13. Wahlperiode

Drucksache **13/584**

HESSISCHER LANDTAG

10. 09. 91

Vorlage der Landesregierung

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

Vorgelegt mit der Stellungnahme zum Neunzehnten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten – Drucks. 12/7951 – gemäß § 30 Abs. 2 des Hessischen Datenschutzgesetzes vom 11. November 1986.

Eingegangen am 10. September 1991 · Ausgegeben am 3. Oktober 1991

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

Inhaltsverzeichnis

1.	Vorbemerkung	5
2.	Bearbeitung von Beschwerden gegen datenverarbeitende Stellen des Dritten Abschnitts des Bundesdatenschutzgesetzes alte Fassung (a.F.)	5
3.	Bearbeitung von Beschwerden gegen datenverarbeitende Stellen des Vierten Abschnitts des Bundesdatenschutzgesetzes (a.F.)	6
4.	Prüfung datenverarbeitender Stellen des Vierten Abschnitts des Bundesdatenschutzgesetzes (a.F.) von Amts wegen	6
4.1	Meldepflicht gem. § 39 Abs. 1 i.V.m. § 31 Abs. 1 Nr. 1-3 BDSG a.F.	6
4.1.1	„outsourcing"	6
4.1.2	Verbundene Unternehmen	7
4.2	Register	7
4.3	Prüfungsübersicht	7
5.	Kreditkartenunternehmen	8
5.1	Teilnahme am SCHUFA-Verfahren	8
5.2	Werbung mit Kreditkartenadressen	8
5.3	Versicherungsangebote von Kreditkartenunternehmen	9
5.4	Kartenmißbrauch und betrügerische Praktiken	9
6.	Wirtschaftsauskunfteien	10
6.1	Benachrichtigung	10
6.2	Darlegung und Dokumentation des berechtigten Interesses gem. § 32 Abs. 2 BDSG a.F.	10
6.2.1	Vorgetäuschte Darlegung des berechtigten Interesses	11
6.2.2	Dokumentation der Gründe für das Vorliegen eines berechtigten Interesses und der Mittel für ihre glaubhafte Darlegung	11
6.3	Spekulative Speicherung geschützter personenbezogener Daten	12
6.4	Ehegattendaten	12
6.5	Wechselprotestlisten	13
6.6	SCHUFA	13
7.	Werbewirtschaft	14
8.	Versand- und Einzelhandel	15
9.	Auslandsdatenverarbeitung	15
10.	Verbindungen zwischen nicht-öffentlichem und öffentlichem Bereich	16
11.	Patientendaten	16
12.	Mieterdaten	16
13.	Betrieblicher Datenschutzbeauftragter	16
14.	Datensicherung	17
14.1	Zugangskontrolle	17
14.2	Zugriffskontrolle	18

14.3 Datenträgerverwaltung: Abgangskontrolle – Transportkontrolle 19
14.4 Datenträgervernichtung 19
14.5 Beauftragung von Sub-Datenverarbeitungsunternehmen . 19
15. Ordnungswidrigkeiten 20

1. Vorbemerkung

Der vorliegende Tätigkeitsbericht schließt die Reihe der Berichte ab, die das vorrangige Ziel hatten, die hessischen Erfahrungen für die Novellierung des Bundesdatenschutzgesetzes nutzbar zu machen.

Das am 1. Juni 1991 in Kraft getretene Bundesdatenschutzgesetz hat nicht alle Erwartungen der Landesregierung erfüllt. Vor allem ist die von Hessen im Bundesrat beantragte Ausdehnung des Geltungsbereiches auf Akten nicht erfolgt. Mit dieser Feststellung soll nach Abschluß des Gesetzgebungssverfahrens keine nutzlose Kritik um ihrer selbst willen vorgebracht werden, sondern den Betroffenen soll deutlich gemacht werden, was sie von dem neuen Gesetz nicht erwarten dürfen.

Anders als die Datenschutzbeauftragten im öffentlichen Bereich kann die Aufsichtsbehörde im privaten Bereich einer Beeinträchtigung des Persönlichkeitsrechts beim Umgang mit personenbezogenen Daten nur entgegentreten, wenn die Daten in einer Datei gespeichert sind oder aus ihr stammen.

Außerdem müssen sich Betroffene und datenverarbeitende Stellen auf eine Zeit der Unsicherheit einstellen, da die vielen in einem zu langen Gesetzgebungsverfahren gefundenen nicht immer bis in alle Konsequenzen durchdachten Kompromisse zu einigen unklaren Regelungen geführt haben.

Zu begrüßen ist dagegen die Stärkung der den Aufsichtsbehörden eingeräumten Befugnisse. Die Aufsichtsbehörden werden sie vor allem nutzen, um die Anforderungen durchzusetzen, die schon nach dem bisherigen Gesetz zu erfüllen waren.

Soweit die Novellierung neue Verpflichtungen schafft, werden die Aufsichtsbehörden in enger Abstimmung mit den Ländern Auslegungs- und Anwendungsprobleme mit den Betroffenen erörtern, bevor sie von ihren Durchsetzungsmöglichkeiten Gebrauch machen. Klarstellende Verwaltungsvorschriften sind vorerst nicht sinnvoll, da keine vermuteten Probleme gelöst werden sollen, sondern nur solche, die in der Praxis auch tatsächlich auftreten. In deren Darstellung wird eine der wesentlichen Aufgaben der künftigen Berichte liegen, damit die Betroffenen die gefundenen Lösungen nachvollziehen können, was für den Erfolg der Neuregelungen von erheblicher Bedeutung sein dürfte.

2. Bearbeitung von Beschwerden gegen datenverarbeitende Stellen des Dritten Abschnitts des Bundesdatenschutzgesetzes alte Fassung (a.F.)

Gegen Stellen, die Datenverarbeitung als Hilfsmittel für die Erfüllung ihrer eigenen Geschäftszwecke oder -ziele verarbeiten, gingen im Berichtsjahr 81 Beschwerden ein. Die Beschwerden betrafen:

- Kreditkartenunternehmen in 19 Fällen,
- Versicherungen und Versicherungsagenturen in 12 Fällen,
- den Handel (Versand- sowie Einzelhandel) in 7 Fällen,
- Kreditinstitute in 8 Fällen,
- das Gesundheitswesen (Ärzte, Apotheken, Krankenhäuser) in 6 Fällen,
- Touristikunternehmen in 3 Fällen,
- Verlage in 2 Fällen,
- Inkassounternehmen in 1 Fall,
- sonstige Unternehmen in 23 Fällen.

In elf Fällen waren die Beschwerden begründet, davon in je zwei Fällen gegen Kreditkartenunternehmen, Handelsunternehmen und Kreditinstitute, in je einem Fall gegen eine Versicherung bzw. Versicherungsagentur, eine Apotheke und ein Inkassounternehmen sowie in zwei Fällen gegen sonstige Unternehmen. Bei zwei Beschwerden konnte nicht mehr abschließend festgestellt werden, ob die Datenverarbeitung in zulässiger oder unzulässiger Art und Weise erfolgt war. In sieben Fällen sind die Ermittlungen der Aufsichtsbehörden noch nicht abgeschlossen.

Von den genannten Beschwerden abgesehen, wurden von den Aufsichtsbehörden zahlreiche schriftliche und mündliche Anfragen und Vorspra-

chen von betroffenen Bürgern, Betriebsräten, Datenschutzbeauftragten und Unternehmen zu Fragen des Datenschutzes bei datenverarbeitenden Stellen des Dritten Abschnitts des BDSG a.F. beantwortet.

3. Bearbeitung von Beschwerden gegen datenverarbeitende Stellen des Vierten Abschnitts des Bundesdatenschutzgesetzes (a.F.)

Im Berichtsjahr gingen 22 Beschwerden betroffener Bürger gegen Unternehmen ein, die geschäftsmäßige Datenverarbeitung für fremde Zwecke betreiben. Die Beschwerden betrafen:

- Kreditinformationsdienste (Wirtschaftsauskunftteien und SCHUFA) in 18 Fällen,
- Adresshändler in 4 Fällen.

In sieben Fällen (Kreditinformationsdienste) waren die Beschwerden begründet. Bei zwei Beschwerden gegen Unternehmen des Adresshandels konnte nicht mehr abschließend festgestellt werden, ob die Datenverarbeitung in zulässiger oder unzulässiger Art und Weise erfolgt war.

Auch im Bereich des Vierten Abschnitts des BDSG a.F. wurden zahlreiche schriftliche und mündliche Anfragen betroffener Bürger beantwortet.

4. Prüfung datenverarbeitender Stellen des Vierten Abschnitts des Bundesdatenschutzgesetzes (a.F.) von Amts wegen

4.1 Meldepflicht gem. § 39 Abs. 1 i.V.m. § 31 Abs. 1 Nr. 1-3 BDSG a.F.

Gemäß § 39 Abs. 1 BDSG a.F. haben die in § 31 Abs. 1 Nr. 1-3 BDSG a.F. genannten Personen und Gesellschaften, die Datenverarbeitung für fremde Zwecke betreiben, die Aufnahme der meldepflichtigen Tätigkeit der zuständigen Aufsichtsbehörden binnen eines Monats zur Aufnahme in das bei ihr geführte Register (siehe Punkt 4.2.) anzuzeigen.

Wie bereits in den Vorjahren fielen insbesondere im Bereich der Serviceunternehmen (Datenerfasser, Vernichter-, Auftragsverarbeitung) zahlreiche kleinere Unternehmen auf, die zum Teil seit mehreren Jahren der Meldepflicht nicht nachgekommen waren. Um hier Abhilfe zu schaffen, wurden die Industrie- und Handelskammern gebeten, auf die Meldepflicht nach dem BDSG, die möglichen Folgen des Versäumens sowie auf grundsätzliche Anforderungen im Bereich der Fremddatenverarbeitung in ihren Publikationen hinzuweisen. Die daraufhin erschienenen Hinweise in den Kammerpublikationen hatten jedoch nur wenige Meldungen an die Aufsichtsbehörde zur Folge.

Des weiteren ist immer noch festzustellen, daß die Meldepflicht im Bereich verbundener Unternehmen selten richtig beurteilt wird. Unsicherheit besteht hier sowohl in einem bestimmten Bereich des „outsourcing" als auch bei dem Problem der „Funktionsübernahme".

4.1.1 „outsourcing"

Es ist zu beobachten, daß Unternehmen in zunehmendem Umfang die Datenverarbeitung auf andere spezialisierte Unternehmen übertragen, die nicht nur Maschinen und Personal zur Verfügung stellen, sondern auch die Entwicklung und Pflege der speziellen Anwendungen übernehmen. Hierbei wird manchmal die Datenverarbeitung nicht gänzlich außer Haus gegeben, was bei der Zuordnung zum Vierten Abschnitt des BDSG a.F. in der Regel keine Schwierigkeiten bereitet. Es gibt vielmehr auch die Gestaltung, daß das Dienstleistungsunternehmen Mitarbeiter allein für einen Auftraggeber abstellt und ihre Arbeitsplätze im Hause des Auftraggebers einrichtet. Auch in diesem Fall findet eine nach § 31 Abs. 1 Ziff. 3 BDSG a.F. meldepflichtige Tätigkeit statt, für die allerdings die beim Auftraggeber eingerichtete Zweigniederlassung oder unselbständige Zweigstelle des Serviceunternehmens meldepflichtig ist, sofern eine eigene Eintragung im Handelsregister vorliegt bzw. der Datenverarbeitungsgruppe vor Ort eine gewisse organisatorische Eigenständigkeit zukommt (vgl. vorläufige Verwaltungsvorschriften zum BDSG, Staatsanzeiger 1981, S. 430).

4.1.2 Verbundene Unternehmen

Unklar ist oft auch die rechtliche Bewertung der Datenverarbeitung in verbundenen Unternehmen. So mußten oft Fälle von Unternehmensübernahmen einer sehr genauen und umfangreichen Prüfung unterzogen werden. Solange ein aufgekauftes Unternehmen unabhängig von den neuen Beteiligungs- bzw. Eigentumsverhältnissen in seiner Eigenständigkeit erhalten bleibt und weiter lediglich eigene Datenverarbeitung betreibt, ändert sich die datenschutzrechtliche Einordnung in den Dritten Abschnitt des BDSG a.F. nicht. Wird jedoch die Datenverarbeitung, weil in kleineren Einheiten zu aufwendig, auf eines der verbundenen Unternehmen konzentriert, so entsteht für dieses Unternehmen die Meldepflicht.

Auch der ähnlich zu beurteilende Fall, daß die Datenverarbeitung eines Unternehmens, ohne daß irgendeine räumliche Veränderung erfolgt, rechtlich abgetrennt und zum Beispiel in Form einer eigenen Gesellschaft weitergeführt wird, löst die Meldepflicht aus, sofern weiter personenbezogene Daten für das Mutterunternehmen verarbeitet werden.

Dabei spielt es keine Rolle, ob die Verantwortungsträger von auftraggebendem und beauftragtem Unternehmen identisch sind. In einigen Fällen waren auf diese Weise Veränderungen in Unternehmen durchgeführt worden, ohne die datenschutzrechtlichen Konsequenzen zu überblikken.

Noch schwieriger in der Bewertung gestalteten sich die Fälle, bei denen aufgrund von Unternehmensverflechtungen nicht nur die eigentliche Datenverarbeitung, sondern die damit unterstützte Funktion zum Teil oder in Gänze auf eines der Unternehmen übertragen wurde. Da zunehmend auch die die Funktion bildende Verwaltungsarbeit automatisiert und von der Datenverarbeitung mitübernommen wird, die Verwaltung somit mehr und mehr lediglich als Zulieferer von Daten handelt, ist die Unterscheidung zwischen meldepflichtiger Datenverarbeitung im Auftrag und nicht meldepflichtiger Tätigkeit aufgrund Funktionsübertragung manchmal sehr schwierig.

4.2 Register

Zur Zeit sind zu dem gem. § 40 Abs. 1 Satz 2 BDSG a.F. geführten Register 519 Unternehmen gemeldet.

4.3 Prüfungsübersicht

Im Berichtsjahr 1990 wurden 66 Prüfungen gem. § 40 BDSG a.F. durchgeführt. Davon betrafen Datenverarbeiter nach § 31 Abs. 1 Satz 1 Ziffer 3 BDSG a.F. insgesamt 48, nämlich

- Servicerechenzentren 26,
- Konzerndatenverarbeiter 7,
- Datenerfasser 9,
- Mikroverfilmer 2,
- Datenträgervernichter 1,
- Telemarketing 3.

Des weiteren wurden zehn Kreditinformationsdienste und drei Branchen· informationsdienste sowie acht Unternehmen aus dem Bereich der Markt- und Meinungsforscher geprüft.

Die Prüfungen brachten folgendes Ergebnis:

- Beanstandungen 42,
- Empfehlungen 19,
- ohne wesentliche Beanstandungen 5.

Folgende wesentliche Mängel wurden am häufigsten festgestellt:

1. Keine bzw. verspätete oder unvollständige Registermeldung nach § 39 BDSG a.F.
2. Keine bzw. unwirksame Bestellung des Datenschutzbeauftragten
3. Unzureichende Zugangskontrolle (Raum/Objektsicherung)
4. Unzureichende Datenträgerverwaltung
5. Unzureichende Zugriffskontrolle (Passwort)

6. Keine Benachrichtigung bei der ersten Datenübermittlung gem. § 34 Abs. 1 BDSG a.F.
7. Keine Verpflichtung der Mitarbeiter nach § 5 BDSG a.F.
8. Unzureichende Auftragskontrolle
9. Unzureichende Dokumentation

in 13 Fällen wurden Prüfungen vorzeitig abgebrochen, da sich herausstellte, daß keine meldepflichtige Tätigkeit mehr ausgeübt wurde.

5. Kreditkartenunternehmen

5.1 Teilnahme am SCHUFA-Verfahren

Im Berichtsjahr wurden sämtliche Kreditkartenunternehmen von der SCHUFA aufgefordert, ihre bisherigen Verträge mit der SCHUFA neu zu gestalten. Bis dahin hatten die Kreditkartenunternehmen der SCHUFA lediglich Daten über nicht vertragsgemäße Abwicklung (Negativmerkmale) übermittelt. Sie erhielten ihrerseits von der SCHUFA auch nur Auskünfte über vorhandene Negativmerkmale, das sind Mitteilungen über nicht vertragsgemäßes Verhalten von Kunden, nicht jedoch über aufgenommene Kredite und bestehende Bürgschaftsverpflichtungen. Nunmehr übermitteln auch die Kreditkarteninstitute wie sonstige der SCHUFA angeschlossene Kreditinstitute der SCHUFA Daten über die Beantragung, den Abschluß und die Beendigung des Kreditkartenvertrages aufgrund einer Einwilligung des Kunden, die dieser mit seinem Kartenantrag erteilt. Die Kreditkartenunternehmen erhalten damit auf Anfrage auch Auskünfte über alle bei der SCHUFA vorhandenen Daten. In diesen Auskünften ist jedoch nicht enthalten, wer diese Daten zur Speicherung ursprünglich an die SCHUFA übermittelt hat, anders als in den Selbstauskünften, die jeder Betroffene bei der örtlich zuständigen SCHUFA über sich selbst einholen kann.

Diese Umstellung der Verträge zwischen den Kreditkartenunternehmen und der SCHUFA hatte zur Folge, daß die Kreditkartenunternehmen auf Forderung der SCHUFA eine einheitliche Formulierung der SCHUFA-Klausel in ihre Antragsformulare aufnehmen mußten. Zumindest, was die SCHUFA-Klausel betrifft, wurden damit Forderungen der Aufsichtsbehörde an die Kreditkartenunternehmen nach größerer Klarheit und Ausführlichkeit der auf den Antragsformularen abgedruckten Vertragsbedingungen im Interesse der Kreditkartenkunden erfüllt.

Leider läßt sich dies für die weiter auf den Antragsformularen aller Kreditkartenunternehmen vorhandenen formularmäßigen Einwilligungserklärungen des Kunden zur Einholung von Auskünften bzw. für die Übermittlung ihn betreffender Daten an das Kreditkartenunternehmen nicht dermaßen uneingeschränkt sagen. Zwar sind die Unternehmen der Forderung der Aufsichtsbehörde nach Nennung der speichernden Stelle – die bei Vorliegen einer Funktionsübertragung nicht unbedingt identisch sein muß mit dem Kartenherausgeber – mit Namen und Anschrift im Antragsformular nachgekommen. Dennoch ist gelegentlich festzustellen, daß weder die in dem SCHUFA-Teil vorhandene noch die weitere datenschutzrechtlich erhebliche Einwilligungserklärung des Kunden in irgend einer Weise besonders in dem zumeist sehr unübersichtlichen Formulartext hervorgehoben wird. Es besteht damit die Gefahr, daß der Kunde nicht überblickt, welche Erklärungen er mit der Abgabe seines Kartenantrages eigentlich abgibt.

5.2 Werbung mit Kreditkartenadressen

Die in der Vergangenheit teilweise von Kreditkartenunternehmen geübte Praxis, die Adressen von Kreditkartenkunden über einen Adressmakler (listbroker) anderen Unternehmen zu Werbezwecken zu vermieten, war im Berichtszeitraum Gegenstand nur noch einer einzigen Beschwerde. Zur Zeit bestehen keine Anhaltspunkte mehr dafür, daß diese in der Vergangenheit mehrfach beanstandete Praxis fortgesetzt wird.

Für den Werbungsempfänger war in der Vergangenheit nicht erkennbar, daß er z.B. durch die Rücksendung einer vorgedruckten Antwortkarte an das werbende Unternehmen gleichzeitig seine Eigenschaft als Kreditkarteninhaber und damit unter Umständen auch Daten über sein Mindesteinkommen preisgab.

Diese Befürchtung der unbeabsichtigten Informationspreisgabe besteht dann nicht mehr, wenn das Kreditkartenunternehmen die Werbung von Drittunternehmen z.B. der eigenen Werbung oder der Kreditkartenabrechnung hinzufügt. Man kann dann davon ausgehen, daß der Kreditkartenkunde die Verbindung zwischen Kreditkartenunternehmen und werbendem Unternehmen erkennt und in der Regel weiß, daß er durch Reaktion auf die Werbung dem werbenden Unternehmen seine Kreditkarteninhabereigenschaft offenlegt. Wenn, wie dies häufig der Fall ist, die Bestellung beim werbenden Unternehmen dann noch die Angabe der Kartennummer erfordert, müßten die Informationsflüsse jedem offenkundig sein. Datenschutzrechtliche Bedenken bestehen deshalb in diesem Zusammenhang nicht mehr.

5.3 Versicherungsangebote von Kreditkartenunternehmen

Kreditkartenunternehmen verbinden ihre Hauptdienstleistung aus Marketinggründen häufig mit zusätzlichen Versicherungsangeboten. Dies sind in der Regel Gruppenversicherungen, bei denen dem Versicherungsunternehmen nur die Zahl der Versicherten, aber nicht der einzelne Versicherte bekannt ist. In einem von der Aufsichtsbehörde geprüften derartigen Einzelfall konnte sich der Versicherungsnehmer im Schadensfall direkt an das Versicherungsunternehmen wenden und wurde damit erst zu diesem Zeitpunkt namentlich bekannt, ohne daß Daten des Versicherungsfalles auch dem Kreditkartenunternehmen zugänglich wurden. Datenschutzrechtlich ist eine derartige Vorgehensweise empfehlenswert, weil Datenflüsse nur diejenigen erreichen, für deren Zwecke sie auch bestimmt sind. Angeboten werden jedoch auch Einzelversicherungen, wobei in der Regel die Prämie über die Kreditkarte gezahlt wird. Bereits aus der Prämienhöhe lassen sich mit Kenntnis des Alters, der Versicherungsart und der allgemeinen Prämienstruktur Rückschlüsse auf die Person, evtl. auch auf besondere Risiken, ziehen. Das Kreditkartenunternehmen verfügt darüber hinaus mit dem Versicherungsantrag, den es vergleichbar einem Versicherungsvertreter an die Versicherung weiterleitet, über alle relevanten Daten.

In Anbetracht dessen, daß ein Kreditkartenunternehmen aus den laufenden Transaktionen des Kunden bereits über eine große Informationsbasis verfügt, ist eine derartige Wissenserweiterung nicht gänzlich unbedenklich. Aus mehreren Anfragen ist auch bekannt, daß an der wirtschaftlichen Nutzung solcher Datensammlungen ein überaus großes Interesse besteht. In diesem Zusammenhang sind jedoch bis jetzt noch keine Beschwerden bekannt geworden. Es bestand deshalb auch noch keine Gelegenheit, im konkreten Einzelfall den gesamten Informationsfluß im Zusammenhang mit Versicherungen zu überprüfen.

5.4 Kartenmißbrauch und betrügerische Praktiken

Die wachsende Verbreitung von Kreditkarten macht sich, wie bereits in der Öffentlichkeit bekannt wurde, auch in einer wachsenden Anzahl von Mißbrauchsfällen sowie in steigenden Schadenssummen bemerkbar. Datenschutzrechtlich wurde dieser Bereich dadurch relevant, daß Betroffene die Löschung von persönlichen bzw. ihnen zurechenbaren Daten bei Kreditkartenunternehmen anstrebten, die z.B. aufgrund von gefälschten Kreditkartenanträgen bei Kreditkartenunternehmen gespeichert wurden.

Ein Betroffener bekam, ohne entsprechende Kreditkartenanforderungen gestellt zu haben, von verschiedenen Kartenunternehmen Kreditkarten zugesandt. Er wandte sich deshalb an die Kreditkarteninstitute, wobei sich herausstellte, daß ein Dritter auf den Namen des Betroffenen Kreditkartenanträge gestellt hatte, offensichtlich mit der Absicht, die Karten sich selbst zu verschaffen. Anläßlich verschiedener Telefonate mit den Kreditkartenunternehmen erfuhr der Beschwerdeführer, daß seine Daten dort in der Rubrik „Betrug" mit der Bemerkung „Betrugsversuch" gespeichert waren. Da die Kreditkartenunternehmen dem Verlangen des Beschwerdeführers, alle zu seiner Person gespeicherten Daten zu löschen, nicht nachkamen, wandte sich der Beschwerdeführer mit der Bitte um Unterstützung an die Aufsichtsbehörde. Allseits akzeptiert wurde, daß die Daten des Betroffenen nicht mehr als Kundendaten geführt werden durften. Über die weitere Speicherung des Namens des Betroffenen in einer Datei über Betrugs- bzw. Mißbrauchsfälle bestanden jedoch Differenzen. Die Unternehmen machten zum Teil ein Dokumentationsinteresse geltend, das auch

die Speicherung der personenbezogenen Daten des Betroffenen erfordere. Sollte die Speicherung in weiteren Dateien der Kreditkarteninstitute – z.B. in einer „Mißbrauchsdatei" – jedoch derart gestaltet sein, daß der Betroffene dadurch in einen negativen Zusammenhang mit einer Straftat gebracht wird, wäre eine solche Speicherung unzulässig, da dadurch schutzwürdige Belange des Betroffenen beeinträchtigt würden.

Die Beteiligten einigten sich schließlich, nur einen Hinweis auf den Aktenvorgang ohne Namensnennung zu speichern. Eines der beteiligten Kartenunternehmen verzichtete ganz auf die weitere Speicherung der Daten zu dem Mißbrauchsfall.

In diesem wie in ähnlichen Fällen der betrügerischen Erschleichung von Kreditkarten ist zu beachten, daß die Kartenunternehmen Daten, die das Kreditkartenverhältnis betreffen, an die SCHUFA übermitteln (siehe oben 5.1). Dies kann unter Umständen kurzfristig dazu führen, daß Anschlußpartner der SCHUFA Betroffene, die gar nicht wissen, daß auf ihren Namen eine Kreditkarte betrügerisch eingesetzt wird, aufgrund der eingetragenen Negativmerkmale als nicht oder nicht ausreichend kreditwürdig betrachten. Die Schäden, die hierdurch den Betroffenen entstehen können, sind leicht vorstellbar.

6. Wirtschaftsauskunfteien

6.1 Benachrichtigung

Im Dritten Tätigkeitsbericht waren vorgefundene Mängel bei der Erfüllung der Benachrichtigungspflicht gem. § 34 Abs. 1 BDSG a.F. geschildert worden. Das Tätigwerden der Aufsichtsbehörden, d.h. die Forderung an die Auskunftei, die Benachrichtigungen durchzuführen bzw. nachzuholen, hat jedoch zu Irritationen der Betroffenen und zahlreichen mündlichen und schriftlichen Anfragen und Beschwerden geführt. Es wurde vermutet, daß mit der Benachrichtigung über das Vorliegen einer Speicherung und dem Angebot, gegen Entgelt Auskunft über die im einzelnen gespeicherten Daten zu geben, lediglich eine Einnahmequelle für die Auskunftei erschlossen werden sollte. Die Betroffenen brachten auch deutlich ihre Unsicherheit zum Ausdruck, in welchem Umfang und zu welchem Zweck ihre Daten bei einer Auskunftei gespeichert würden. Nach Darstellung der datenschutzrechtlichen Regelungen, die für Auskunfteien gelten, waren die Betroffenen zwar etwas beruhigt, äußerten aber ausnahmslos überhaupt kein Verständnis dafür, daß ihnen der Auftraggeber der Auskunftei, d.h. derjenige, an den die Auskunftei ihre Daten übermittelt hatte, verschwiegen wurde. An diesem Zustand ändert leider auch die Novellierung des BDSG nichts Grundlegendes, da danach der Betroffene Auskunft über den Empfänger der Daten nur dann verlangen kann, wenn er begründete Zweifel an der Richtigkeit der Daten geltend macht (§ 34 Abs. 2 Satz 2 BDSG neue Fassung n.F.).

6.2 Darlegung und Dokumentation des berechtigten Interesses gem. § 32 Abs. 2 BDSG a.F.

Häufig wenden sich Bürger beschwerdeführend an die Aufsichtsbehörde, weil sie sich dagegen verwahren, daß Wirtschaftsauskunfteien Daten zu ihrer Person speichern und an Dritte weitergeben. In diesen Fällen erklärt die Aufsichtsbehörde dem Betroffenen, daß das BDSG die Verarbeitung geschützter personenbezogener Daten von Privatpersonen unter bestimmten Voraussetzungen erlaubt. § 32 BDSG a.F. gibt die Erlaubnis zum Speichern personenbezogener Daten unabhängig von der Einwilligung oder der Kenntnis der Betroffenen, soweit kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Nach Abs. 2 dieser Vorschrift ist auch das Übermitteln personenbezogener Daten an Dritte – ebenfalls ohne die Einwilligung oder vorherige Kenntnis der Betroffenen – zulässig, wenn der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat. Die Neufassung des BDSG trifft hier mit § 29 ganz ähnliche Regelungen, wobei in Abs. 2 für die Übermittlung im Vergleich zum bisher geltenden Recht klargestellt wird, daß auch die schutzwürdigen Interessen des Betroffenen an dem Ausschluß der Übermittlung zu berücksichtigen sind.

Als berechtigte Interessen des Empfängers sind auch wirtschaftliche Interessen anerkannt. So dürfen z.B. Wirtschaftsunternehmen vor Abschluß von Verträgen, wie unter anderem Kredit-, Raten- und

Leasingverträgen, und der Anbahnung und Erweiterung anderer geschäftlicher Beziehungen Auskünfte über die Bonität ihrer Vertragspartner einholen. Auch die Erstbestellung bei einem Versandhaus oder die Einräumung eines Kredites im Versandhandel kann zu einer Überprüfung des Bestellers durch eine Auskunftei führen.

6.2.1 Vorgetäuschte Darlegung des berechtigten Interesses

Das Verfahren verschiedener Auskunfteien, Anfragescheine auszugeben, auf denen die Anfrager die Art des jeweiligen berechtigten Interesses nur auf einem vorgedruckten Formular ankreuzen müssen, erleichtert, daß sich manche Anfrager Auskünfte erschleichen, indem sie ein nicht zutreffendes Anfragemerkmal ankreuzen.

Die vorgetäuschte Darlegung eines berechtigten Interesses soll der folgende Fall deutlich machen:

Der Geschäftsführer eines Unternehmens wollte für seinen Urlaub eine Ferienwohnung mieten. Da er eine erhebliche Vorauszahlung leisten sollte, wollte er sich der Bonität des Wohnungsvermieters versichern. Er fragte deshalb bei einer Wirtschaftsauskunftei über den Wohnungsvermieter an, wobei er seinen Firmennamen benutzte und auf dem Anfrageschein als berechtigtes Interesse „Bonitätsprüfung, Kredit 20.000,– DM" angab. Nachdem der Betroffene von der Auskunftei gem. § 34 Abs. 1 BDSG a.F. über die erfolgte Datenspeicherung benachrichtigt worden war, wandte er sich beschwerdeführend an die Auskunftsbehörde, da er davon ausging, daß zum Zeitpunkt der Anfrage kein berechtigtes Interesse an einer Auskunft zu seiner Person vorgelegen haben konnte. Die Ermittlungen der Aufsichtsbehörde ergaben zunächst, daß ein anfragendes Unternehmen um Auskunft über den Betroffenen nachgefragt hatte und dabei als berechtigtes Interesse, wie oben geschildert, „Bonitätsprüfung, Kredit 20.000,– DM" glaubhaft dargelegt hatte. Daß nicht das anfragende Unternehmen, sondern vielmehr dessen Geschäftsführer aus privatem Interesse die Datenübermittlung veranlaßt hatte, und daß das vorgebrachte berechtigte Interesse nicht zutraf, konnte die Aufsichtsbehörde zu diesem Zeitpunkt nicht erkennen, denn das BDSG erlaubt es der Aufsichtsbehörde – sofern die Daten weder automatisiert verarbeitet noch regelmäßig übermittelt werden – nicht, dem Betroffenen mitzuteilen, wer über ihn angefragt hat und welches berechtigte Interesse angegeben wurde. Somit sind die Betroffenen selbst zunächst gar nicht in der Lage festzustellen, ob Anfragen über ihre Person ein berechtigtes Interesse zugrunde gelegen hat. Außerdem gilt die Identität des Empfängers der Auskunft gem. § 30 des hessischen Verwaltungsverfahrensgesetzes als „fremdes Geschäftsgeheimnis", welches dem Betroffenen nicht mitgeteilt werden darf. Erst dann, wenn durch die Aufsichtsbehörde positiv festgestellt wird, daß in einem Beschwerdefall gegen Bestimmungen des BDSG verstoßen wurde, ist dem Betroffenen der Empfänger der Daten mitzuteilen, wenn die Betroffenen diese Information zur Verfolgung ihrer Rechte auf zivilrechtlichem Wege benötigen. Im geschilderten Fall wurde das eigentliche Interesse des Geschäftsführers an der Kenntnis der Daten des Betroffenen erst bekannt, nachdem das anfragende Unternehmen auf Anforderung eine Stellungnahme zu dieser Anfrage abgab. Der Vorgang hatte für den Anfrager zur damaligen Zeit noch keine Konsequenzen. Es ist aber darauf hinzuweisen, daß die Novelle des BDSG einen solchen Sachverhalt nunmehr als Antragsdelikt unter Strafe stellt (§ 43 Abs. 2 Ziff. 1 BDSG n.F.).

6.2.2 Dokumentation der Gründe für das Vorliegen eines berechtigten Interesses und der Mittel für ihre glaubhafte Darlegung

Nach § 32 Abs. 2 Satz 2 BDSG a.F. sind bei der Übermittlung von Daten von z.B. durch Auskunfteien an Dritte die Gründe für das Vorliegen eines berechtigten Interesses des Empfängers an der Kenntnis der Daten sowie die Mittel für ihre glaubhafte Darlegung aufzuzeichnen. Dies gilt unverändert auch nach § 29 Abs. 2 Satz 3 BDSG (n.F.). Damit wird überhaupt erst die nachträgliche Überprüfung von Übermittlungsvorgängen durch die Aufsichtsbehörde möglich. Die Nachprüfung des berechtigten Interesses gestaltet sich jedoch gelegentlich schwierig. Im Einvernehmen mit den obersten Aufsichtsbehörden der Länder überprüfen die Auskunfteien in einem Promille der Fälle selbst das berechtigte Interesse beim Datenempfänger. Bei einer behördlichen Regelüberprüfung wurde jedoch festgestellt, daß diese Kontrollen nur einmal im Jahr und nicht über das

ganze Jahr verteilt vorgenommen werden. Dies wurde beanstandet, weil damit auftretende Fehlentwicklungen unter Umständen nur sehr spät erkannt werden können.

Außerdem trägt der große zeitliche Abstand zu dem der Anfrage zugrundeliegenden Vorgang die Gefahr in sich, daß Nachweise nicht mehr auffindbar sind und sich auch niemand mehr an Einzelfälle erinnern kann. Im Berichtszeitraum gab es Beschwerdefälle, in denen sich die Aufzeichnungen der Auskunftei als zu ungenügend erwiesen, um im Einzelfall das berechtigte Interesse tatsächlich zu belegen. In diesen Fällen war eine Überprüfung bei dem Anfrager erforderlich. In einem Fall mußte jedoch festgestellt werden, daß sowohl die Auskunftei aufgrund der bei ihr über die Anfrage gespeicherten Daten, als auch das anfragende Unternehmen, bei dem der zugehörende Vorgang weder aufzufinden, noch in irgendeiner Weise erinnerlich war, kein berechtigtes Interesse an der Übermittlung mehr nachweisen konnten. Hierbei wurde deutlich, daß das als Kompromiß zugelassene Selbstkontrollverfahren überdacht werden muß.

6.3 Spekulative Speicherung geschützter personenbezogener Daten

Ein Einzelkaufmann wandte sich an die Aufsichtsbehörde, weil er festgestellt hatte, daß eine Auskunftei zu seiner Person und seinem Unternehmen unzutreffende Daten gespeichert und an Dritte übermittelt hatte. Der Beschwerdeführer gab an, daß zum Teil erhebliche Abweichungen von den tatsächlichen Verhältnissen – z.B. zum Umsatz, zum Grundbesitz, zu Forderungen und Außenständen, zu kurzfristigen Verbindlichkeiten und zum Warenlager – gespeichert und an Dritte übermittelt würden. Ein Großteil der bestrittenen Daten war in einer dem Betroffenen vorgelegten Selbstauskunft als „Schätzung außenstehender Quellen" gekennzeichnet.

Die Auskunfteien müssen, da nur zutreffende Daten gespeichert werden dürfen, bezüglich der bestrittenen Daten erneut recherchieren. Sofern sich trotzdem weder die Richtigkeit noch die Unrichtigkeit der bestrittenen Daten durch die Auskunftei objektiv feststellen läßt, müssen die bestrittenen Daten gem. § 35 Abs. 2 BDSG a.F. (§ 35 Abs. 4 BDSG n.F.) gesperrt werden. Sperrung bedeutet, daß die bestrittenen Daten nicht mehr verarbeitet, insbesondere übermittelt oder sonst genutzt werden dürfen. Legt der Betroffene – wie im Fall des Beschwerdeführers – der Behörde Nachweise vor, daß die Schätzung in verschiedenen Punkten unrichtig war, zieht die Behörde diese Information zwar zur abschließenden Beurteilung des Falles heran, gibt die konkreten Daten jedoch nicht an die Auskunftei weiter.

Im geschilderten Fall hatte die Auskunftei zunächst die bestrittenen Daten gesperrt und versucht, neu zu recherchieren. Hier zeigte sich jedoch die Schwierigkeit, über Einzelkaufleute, die nicht zu einer Selbstauskunft bereit sind, durch Recherchen über Dritte zutreffende Daten zu erheben. Auch bei der Kennzeichnung der Daten als „geschätzt" wird von der Aufsichtsbehörde bei erheblichen Differenzen verlangt, daß die gespeicherten Daten nicht weiter genutzt werden.

Aufgrund dieser Situation stellte die Auskunftei die Auskunft über den Beschwerdeführer ein. Ob dies jedoch für den Betroffenen in Anbetracht möglicherweise anfragender Geschäftspartner günstiger ist als die Bekanntgabe der tatsächlichen Daten durch den Betroffenen an die Auskunftei, mag dahingestellt bleiben, zeigt jedoch das Dilemma auf, in dem sich derjenige befindet, der Daten zu seiner Person Auskunfteien nicht bekannt geben möchte.

6.4 Ehegattendaten

Die Gleichberechtigung von Mann und Frau verbietet es, Daten einer Frau als informatorisches Anhängsel ihres Ehemannes zu speichern. Die Daten der Ehepartner sind getrennt zu erfassen, zu speichern und zu übermitteln, sofern die gesetzlichen Voraussetzungen dafür vorliegen. Auch die Benachrichtigung über die Speicherung hat getrennt zu geschehen. Ob diese Grundsätze eingehalten werden, wurde in einer großen Auskunftei überprüft. Die Daten von zwölf Familienunternehmen im Rhein-Main-Gebiet wurden abgefragt. In acht Fällen waren familiäre Daten überhaupt nicht gespeichert, in drei Fällen abstrakt („verheiratet, zwei Kinder") und in einem Fall konkret: „verheiratet mit A... geborene M..., geboren am 1. 1.

1950, Familie". Die Ehefrau übte in der Firma keine geschäftliche Funktion aus, sondern wurde nur in ihrer Rolle als Ehefrau und Mutter erwähnt. Die Auskunftei wurde aufgefordert, die Daten der Ehefrau zu löschen, da die weitere Speicherung und Übermittlung als unzulässig angesehen wurde. Die Auskunftei erklärte sich bereit, in Zukunft von sich aus verstärkt darauf zu achten, ob die Speicherung von Ehegattendaten berechtigt ist. Andere Auskunfteien sollen in gleicher Weise überprüft werden, da auch hier bekannt wurde, daß Daten der Ehegatten bis hin zu Beruf und ausgeübter Tätigkeit gespeichert und bei Auskünften übermittelt werden.

6.5 Wechselprotestlisten

Die Nutzung der von der Arbeitsgemeinschaft des Bankengewerbes in Form einer wöchentlichen Liste herausgegebenen Wechselprotestinformationen durch Auskunfteien wird bereits seit längerem kritisch beobachtet (siehe Vorjahresbericht Ziffer 5.3). Bisher bestand jedoch keine Möglichkeit, die Verwendung dieser Daten, die ursprünglich lediglich den Banken zugänglich sein sollten, im Auskunfteibereich zu reglementieren, da mangels des Vorliegens einer Datei im Sinne des BDSG dieses nicht anwendbar ist. Da bisher das BDSG auch nicht die Erhebung der Daten, d.h. den Weg, auf dem die Daten vor der Einspeicherung in eine Datei erlangt worden sind, erfaßte, wird erst die Rechtslage aufgrund des neuen ab 1. 6. 1991 geltenden BDSG ein Tätigwerden der Aufsichtsbehörde ermöglichen. Dann ist auch die Erhebung der Daten in den Schutzbereich einbezogen und ausdrücklich geregelt, daß Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben werden müssen (§ 28 Abs. 1 letzter Satz BDSG n.F.).

6.6 SCHUFA

Gemessen an der großen Datenflut, die von der SCHUFA verarbeitet wird, ist die Zahl der eingegangenen Beschwerden sehr gering. Eine Speicherung und Übermittlung falscher Daten geht in diesen Fällen meistens auf die falsche, verspätete oder unterlassene Datenübermittlung des SCHUFA-Vertragspartners zurück. Die Verantwortung für die daraufhin erfolgte Speicherung bleibt trotzdem beim speichernden Unternehmen, also bei der SCHUFA.

So war in einem Fall bei der SCHUFA über einen längeren Zeitraum ein Girokonto und ein damit verbundener hoher Kredit unberechtigterweise gespeichert. Die betroffene Bank behauptete, sie habe die Löschung des Kontos an die SCHUFA schriftlich gemeldet, die SCHUFA bestritt den Erhalt dieser Meldung. Eine Löschung der Konten und damit auch der Kreditdaten unterblieb. Hier wäre zu überlegen, ob seitens der Banken, die in aller Regel die Kundenkonten automatisiert führen, bereits programmseitig eine Routine installiert wird, die mit der Löschung eines Kontos bzw. Kredits automatisch die Meldung an die SCHUFA verbindet und ausführt. Das noch praktizierte Verfahren, die Löschungsmeldungen der Abarbeitung durch Sachbearbeiter auf dem Schriftweg zu überlassen, provoziert nicht nur mögliche Übermittlungsfehler, sondern auch Verzögerungen und Unkontrollierbarkeiten.

In einem anderen Fall stellte eine Betroffene nach Ablehnung der Erweiterung eines Überziehungskredits durch die Einholung einer SCHUFA-Selbstauskunft fest, daß dort Daten zu Zwangsvollstreckungen ohne Hinweis auf den zwischenzeitlich erfolgten Zahlungsausgleich verzeichnet waren. Die Ermittlungen der Aufsichtsbehörde, die die Betroffene eingeschaltet hatte, ergaben, daß der Zahlungsausgleich der Forderungen bereits zwei Monate vor Einholung der Selbstauskunft erfolgt war, von dem SCHUFA-Anschlußpartner aber erst vier Wochen nach Ausgleich der Forderung eingemeldet worden war. Darüber hinaus hatte die SCHUFA den Zahlungsausgleich erst zu einem nicht mehr genau nachvollziehbaren Zeitpunkt vier bis fünf Wochen nach der Einmeldung durch den Vertragspartner in den zur Person der Beschwerdeführerin geführten Datenbestand eingearbeitet. Diese Frist war ebenso wie das Zuwarten des Vertragspartners mit der Einmeldung zu lang, da Änderungen in den Datenbeständen der Betroffenen in deren Interesse, insbesondere wenn es sich wie im Beschwerdefall um Zahlungsausgleiche oder Erledigtvermerke handelt, der SCHUFA unverzüglich zu melden und möglichst zeitnah in die dort geführten Datenbestände einzuarbeiten sind. Sowohl das Ver-

fahren als auch die unzureichende Dokumentation der Änderungseingaben waren daher Grund für eine Beanstandung.

7. Werbewirtschaft

Auch in diesem Berichtsjahr beschwerten sich zahlreiche Bürger über ihnen unverlangt zugegangene Werbebriefe. Mit gut einem Viertel am Anteil aller der Aufsichtsbehörde schriftlich vorgetragenen Beschwerden bildete der Bereich Adresshandel und Werbung einen Schwerpunkt der Tätigkeit nach § 30 Abs. 1 BDSG a.F.

Am Beispiel der Beschwerde eines Betroffenen, der innerhalb eines kurzen Zeitraumes mehrere unverlangt zugegangene Werbesendungen erhielt, soll dieser Problemkreis näher beleuchtet werden.

Der Betroffene fragte sich zunächst, wie die werbenden Unternehmen an seine Adresse gelangt waren, da er zu den werbenden Stellen noch keinen Kontakt hatte, also dort noch nichts bestellt hatte oder sonstige Geschäftsbeziehungen eingegangen war. Er wandte sich mit dieser Frage direkt an die werbenden Unternehmen. Von dort erfuhr er, daß seine Adresse für alle Werbeaktionen jeweils von demselben Adresshändler angemietet worden war. Um zu verhindern, daß dieser Adresshändler seine Adresse an weitere werbende Unternehmen vermietet, wandte sich der Beschwerdeführer an diesen mit der Bitte um Mitteilung, ob der Adressverlag über Namen und Anschrift hinaus weitere Daten zu seiner Person gespeichert habe und auf welche Art und Weise der Verlag Kenntnis von diesen Daten erlangt habe. Falls erforderlich wollte der Bürger auch bei der Datenquelle sein Recht auf Löschung seiner personenbezogenen Daten geltend machen. Da der Beschwerdeführer die gewünschte Auskunft von dem Adresshändler zunächst nicht erhielt, wandte er sich mit der Bitte um Unterstützung an die Aufsichtsbehörde. Wie die dortigen Ermittlungen ergaben, hatte eines der Unternehmen, das ihm eine unverlangte Werbesendung hatte zukommen lassen, gleich nachdem sich der Umworbene mit seiner Frage, woher seine Adresse stamme, an den Adressverlag gewandt und diesen über das Anliegen des Beschwerdeführers informiert. Daraufhin hatte der Adressverlag die zu dem Beschwerdeführer geführten Daten aus seinem Datenbestand gelöscht, da er davon ausgegangen war, der Betroffene wünsche keine weiteren unverlangten Werbesendungen. Aufgrund der vorzeitigen Löschung konnte der Betroffene jedoch sein Recht auf Auskunft über die zu seiner Person gespeicherten Daten und vor allem über die Herkunft seiner Adresse nicht mehr verwirklichen.

Wie im geschilderten Beispiel wurden der Aufsichtsbehörde mehrere Fälle bekannt, in denen aufgrund einer vorzeitigen Löschung nicht mehr geklärt werden konnte, ob die jeweiligen Listeninhaber (Adresshändler bzw. Direktwerbeunternehmen) in zulässiger Art und Weise an die von ihnen gespeicherten und vermieteten Daten gelangt waren. Aus diesem Grund wurde dem betroffenen Adressverlag vorgeschlagen, zunächst bei der Mitteilung von Listenanmietern, daß sich Umworbene über die unverlangt zugesandte Werbung beschweren, die personenbezogenen Daten dieser Betroffenen – sofern sie es nicht selbst wünschen – nicht sofort zu löschen, sondern zunächst nur zu sperren. Durch diese Vorgehensweise bleibt den Betroffenen das Recht auf Auskunft zu den zu ihrer Person gespeicherten Daten erhalten. Auch jedem Bürger, der sich von unverlangt zugesandter Werbung belästigt fühlt, ist anzuraten, nicht sofort die Löschung sämtlicher Daten, sondern zunächst nur die Sperrung zu verlangen, wenn er – mit oder ohne Hilfe der Aufsichtsbehörde – noch in Erfahrung bringen will, woher seine Adresse stammt und an wen sie weitervermittelt wurde. Ein Problem, das mit dem neuen BDSG und den erweiterten Nutzungsmöglichkeiten von Daten für Werbezwecke noch an Bedeutung gewinnen wird, ist die Behandlung von „Verweigererdateien". Relevant wurde dies in dem Fall einer Beschwerde gegen ein Unternehmen, das Werbematerial im Auftrag von Werbetreibenden an Haushalte verteilt. Um seiner Verpflichtung nachzukommen, nicht Personen mit Werbung zu beliefern, die sich ausdrücklich dagegen verwahren, z.B. mittels Aufkleber am Briefkasten oder persönlicher Beschwerde beim Werbetreibenden, schrieb es die Personen, die ihm durch die Werbetreibenden zum Teil bereits vor Jahren namentlich genannt worden waren, an und bat um Erklärung, ob sie weiterhin die Zustellung von Werbematerial ablehnten. Es wollte damit vermutete „Karteileichen" aus seiner Werbeverweigererdatei aussondern. Dabei war von Bedeutung, daß bei auch nur

einem „Verweigerer" in einem Mehrfamilienhaus üblicherweise das ganze Haus nicht mehr mit Werbung beliefert wurde. Zu einer Herausnahme aus der „Verweigererdatei" sollte dabei nur die ausdrückliche Erklärung führen, wieder Werbung beziehen zu wollen, nicht jedoch das Schweigen der Angeschriebenen.

Die Aufsichtsbehörde konnte an diesem Verfahren datenschutzrechtlich nichts beanstanden, zumal das Unternehmen mit der Aufnahme der „Werbungsverweigerer" in eine Datei nur deren ursprünglich allerdings an das auftraggebende, werbetreibende Unternehmen gerichteten Wunsch nachgekommen war. Einer Löschung derjenigen, die auf das Anschreiben nicht reagierten, hätte die Aufsichtsbehörde allerdings widersprochen. Die Löschung aus der „Verweigererdatei" trotz der wenn auch zum Teil bereits Jahre zurückliegenden eigenen Erklärung der Betroffenen hätte eine Beeinträchtigung schützwürdiger Belange der Betroffenen bedeutet.

Das Problem, mit zu einem großen Teil veralteten Daten umzugehen, besteht in gleicher Weise auch für den deutschen Direktmarketingverband e.V., der für Bürger, die nicht mit persönlicher Werbung bedacht werden wollen, die Eintragung in die sog. „Robinsonliste" anbietet. Vor allem durch Umzug und Heirat veralten die Daten schnell. Eine Löschung aller Daten, die bereits seit Jahren gespeichert sind, stehen die oben geschilderten Bedenken entgegen. Neuerdings wird die Eintragung für fünf Jahre befristet vorgenommen, worauf die Betroffenen hingewiesen werden. Diese Regelung erscheint für beide Seiten in der Praxis akzeptabel.

8. Versand- und Einzelhandel

Die Beschwerden im Bereich des Versand- bzw. Einzelhandels haben im Berichtszeitraum deutlich abgenommen.

Ein Hauptproblempunkt bestand darin, daß oft unnötig offen mit personenbezogenen Daten von Kunden umgegangen wird.

In einem Fall konnte ein Einzelhandelsunternehmen überzeugt werden, in allen Filialen im Bundesgebiet Verfahrensänderungen durchzuführen. Dort waren bei Bezahlung der gekauften Waren mit Euroscheck auf einem für Kunden einsehbaren Kleinbildschirm nicht nur der Warenwert, sondern auch die vom Euroscheckformular übernommene Schecknummer und Bankleitzahl der Kundenbank angezeigt worden. Die Anzeige war ohne Schwierigkeit für andere Kunden lesbar. Im Interesse des Schutzes der Kunden wurde auf diese Anzeige verzichtet, wenn auch die Daten weiterhin bis zur Einlösung des Scheckbetrages automatisiert zu Kontrollzwecken gespeichert bleiben.

Vom nicht gerade sensiblen Umgang mit Kundendaten zeugen Beschwerden gegen Unternehmen, die eine Politik des „offenen Bildschirms" betreiben, wenn z.B. Optiker Daten über eine Brillenbestellung im PC verarbeiten, der so postiert ist, daß jeder andere Kunde, der vielleicht noch auf Bedienung wartet, die Daten des gerade Bedienten Kunden einfach ablesen kann. Auch hier wurde jedoch nach Beratung Abhilfe zugesagt.

9. Auslandsdatenverarbeitung

Ein Bereich, der wieder stärker in den Vordergrund trat, waren die zunehmenden Datenströme vom und ins Ausland besonders auf dem Hintergrund der näherrückenden europäischen Integration.

Die Aufsichtsbehörde wurde hier mehrfach um Beratung bzw. um Darstellung ihres Rechtsstandpunktes gebeten, da z.B. Verlagerungen der Datenverarbeitung ins Ausland erhebliche Investitionen erfordern und man dies mit einer positiven Stellungnahme der Behörde abzusichern sucht. Anerkennend ist hier hervorzuheben, daß auch über das rechtlich unabdingbar Erforderliche hinaus meistens die Bereitschaft festzustellen ist, die Rechte der Betroffenen, wie sie das BDSG garantiert, so umfassend wie möglich auch bei Bearbeitung im Ausland zu sichern. Hier macht das Beispiel der SCHUFA Schule, die mit Vertragspartnern im Ausland Verträge abschließt, die für Betroffene im Ausland ähnliche Rechte sicherstellen, wie sie das BDSG für das Inland festlegt. Obwohl es sowohl auf seiten der Wirtschaft wie auf seiten der Daten- und Verbraucherschützer auch Stimmen gibt, die solche Verträge ablehnen, scheint doch ein breiter Konsens zu bestehen, im Interesse der sozial verträglichen

Entwicklung der wirtschaftlichen Verflechtung und nicht zuletzt im Interesse der Integrität der eigenen Unternehmenspolitik Vertragslösungen zu befürworten. Inwieweit die Vertragslösungen tatsächlich geeignet sind, Persönlichkeitsrechte wirksam unabhängig vom Ort zu schützen, muß und wird, solange keine europaweit gleich wirksame Datenschutzgesetzgebung vorhanden ist, die Zukunft zeigen.

10. Verbindungen zwischen nicht-öffentlichem und öffentlichem Bereich

In zwei Fällen wurden Verkehrsteilnehmer, die als Halter bzw. Fahrer eines Kraftfahrzeuges an Unfällen beteiligt waren, von den zuständigen Ordnungsbehörden aufgefordert nachzuweisen, daß ihre Fahrzeuge wieder ordnungsgemäß in Stand gesetzt bzw. abgemeldet seien.

In beiden Fällen waren den Behörden konkrete Daten über die Unfallbeteiligung der Betroffenen und den Schadensumfang unaufgefordert von Kraftfahrzeugversicherungen übermittelt worden, die auf seiten des jeweiligen Unfallgegners mit der Schadensabwicklung befaßt waren. Die Versicherer stützten sich dabei auf die vom Bundesministerium für Verkehr erlassene Verwaltungsrichtlinie Nr. 111 – zulassungsrechtliche Behandlung totalbeschädigter Kraftfahrzeuge – vom 27. 6. 1989 (abgedruckt in Verkehrsblatt 1989, S. 435). Darin wird Versicherern „empfohlen", sich um Abmeldung der ihnen als total beschädigt bekannten Fahrzeuge zu bemühen bzw. die Zulassungsstellen mittels Formschreiben zu informieren, wenn diese Bemühung erfolglos war.

Die Sachverhalte wurden von der Aufsichtsbehörde insbesondere deshalb kritisch betrachtet, weil die Richtlinie des Ministeriums von den Versicherern als Rechtsgrundlage für die Übermittlung der Daten in Anspruch genommen wurde. Unter Beachtung der Grundsätze, die das Bundesverfassungsgericht zum informationellen Selbstbestimmungsrecht aufgestellt hat (BVerfGE 65, 1 ff.), kommen als Rechtsgrundlage für Datenübermittlungen grundsätzlich nur formelle Gesetze in Betracht.

Die Recherchen ergaben jedoch, daß eine mögliche Anwendbarkeit des BDSG bereits am fehlenden Merkmal der Übermittlung aus einer Datei im Sinne des § 1 Abs. 2 BDSG a.F. scheiterte.

11. Patientendaten

Der Patient einer Klinik, der dort ambulant eine Fingerschiene erhalten hatte, wunderte sich zu Recht darüber, daß er über diese Schiene eine Rechnung von einem ihm unbekannten Orthopädie-Fachhändler erhielt, obwohl er im Krankenhaus seinen Krankenschein abgegeben hatte. Tatsächlich war die Übermittlung der personenbezogenen Daten nach der zum 1.1.1990 in Kraft getretenen „Verordnung über Hilfsmittel von geringem therapeutischen Wert" nicht mehr erforderlich, da ohnehin keine Übernahme der Kosten durch die Krankenkasse mehr erfolgte.

12. Mieterdaten

In § 28 des Formularmietvertrages eines Haus- und Grundeigentümer-Verbandes heißt es u. a. „Der Mieter ist damit einverstanden, daß Angaben zur jeweiligen Miethöhe sowie zur Art, Größe, Ausstattung, Beschaffenheit und Lage der Wohnung zum Zwecke der Erstellung von Mietpreisübersichten und Vergleichsmietensammlungen weitergegeben und dort gespeichert werden".

Während nach dieser Formulierung nur Daten übermittelt werden sollten, die sich ganz speziell und ausschließlich auf die jeweilige Wohnung beziehen, ohne daß der Name des Mieters erscheint, hat der Haus- und Grundeigentümer-Verband an seine Mitglieder tatsächlich ein Formular versendet, in dem auch der Name des jeweiligen Mieters vorgesehen war.

Hiergegen bestehen aus datenschutzrechtlicher Sicht jedoch Bedenken, weil die Angabe des jeweiligen Mieters für die Erstellung eines Mietkatasters nicht erforderlich ist.

13. Betrieblicher Datenschutzbeauftragter

Nach dem Bundesdatenschutzgesetz müssen sowohl Unternehmen, die eigene, als auch Unternehmen, die personenbezogene Daten für Dritte

verarbeiten, einen Datenschutzbeauftragten schriftlich bestellen, wenn eine bestimmte Zahl von Beschäftigten mit der Datenverarbeitung betraut ist.

Bei den meisten Prüfungen nach § 40 BDSG gab es hierbei mehr oder weniger bedeutsame Beanstandungen.

Von der Bestellung sind zunächst diejenigen ausgeschlossen, die Inhaber, Vorstandsmitglieder, Geschäftsführer oder sonst zum Leiter des Betriebes oder Unternehmens berufen sind (Rückschluß aus § 28 Abs. 3 BDSG a.F.). Eine Identität würde der Aufsichtsbehörde bereits bei der Abgabe der Registermeldung auffallen, weil dabei auch die Besetzung aller genannten Positionen anzugeben ist. Probleme tauchten jedoch deshalb auf, weil öfter Leiter der Personalverwaltung oder Vertriebsleiter oder gar Leiter der Datenverarbeitung zum Datenschutzbeauftragten bestellt wurden. Dies widerspricht in der Regel der Intention, die das Gesetz mit der Einrichtung des internen Datenschutzbeauftragten erreichen will, da diese Personen in der besonderen Gefahr stehen, in kaum lösbare Interessenkonflikte zu geraten. Mit anderen Worten: derjenige, der in seiner Hauptfunktion gegenüber seinem Arbeitgeber verantwortlich für den Umgang mit personenbezogenen Daten ist, soll nicht als Datenschutzbeauftragter nachträglich eben diesen Umgang kontrollieren. Dennoch wird nicht nur bei mittleren, sondern auch bei größeren Unternehmen, die durchaus über einen geeigneten Personalbestand verfügen, eine solche Fehlbesetzung festgestellt. Oft geht dies Hand in Hand mit der Feststellung, daß die vom Gesetz genannten Aufgaben des Datenschutzbeauftragten (§ 29 BDSG a.F., § 37 BDSG n.F.) nicht oder nur sehr vereinzelt wahrgenommen werden. Eine solche Besetzung der Funktion des Datenschutzbeauftragten muß allerdings nicht zwangsläufig zu einer Beanstandung oder gar zu einem Ordnungswidrigkeitenverfahren führen. Werden mögliche Interessenkonflikte durch Kompetenzverteilung verringert, revisionsfähige Kontrollverfahren und Nachweise geschaffen und liegt eine überprüfbare, den gesetzlichen Anforderungen entsprechende Tätigkeit des Datenschutzbeauftragten vor, so ging die Aufsichtsbehörde bisher in Ausnahmefällen davon aus, daß Interessenkonflikte zwischen den Funktionen mit einiger Sicherheit vermeidbar sind.

Aus den aktuellen Prüfungserfahrungen muß schließlich darauf hingewiesen werden, daß nicht nur der neu bestellte Datenschutzbeauftragte gewisse Grundkenntnisse vorweisen bzw. erwerben muß, sondern sich auch in der Folgezeit weiterbilden und auf dem Laufenden halten muß. Die bei Prüfungen stets gestellte Frage nach Qualifizierungsmaßnahmen bzw. Weiterbildung hat zu oft zum Ergebnis geführt, daß allenfalls jahrealte Bestätigungen über den Besuch von Fortbildungsveranstaltungen vorgelegt werden können.

14. Datensicherung

Mängel bei den Datensicherungsmaßnahmen, also den technischen und organisatorischen Maßnahmen zur Erfüllung der in der Anlage zu § 6 Abs. 1 Satz 1 BDSG a.F., (§ 9 Satz 1 BDSG n.F.) enthaltenen Anforderungen, waren in folgenden Bereichen schwerpunktmäßig zu beobachten.

14.1 Zugangskontrolle

In einem Fall mußte festgestellt werden, daß hinsichtlich des Zugangs zu den Datenverarbeitungsanlagen bzw. zu den Auswertungen keinerlei Regelung getroffen worden war. Normalerweise sind zumindest zwei kontrollierte Sicherheitszonen eingerichtet, einmal für das gesamte Betriebsgelände bzw. Gebäude, zum anderen in unterschiedlicher Intensität für den eigentlichen Rechenzentrumsbereich. Je nach Sensitivität der verarbeiteten Daten werden unterschiedliche Anforderungen an die Zugangskontrolle gestellt, insbesondere zu den Räumen der eigentlichen Datenverarbeitungsanlage, des Datenträgerarchivs bzw. zu den Räumen, in denen Maschinenausdrucke gestapelt, sortiert und zur weiteren Behandlung gelagert werden. Der Zugang z.B. über die Betätigung eines Nummernschlosses, bei dem mehrere Mitarbeiter über mehrere Tage eine einzige Nummer benutzen konnten, wurde als nicht ausreichend beanstandet. Beanstandet wurde auch, wenn zwar eine ausreichende individuelle Zugangssicherung installiert war, die Vergabe der Zugangsberechtigungen jedoch nicht kontrollierbar war, weil die Regelungen, wer

überhaupt von seiner Funktion her Zugang zu den jeweiligen Räumen haben sollte, oder die Dokumentation der Ausgabe von Zugangsberechtigungen mangelhaft waren. So wurde in einem Fall festgestellt, daß zwar wie inzwischen üblich die Magnetkarten für die Türschließanlagen für sämtliche Mitarbeiter neu in neutraler Form, also ohne Nennung des Betriebes ausgegeben worden waren, jedoch ausgerechnet ein Vorgesetzter mit umfassenden Zugangsberechtigungen der Bequemlichkeit halber eine alte Karte mit voller Nennung des Namens und der Anschrift des Betriebes benutzte.

Aber auch bei einfachsten Zugangssicherungen, z.B. Verschluß von sensiblem Datenmaterial in Tresoren, besonderer Absicherung von Türen und Fenstern, insbesondere bei ebenerdigen Arbeitsräumen, gab es oft Grund, Mängel festzustellen. Insbesondere bei kleineren Betrieben der Datenerfassung wurde hier oft geraten, die Kompetenz der kriminalpolizeilichen Beratungsstellen in Anspruch zu nehmen.

Nach der Neufassung des BDSG bestehen für die Aufsichtsbehörden hier erstmals Möglichkeiten, Auflagen zu erteilen. Fälle, in denen über zwei Jahre um die Verbesserung von Türsicherungen gerungen werden muß, sind nun hoffentlich Vergangenheit.

Eine Besonderheit bilden die nicht seltenen Fälle, bei denen das zu kontrollierende Rechenzentrum aus der ehemaligen Datenverarbeitungsabteilung der Muttergesellschaft hervorgegangen ist und nunmehr als selbständiges Unternehmen geführt wird. Mitarbeiter früherer Nachbarabteilungen werden hier zu Unbefugten, denen grundsätzlich der Zugang verwehrt sein muß. Da sich in einem solchen Fall weder in der Arbeit des Rechenzentrums noch bei den Beschäftigten faktisch etwas geändert hatte, war es hier nötig, die Verantwortlichen von der Notwendigkeit einer Abschottung des Rechenzentrumsbereichs gegenüber der gesamten Umgebung zu überzeugen. In diesem Fall konnte übergangsweise eine Kompromißlösung akzeptiert werden, da innerhalb des Unternehmenskomplexes ein Neubau für den bereits unter Platzmangel leidenden Rechenzentrumsbetrieb geplant war.

14.2 Zugriffskontrolle

Als weiteres schwerwiegendes Problem stellt sich die Verwirklichung der Zugriffskontrolle und damit gleichzeitig der Eingabe- und Speicherkontrolle dar. Der bereits im letzten Tätigkeitsbericht dargestellte Trend insbesondere bei Mängeln der Datenverarbeitung in PC-Netzen hat sich damit auch im Berichtsjahr bestätigt.

Fast bei jeder Prüfung solcher Systeme war die Verwaltung der Passworte ein Problem. Beanstandet wurden so die zum Teil völlig ungeregelte Dauer der Verwendung desselben Passworts, die Weiterverwendung von Passwörtern ausgeschiedener Mitarbeiter, die Bekanntgabe der Passwörter einer ganzen Mitarbeitergruppe. In einem geprüften Einzelfall bestand die Passwortsicherung darin, daß jeder Mitarbeiter der Einfachheit halber dasselbe Passwort benutzte, da das installierte System beim log-in ein Passwort verlangte. Sinn und Zweck des Passwortes wurden damit völlig verfehlt.

Eine Alternative zur Zugriffsicherung per Passwort ist die Verwendung einer Chipkarte in Verbindung mit einer pin (personal identification number). Die Chipkarte ist in der Lage, ein Passwort selbst zu erzeugen und die Anmeldeprozedur zu vereinfachen. Damit ließen sich vermutlich auch Widerstände der Mitarbeiter gegen komplizierte Prozeduren überwinden, die oft zu weniger statt zu mehr Sicherheit führen.

Wie aus den in der Anlage zu § 6 Abs. 1 Satz 1 BDSG a.F. (§ 9 Satz 1 BDSG n.F.) nebeneinander genannten Anforderungen Zugriffskontrolle (Ziffer 1) und Speicher- bzw. Eingabekontrolle (Ziffer 3 bzw. Ziffer 7) zu ersehen ist, kommt es nicht nur darauf an, daß grundsätzlich nur Befugte mit der Datenverarbeitungsanlage arbeiten können, sondern es muß auch nachträglich festgestellt werden können, wer aus dem Kreis der Befugten tätig war. Dies bedingt neben der sicheren Identifikation auch die Authentifikation der Person (siehe hierzu 19. Tätigkeitsbericht des hessischen Datenschutzbeauftragten, Landtagsdrucksache 12/79 51, Ziffer 15.5.1) sowie die Dokumentation dieser Daten. Auch hier waren Schwächen zu verzeichnen. So muß unbedingt eine genaue Dokumentation der vergebenen Zugriffsberechtigungen verlangt werden. Hierfür muß eine

bestimmte Stelle verantwortlich sein. Der Zugriff zu diesen Daten ist streng zu begrenzen. Auch die Kontrolle der Nutzung der Berechtigungen muß verlangt werden. Die Kontrolle sollte vom betrieblichen Datenschutzbeauftragten durchgeführt werden. Häufigkeit und Art solcher Kontrollen geben im übrigen stets auch Hinweise auf Qualifikation und Engagement des betrieblichen Datenschutzbeauftragten.

14.3 Datenträgerverwaltung: Abgangskontrolle – Transportkontrolle

Die Datenträgerverwaltung ist weiterhin besonders bei Betrieben der Datenerfassung problematisch. Es bereitet Schwierigkeiten, die Erkenntnis durchzusetzen, daß alle – auch die nicht benutzten Datenträger – markiert, registriert und laufend verwaltet werden müssen. Dies gilt selbstverständlich auch bei Disketten.

Ein Problem des Eigenschutzes und des Datenschutzes sind die oft von Mitarbeitern privat mitgebrachten Spielprogramme, sowie die bereits festgestellte Praxis besonders eifriger Mitarbeiter, auch noch nach Feierabend mit Disketten aus dem Betrieb zu Hause auf dem privaten PC zu arbeiten. In beiden Fällen besteht die Gefahr, daß Virenprogramme eingeschleppt werden, die zur Gefahr für den gesamten Datenbestand werden können. Dieses Thema wird zwar immer wieder lebhaft erörtert, effektive Schutzmaßnahmen, wie z.B. eine „Viren-Quarantäne-Station", werden von den Unternehmen jedoch nur selten eingeführt. Möglich ist hier, vergleichbar den Datenträgerverwaltungssystemen bei Großrechnern, die notwendige Vorbehandlung (Initialisierung) aller Disketten vor ihrer Verwendung in den PC's des Unternehmens. Bei fremdbeschriebenen Disketten sollten diese nach einer Virenprüfung auf eigene Disketten kopiert werden und die Kopien in die laufende Verarbeitung einbezogen werden.

Für die eigenen Disketten könnten auch kryptographische Verfahren verstärkt genutzt werden. Fremde Datenträger (Disketten) sollten dann nur noch Sicherungszwecken dienen (Beispiel Programmdisketten) bzw. wieder zurückgegeben werden.

14.4 Datenträgervernichtung

Die Vernichtung von Datenträgern wird in vielen Fällen von auf Aktenvernichtung spezialisierten Unternehmen, aber auch von Containerdiensten als Dienstleistung angeboten. Sie ist als eine nach §§ 31 Abs. 1 Satz 1 Ziff. 3, 39 BDSG a.F. (§§ 11 Abs. 1, 32 Abs. 1 Ziff. 3 BDSG n.F.) meldepflichtige Tätigkeit anzusehen.

Während es bei den auf Aktenentsorgung spezialisierten Unternehmen, was die Qualität der Vernichtung betrifft, kaum Beanstandungen gab, waren Beschwerden und Mißstände deutlich häufiger, wenn die Entsorgung bzw. die Auswahl des Auftragnehmers ohne besondere Überlegung vorgenommen wurde. So wurde die Aufsichtsbehörde öfter angesprochen, weil Unterlagen mit zum Teil aus dem intimen bzw. gesundheitlichen Bereich stammenden Daten in Müllcontainern mehr oder weniger öffentlich zugänglich vorgefunden wurden. In keinem einzigen Fall dieser „Müllfunde" wurde jedoch eine Beschwerde eines persönlich Betroffenen bekannt, was nach der bisher geltenden Fassung des BDSG Voraussetzung für eine Überprüfung durch die Aufsichtsbehörde hätte sein müssen. Nur im Bereich der Datenverarbeitung für fremde Zwecke, also im Vierten Abschnitt des bisherigen BDSG (§§ 31 ff.) konnte die Aufsichtsbehörde auch ohne die Beschwerde eines Betroffenen einschreiten. In Zukunft kann nach § 38 BDSG n.F. die Aufsichtsbehörde auch dann die Einhaltung der Vorschriften des BDSG sowie anderer Vorschriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien regeln, überprüfen, wenn ihr hinreichende Anhaltspunkte für eine Verletzung des Datenschutzes vorliegen. Hiervon wird zweifellos gerade in diesen Fällen Gebrauch gemacht werden.

14.5 Beauftragung von Sub-Datenverarbeitungsunternehmen

Auftraggeber sind nach den §§ 22 Abs. 2 bzw. 31 Abs. 2 BDSG a.F. (§ 11 Abs. 1 BDSG n.F.) verpflichtet, den Auftragnehmer nach Eignung sorgfältig auszuwählen.

In geprüften Einzelfällen ließ diese Sorgfalt erheblich zu wünschen übrig. Leider wurden die Auftragnehmer nur in Einzelfällen verpflichtet, weitere Subunternehmen nur nach Kenntnisnahme und mit Genehmigung des Auftraggebers zu beschäftigen. Wo der einzelne Auftrag dann tatsächlich erledigt wird, ist oft zufallsbedingt. Zu raten ist, daß in dem schriftlichen Auftrag der Ort der Verarbeitung möglichst festgelegt wird. Die wünschenswerte Überprüfung durch Rückfrage bei der Aufsichtsbehörde, ob der zukünftige Auftragnehmer nach § 39 BDSG a.F. (§ 32 BDSG n.F.) zum Register gemeldet ist und damit der laufenden Überwachung unterliegt, findet nur in Ausnahmefällen statt.

Bei Prüfungen wurde es bisher schon als positiv bewertet, wenn die Weisungen nach § 37 BDSG schriftlich vorlagen. Das neue BDSG schreibt nun ausdrücklich die schriftliche Erteilung des Auftrages vor (§ 11 Abs. 2 BDSG n.F.), wobei auch die Datenverarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Es ist zu hoffen, daß damit die gröbsten Mißstände beseitigt werden. Nach wie vor besteht jedoch die Gefahr, daß der Auftraggeber weder die betrieblichen Verhältnisse des Auftragnehmers kennt bzw. sich die notwendige Kenntnis hierüber verschafft, noch die Einhaltung seiner Weisungen kontrolliert. Dies ist jedoch dringend erforderlich.

15. Ordnungswidrigkeitsverfahren

Im Berichtsjahr wurden 15 Ordnungswidrigkeitenverfahren eingeleitet, die alle mit einem Bußgeldbescheid rechtskräftig abgeschlossen wurden. Die Mehrzahl der Verfahren betraf – wie in den Vorjahren – die verspätete Abgabe der nach § 39 BDSG erforderlichen Meldungen an die Aufsichtsbehörde (Ordnungswidrigkeit nach § 42 Abs. 1 Nr. 4 BDSG a.F.).

So wurde der Aufsichtsbehörde in elf Fällen die Aufnahme der meldepflichtigen Tätigkeit nicht innerhalb der in § 39 Abs. 1 BDSG a.F. geforderten Monatsfrist gemeldet, sondern die meldepflichtige Geschäftstätigkeit wurde zum Zeitpunkt der Abgabe der Meldung schon seit Jahren ausgeübt.

Zwei weitere dieser Verfahren betrafen die verspätete Abgabe von Änderungsmeldungen gem. § 39 Abs. 3 i.V.m. Abs. 2 BDSG a.F.

In sieben dieser Fälle kam hinzu, daß entgegen § 38 i.V.m. § 28 Abs. 1 BDSG a.F. ein Beauftragter für den Datenschutz nicht oder nicht rechtzeitig bestellt worden war (Ordnungswidrigkeit nach § 42 Abs. 1 Nr. 2 BDSG a.F.).

In einem anderen Fall war der Vertriebsleiter einer Bausparkasse, welcher zuvor bei einer Vermögensberatungsgesellschaft tätig war, von dieser mit dem Datenbestand eines Kunden zu der Bausparkasse gewechselt. Dabei wurde der persönlich Betroffene nicht nach § 26 Abs. 1 BDSG von der erfolgten Datenspeicherung bei der Bausparkasse benachrichtigt (Ordnungswidrigkeit nach § 42 Abs. 1 Nr. 1 BDSG a.F.).

Bei einem weiteren Verfahren war ein meldepflichtiges Unternehmen seiner Auskunftspflicht gegenüber der Aufsichtsbehörde nach § 40 Abs. 2 i.V.m. § 30 Abs. 2 BDSG a.F. nicht nachgekommen (Ordnungswidrigkeit nach § 42 Abs. 1 Nr. 5 BDSG a.F.).

Wiesbaden, den 5. September 1991

Der Hessische Ministerpräsident
Eichel

Der Hessische Minister des Innern
und für Europaangelegenheiten
Dr. Günther