Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 6, 2. Alternative BDSG).

Gegen einen Adreßverlag hat die Aufsichtsbehörde 3 Verfahren eingeleitet. Gegen dieses Unternehmen war in dem dem Berichtsjahr vorangehenden Jahr eine Verfügung über Anordnungen von Maßnahmen nach § 38 Abs. 5 BDSG getroffen worden. Der betroffene Adreßhändler hatte bei Beschwerden von Betroffenen gegen unverlangte Werbezusendungen, die aufgrund der Anmietung ihrer Daten bei dem Adreßhändler erfolgt waren, die Daten der Beschwerdeführer sofort aus seinen Datenbeständen gelöscht. So konnte regelmäßig nicht mehr festgestellt werden, ob die zuvor erfolgte Verarbeitung der Daten der Beschwerdeführer zulässig war. Die Anordnung sah deshalb vor, die Daten von Beschwerdeführern nicht sofort zu löschen, sondern für eine bestimmte Frist weiterhin - in gesperrtem Zustand - im Bestand zu führen, um eine Überprüfung zu ermöglichen.

Anläßlich der Kontrolle eines Einzelfalles stellte sich heraus, daß der Anordnung seit einiger Zeit nicht mehr nachgekommen wurde. Damit hat das Unternehmen der vollziehbaren Anordnung zuwider gehandelt (Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 7 BDSG). Das gleiche Unternehmen hat in einem Fall den Zutritt der 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 (Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 6, 2. Alternative BDSG). Darüber hinaus wurden von dem Adreßhändler in einem Fall Auskünfte zu einer Beschwerde entgegen § 38 Abs. 3 Satz 1 BDSG nicht erteilt (Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 6, 1. Alternative BDSG).

Wegen einer Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 6, 1. Alternative BDSG wurde auch gegen ein weiteres Unternehmen ein Ordnungswidrigkeitenverfahren eingeleitet.

Da die erwähnten Verfahren bis auf eine Ausnahme erst gegen Ende des Berichtsjahres eingeleitet wurden, sind sie noch nicht abgeschlossen.

Die Einleitung von Bußgeldverfahren unterliegt dem Opportunitätsprinzip. Das bedeutet, daß die Aufsichtsbehörde nicht verpflichtet ist, in allen Fällen, in denen Bußgeldtatbestände erfüllt sind, auch Bußgeldverfahren einzuleiten. Es ist vielmehr in jedem Einzelfall zu prüfen, ob die Ahndung durch ein Bußgeld auch angebracht ist. Wie die Erfahrungen der Aufsichtsbehörde gezeigt haben, werden Mitteilungen über die Aufnahme der meldepflichtigen Tätigkeit oder über die Änderung der meldepflichtigen Angaben von den dafür verantwortlichen Stellen häufig erst nach Ablauf der dafür vorgesehenen Ein-Monats-Frist- gemacht. In den Fällen, in denen die Meldung ohne besondere Aufforderung durch die Aufsichtsbehörde nicht vorsätzlich und nur geringfügig verspätet eingegangen ist, hat die Aufsichtsbehörde von der Einleitung eines Bußgeldverfahrens abgesehen, wenn eine Überprüfung der betroffenen Stelle vor Ort ergeben hat, daß die Datenverarbeitung weder nach Umfang noch nach ihrer Bedeutung besonders hervorgehoben ist und die Verarbeitung keinen Anlaß zur Beanstandung gegeben hat.

Die Aufsichtsbehörden schreiben Unternehmen an, die nicht im Register der meldepflichtigen Stellen geführt werden, wenn ihr Anhaltspunkte dafür vorliegen, daß diese Unternehmen meldepflichtige Tätigkeiten ausüben. Gerade im Berichtsjahr war es sehr häufig der Fall, daß die angeschriebenen Unternehmen zu den Fragen der Aufsichtsbehörde erjedoch aus Opportunitätsgesichtspunkten keine Ordnungswidrigkeitenverfahren eingeleitet. Vielmehr wurden die betroffenen Unternehmen auf ihre Pflicht zur Auskunftserteilung hingewiesen und aufgefordert, zukünftig die erforderlichen Auskünfte unverzüglich zu erteilen.

Aus dem Vorjahr wurden noch 6 Ordnungswidrigkeitenverfahren übernommen, davon wurden im Berichtsjahr drei mit Bußgeldbescheid bestandskräftig abgeschlossen und ein Verfahren eingestellt.

Wiesbaden, den 12. Juli 1994

Der Hessische Ministerpräsident Eichel

Der Hessische Minister des Innern Dr. Günther

