16. Wahlperiode

Drucksache **16/3650**

HESSISCHER LANDTAG

15. 02. 2005

Vorlage
der Landesregierung

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

Vorgelegt mit der Stellungnahme zum Zweiunddreißigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten - Drucks. 16/2131 - nach § 30 Abs. 2 des Hessischen Datenschutzgesetzes in der Fassung vom 7. Januar 1999.

Eingegangen am 15. Februar 2005 · Ausgegeben am 1. März 2005
Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

	Überblick und Statistiken	Seite
1.	Bearbeitung von Datenschutzbeschwerden und sonstige Prüfungen nach § 38 Abs. 1 BDSG	3
1.1	Bearbeitung von aktuellen Eingaben und Beschwerden	3
1.2	Erledigung von Eingaben und Beschwerden aus den Vorjahren	4
1.3	Anlassabhängige Überprüfungen vor Ort nach § 38 Abs. 1 BDSG	5
1.4	Anlassunabhängige Überprüfungen	5
2.	Bearbeitung von Anfragen zu datenschutzrechtlichen Problemstellungen und Beratungstätigkeit	5
2.1	Anfragebearbeitung und datenschutzrechtliche Beratung	5
2.2	Informationsmaterial und Orientierungshilfen	7
3.	Genehmigungsverfahren nach § 4c Abs. 2 BDSG	7
4.	Register der meldepflichtigen Verfahren nach § 4d BDSG	7
5.	Ordnungswidrigkeitenverfahren	8
	Einzelfälle	
6.	Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA)	9
6.1	Prüfung des Scoring-Verfahrens	9
6.2	Transparenz des Scoring-Verfahrens, Nutzung des Score-Wertes durch Vertragspartner	11
6.3	Filtertext bei Widerspruch gegen Score-Berechnung	12
6.4	Erweiterung des Kreises der Vertragspartner der SCHUFA	12
6.5	Personenverwechslungen	13
7.	Banken	14
7.1	Spenden an gemeinnützige Organisationen	14
7.2	Elektronisches Lastschriftverfahren - Datenübermittlung trotz Kontosperre	15
8.	Inkassounternehmen	15
9.	Aspekte internationaler Datenverarbeitungen	16
9.1	Übermittlung von Schuldnerverzeichnisdaten nach Indien	16
9.2	Übermittlung von Fluggastdaten an die Zoll- und Grenzschutzbehörde der USA	18
9.3	Übermittlung von Daten deutscher Wirtschaftsprüfer in die USA	20
10.	Teledienste, Neue Medien, Internet-Provider	22
10.1	Auskunftserteilung auch bei fehlender Verantwortung für die Datenverarbeitung?	22
10.2	Verwendung von Pseudonymen beim Whois-Dienst der DENIC eG	23
10.3	WWW-Veröffentlichungen und Suchmaschinen-Ergebnisse	24
11.	Private Bildungseinrichtungen	25
12.	Weitergabe gebrauchter Mobiltelefone	25
13.	Werbung, Direktmarketing	26
13.1	Leitfaden des Deutschen Direktmarketing-Verbandes (DDV)	26
13.2	Internationalisierung der Werbewirtschaft	27

1. Bearbeitung von Datenschutzbeschwerden und sonstige Prüfungen nach § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG)

1.1 Bearbeitung von aktuellen Eingaben und Beschwerden

Die Aufsichtsbehörden überprüfen nach § 38 Abs. 1 BDSG die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln.

Die Überprüfungen und Kontrollen wurden insbesondere dann vorgenommen, wenn in Beschwerden konkrete Anhaltspunkte für einen Datenschutzverstoß von betroffenen Bürgerinnen und Bürgern selbst darlegt wurden. Teilweise wandten sich auch Unternehmen, Betriebsräte sowie Vereinigungen und Interessenverbände an die Datenschutzaufsichtsbehörden, weil angenommen wurde, dass bestimmte Unternehmen, Vereine usw. gegen datenschutzrechtliche Vorschriften verstoßen hätten. Auch wenn Meldungen in Presse, Fernsehen oder dem Internet auf einen Verstoß gegen datenschutzrechtliche Vorschriften hindeuteten, gingen die Datenschutzaufsichtsbehörden diesen Hinweisen nach.

Im Berichtsjahr wurden von den Aufsichtsbehörden 540 Fälle überprüft, in denen von nicht öffentlichen Stellen Datenverarbeitungen nach § 28 BDSG für die Erfüllung eigener Geschäftszwecke betrieben oder personenbezogene Daten nach §§ 29, 30 BDSG zur personenbezogenen oder anonymisierten Übermittlung gespeichert und genutzt wurden.

Im Vergleich zum Vorjahr (421 Fälle) hat sich damit die Zahl der Eingaben und Beschwerden um 119 Fälle (28 v.H.) erhöht.

Die telefonischen Beratungen wurden dabei bis auf wenige Ausnahmen nicht erfasst, ebenso wie Anfragen, die durch die Versendung von Informationsmaterial und Orientierungshilfen erledigt werden konnten, was zunehmend auch schnell und einfach per Internet bzw. per E-Mail mit entsprechenden Dateianhängen geschieht.

Die 540 Überprüfungen aufgrund von Eingaben, Beschwerden und Pressemeldungen durch die Aufsichtsbehörden betrafen:

- in 131 Fällen die Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA),
- in 95 Fällen Teledienstеanbieter (Anbieter von Internetzugängen, -diensten und -inhalten, unverlangte E-Mail-Werbung),
- in 48 Fällen Banken, Kreditinstitute und EDV-Dienstleister im Zahlungsverkehr,
- in 45 Fällen Stellen und Unternehmen der Direktmarketing- und Werbewirtschaft,
- in 39 Fällen Handels- und Wirtschaftsauskunfteien,
- in 33 Fällen den Datenschutz in Arbeitsverhältnissen und bei Arbeitsvermittlern,
- in 21 Fällen Inkassounternehmen,
- in 21 Fällen Unternehmen der Freizeit-, Touristik- und Reisebranche,
- in 15 Fällen Unternehmen des Groß- und Einzelhandels,
- in 14 Fällen das Gesundheitswesen (Apotheken, Ärzte, Krankenhäuser, Senioren- und Pflegeheime),
- in 11 Fällen Versicherungsgesellschaften,
- in 9 Fällen Unternehmen der Versandhandelsbranche,
- in 9 Fällen die Videoüberwachung von Grundstücken, Häusern und Wohnungen,
- in 8 Fällen Vereine (Sport, Soziales, Kultur) sowie deren Landes- und Bundesverbände,
- in 7 Fällen Adresshandelsunternehmen,
- in 6 Fällen Kreditkartenunternehmen,
- in 5 Fällen Vermieter sowie Wohnungs- und Immobilienverwaltungsfirmen,

- in 5 Fällen Anwaltskanzleien,
- in 3 Fällen politische Parteien,
  in 3 Fällen Verlage und Presse,
- in 12 Fällen sonstige Stellen (z.B. Soft- und Hardwarehersteller, Verkehrsunternehmen).

Bei ca. 25 v.H. der Beschwerden konnte zeitnah festgestellt werden, dass diese begründet waren. In insgesamt 136 Fällen wurden bei den Nachforschungen der Aufsichtsbehörde unzulässige Verarbeitungen personenbezogener Daten und andere Verstöße gegen Vorschriften des allgemeinen Datenschutzrechts und des Datenschutzrechts der Tele- und Mediendienste festgestellt, die zu Beanstandungen der jeweiligen Verarbeitungsverfahren bei den betroffenen Stellen führten.

Die bei den Überprüfungen beanstandeten 136 Verstöße gegen Datenschutzbestimmungen wurden festgestellt:

- in 36 Fällen bei der Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA), davon in 15 Fällen Verstoß durch den Vertragspartner der SCHUFA,
- in 16 Fällen bei Kreditinstituten und Banken,
- in 14 Fällen bei Anbietern von Tele- und Mediendiensten (Access- und Content-Provider und Versendern von Werbe-E-Mails),
- in 12 Fällen bei Inkassounternehmen,
- in 11 Fällen bei der Verarbeitung von Arbeitnehmer- und Bewerberdaten,
- in 9 Fällen bei Unternehmen der Direktmarketing- und Werbebranche,
- in 5 Fällen bei Handels- und Wirtschaftsauskunfteien,
- in 5 Fällen bei Unternehmen der Freizeit-, Touristik- und Reisebranche,
- in 4 Fällen bei Adresshändlern,
- in 4 Fällen bei Groß- und Einzelhandelsunternehmen,
- in 3 Fällen bei Gewerbebetrieben,
- in 3 Fällen im Gesundheitssektor (Arzt, Krankenhaus),
- in 3 Fällen in der Versandhandelsbranche,
- in 3 Fällen bei Versicherungsgesellschaften,
- in 2 Fällen im Wohnungswesen (Vermieter, Immobilienmakler),
- in 2 Fällen bei Anwaltskanzleien
- sowie in jeweils einem Fall bei einer Videoüberwachung, einem Kreditkartenunternehmen, einer politischen Partei und einem Telekommunikationsunternehmen.

Ein Teil der eingeleiteten Überprüfungen konnten im Berichtsjahr noch nicht abgeschlossen werden und wird in den nächsten Tätigkeitsbericht einfließen.

1.2 Erledigung von Eingaben und Beschwerden aus den Vorjahren

Von den noch aus den Vorjahren anhängigen Beschwerden, die oftmals sehr vielschichtige Verarbeitungszusammenhänge betrafen, wurden im Berichtsjahr 103 Fälle abgeschlossen. Die Beurteilung dieser in der Regel nur mit hohem Ermittlungsaufwand aufklärbaren Eingaben durch die Aufsichtsbehörden ergab, dass davon 53 Eingaben begründet waren. Die Aufsichtsbehörden mussten also in mehr als 50 v.H. dieser Fälle einen Datenschutzverstoß feststellen.

Die beanstandeten 53 Verstöße gegen Datenschutzbestimmungen wurden festgestellt:

- in 14 Fällen bei Anbietern von Telediensten (Internetprovidern),
- in 7 Fällen bei Banken,
- in 6 Fällen bei Arbeitgebern und Arbeitsvermittlern,
- in 4 Fällen bei Unternehmen der Werbewirtschaft und werbenden Einzelhändlern,
- in 4 Fällen bei eingetragenen Vereinen und Verbänden,
- in 4 Fällen bei Handels- und Wirtschaftsauskunfteien,

- in 4 Fällen im Gesundheitswesen,
- in 2 Fällen bei Unternehmen des Groß- und Einzelhandels,
- in 2 Fällen bei Video-Beobachtung öffentlich zugänglicher Räume
- sowie in jeweils einem Fall bei einer Versicherung, einem Kreditkartenunternehmen, einem Adresshändler, einer Videothek, einem Hotel und einem Vermieter.

1.3 Anlassabhängige Überprüfungen vor Ort nach § 38 Abs. 1 BDSG

Bei den im Berichtsjahr insgesamt durchgeführten Prüfungen aufgrund von Eingaben, Beschwerden und Hinweisen auf Datenschutzverstöße (s.o. Nr. 1.1 und 1.2) bestand in 16 Fällen Veranlassung für eine Überprüfung vor Ort. Nur auf diese Weise ließ sich zuverlässig feststellen, ob ein Datenschutzverstoß vorlag.

Die Prüfdauer variierte dabei - je nach Komplexität der Datenverarbeitung und der Schwere des Vorwurfs - von kurzen ein- bis zweistündigen Prüfungen bis zu ganztätigen Prüfungen, Vor- und Nachbereitungszeit nicht eingerechnet.

1.4 Anlassunabhängige Überprüfungen

Im Berichtsjahr wurden 12 anlassunabhängige Kontrollen durchgeführt. Diese betrafen folgende Branchen/Bereiche:

- Videoüberwachungssysteme 4
- Handels- und Gewerbeunternehmen 3
- Ärztliche Praxen/Kliniken/Laboratorien 2
- Public-Relations-Unternehmen 1
- Konzerndatenverarbeitungsdienstleister 1
- Auskunfteien 1

Die Prüfungen wurden vor Ort in den Unternehmen durchgeführt. Bei allen Überprüfungen waren Beanstandungen auszusprechen. Dabei wurden die folgenden wesentlichen Mängel am häufigsten festgestellt:

- Mängel in den Bereichen der Datensicherheit, z.B. fehlende Zugriffsregelungen, Versenden von E-Mails mit Anhängen mit vertraulichen Daten ohne Verschlüsselung, fehlende Vorsorge zur Verfügbarkeit der Daten, mangelnde Dokumentation, fehlende Protokollierung,
- Mängel bei der Fachkunde der betrieblichen Datenschutzbeauftragten,
- Voraussetzungen des § 6b Abs. 1, Abs. 2 BDSG nicht erfüllt,
- fehlende Weisungen nach § 11 BDSG,
- Mängel in der Verpflichtung auf das Datengeheimnis nach § 5 BDSG.

Neben den dargestellten 12 anlassunabhängigen Prüfungen wurden auch die 16 Überprüfungen aus konkretem Anlass (s.o. Nr. 1.3 des Berichtes) überwiegend dazu genutzt, um die Datenverarbeitung der verantwortlichen Stellen umfassender zu prüfen. Die Prüfungen wurden also nicht nur auf den konkreten Beschwerdegegenstand beschränkt.

Häufig musste festgestellt werden, dass Datensicherheitsmängel bestanden, Weisungen nach § 11 BDSG fehlten und dass bei der Bestellung des Datenschutzbeauftragten nicht auf die erforderliche Fachkunde geachtet worden war.

In den Fällen der Videoüberwachung von öffentlich zugänglichen Bereichen musste festgestellt werden, dass die Maßnahme weder zur Wahrnehmung des Hausrechtes noch zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich war. In anderen Fällen lagen zwar die Voraussetzungen des § 6b Abs. 1 BDSG vor, aber die Kennzeichnungspflicht des § 6b Abs. 2 BDSG wurde missachtet.

2. Bearbeitung von Anfragen zu datenschutzrechtlichen Problemstellungen und Beratungstätigkeit

2.1 Anfragebearbeitung und datenschutzrechtliche Beratung

Im Berichtsjahr 2003 ging bei den Aufsichtsbehörden erneut eine große Zahl von Anfragen und Beratungsersuchen ein. Davon wurden 187 Fälle statistisch erfasst, in denen die Beratung und Information insbesondere von Unternehmen,

Vereinen und Verbänden, Arbeitnehmerinnen und Arbeitnehmern sowie Betriebsräten aktenmäßig erfolgte. Die direkte telefonische Erledigung von Anfragen sowie die Übersendung von Informationsmaterial und Orientierungshilfen per E-Mail wurden bis auf wenige Ausnahmen nicht statistisch erfasst.

Die Auswertung der 187 Fälle ergab folgende inhaltlichen Schwerpunkte:

34 Anfragen von und zum betrieblichen Datenschutzbeauftragten
Fragen zur korrekten Bestellung, Bußgeld wegen Nichtbestellung, Aufgaben des betrieblichen Datenschutzbeauftragten, betriebliche Umsetzung des BDSG, Schulung, Vorabkontrolle nach § 4d Abs. 5 BDSG, Verfahrensverzeichnis nach § 4g Abs. 2 BDSG, Auftragsdatenverarbeitung nach § 11 BDSG.

26 Anfragen zum Datenschutz im Internet
Whois-Dienste (siehe Nr. 10.2), Speicherung von Log-Dateien, Spam-E-Mails, Viren und Würmer, Sicherheitsfragen, Datenschutzhinweise in WWW-Angeboten, Opt-In-Verfahren für online erhobene E-Mail-Adressen, unzulässiger Handel mit E-Mail-Adressen.

18 Anfragen zur Auslandsdatenverarbeitung
Datentransfer innerhalb der Europäischen Union, insbesondere zur Frage des anwendbaren Rechts, vor allem aber Fragen zur Datenübermittlung an so genannte "Drittstaaten", also Staaten außerhalb der Europäischen Union und des Abkommens über den Europäischen Wirtschaftsraum, vorwiegend im Zusammenhang mit dem Transfer von Arbeitnehmerdaten an die außereuropäische Muttergesellschaft innerhalb eines Konzerns, Fragen zur Auslagerung von Datenverarbeitungen an Datenverarbeitungsdienstleister in Drittstaaten (siehe Nr. 9.1) und zur Weitergabe von Daten an amerikanische Behörden (siehe Nr. 9.2 und 9.3).

16 Anfragen zur SCHUFA
Grundsätzliches zur Arbeitsweise der SCHUFA und ihrer Vertragspartner, die bei den Anfragern weitgehend unbekannt war.

15 Anfragen zum Arbeitnehmerdatenschutz
Private Nutzung von betrieblichen E-Mail- und Internet-Anschlüssen, Betriebsvereinbarungen, Umgang mit Bewerberdaten, Rücksendung von Bewerbungsunterlagen bei Ablehnung.

12 Anfragen aus dem Gesundheitssektor
Umfang der ärztlichen Schweigepflicht, Entbindung vom Arztgeheimnis, Übermittlung von Patientendaten an eine Krankenversicherung, Weitergabe von Gesundheitsdaten an den TÜV zur Qualitätssicherung nach der Röntgenverordnung, Auswertung anonymisierter Patientendaten für die Marktforschung.

10 Anfragen zur Videoüberwachung
Beobachtung von Grundstückszufahrten, Wohnanlagen, Hausfluren und Treppenhäusern, Fragen zur Ausgestaltung des nach § 6b Abs. 2 BSDG erforderlichen Hinweises, zu Löschungsfristen, auch zur Zulässigkeit der Patientenkontrolle mittels Videoüberwachung im Sozial- und Gesundheitsbereich.

8 Anfragen zum Datenschutz bei Banken
Werbliche Nutzung von Bankverbindungsdaten, Fusion von Banken, Formulierung von Einwilligungserklärungen, Fragen zu datenschutzrelevanten Bestimmungen des Kreditwesengesetzes, Übermittlung der Daten von Spendern an gemeinnützige Organisationen (siehe Nr. 7.1).

7 Anfragen zur Werbewirtschaft
Informationen über die grundsätzliche Zulässigkeit des Adresshandels im Rahmen der §§ 28, 29 BDSG, Beratung zum Recht auf Auskunftserteilung und Informationen zum Werbewiderspruch nach § 28 Abs. 4 BDSG sowie zur Löschung bzw. Sperrung von Daten, Informationen zu datenschutzrechtlichen Aspekten von Kundenbindungs- und Rabattkartensystemen sowie zum Telefonmarketing.

7 Anfragen zur Datenverarbeitung durch Vereine und Dachverbände
Veröffentlichung von Mitgliederdaten und -bildern im Internet, Fragen zur werblichen Nutzung von Mitgliederdaten und zur Übermittlung an Wirtschaftsunternehmen sowie zur Errichtung einer zentralen Mitgliederdatenbank, Anfragen zum Datenschutz und zur Datensicherheit bei Homepages von Vereinen im WWW, Beratung bei der Durchführung einer Mitgliederbefragung.

Die weiteren Anfragen und Beratungsersuchen, die mit ihrem breiten Spektrum sehr anschaulich widerspiegeln, dass Datenschutzaspekte heute in fast

jedem Lebensbereich auftauchen, betrafen unter andrem die Meldepflicht nach §§ 4d, 4e BDSG sowie die Bereiche Datensicherheit, Miete und Wohnen, Markt- und Meinungsforschung, die Reise- und Touristikbranche, den Versandhandel, Inkassounternehmen und Handels- und Wirtschaftsauskunfteien.

2.2 Informationsmaterial und Orientierungshilfen

Das Angebot an Informationsmaterial, das die Datenschutzaufsichtsbehörde beim Regierungspräsidium Darmstadt zu unterschiedlichsten Fragestellungen des Datenschutzrechts bereithält, wurde auch im Berichtsjahr wieder gut angenommen. Zum einen wird mit den Hinweisen und Merkblättern die praktische Arbeit der betrieblichen Datenschutzbeauftragten in den Unternehmen unterstützt, zum anderen interessieren sich auch viele Bürgerinnen und Bürger dafür, welche datenschutzrechtlichen Ansprüche sie gegenüber verarbeitenden Stellen haben und wie diese durchgesetzt werden können.

Auch die Homepage des Datenschutzdezernates beim Regierungspräsidium Darmstadt im WWW (http://www.rpda.de/dezernate/datenschutz), über die Mustertexte, Meldeformulare sowie Merk- und Hinweisblätter abgerufen werden können, erfreut sich großer Beliebtheit und unterstützte die Beratungs- und Informationsfunktion der Datenschutzaufsichtsbehörden wesentlich.

3. Genehmigungsverfahren nach § 4c Abs. 2 BDSG

Im Berichtsjahr gingen zwei Anträge auf Genehmigung des Datentransfers in die USA und andere außereuropäische Staaten ein. Beide Anträge bezogen sich auf den Austausch von Mitarbeiterdaten innerhalb international tätiger Konzerne.

Im einen Fall beabsichtigte ein Pharmakonzern eine spezielle Mitarbeiterdatenbank zu errichten, um die weltweiten Forschungsprojekte zu koordinieren. Diese Koordinierungsaufgabe wurde einer Tochtergesellschaft in den USA zur eigenverantwortlichen Erledigung übertragen. Zu diesem Zweck wurde ein Vertrag entworfen, der sich an dem EU-Standardvertrag vom 15. Juni 2001 orientiert.

In intensiver Abstimmung mit der Aufsichtsbehörde wurden insbesondere die Anlagen zum Vertrag, in denen die komplexe Datenverarbeitung und die Zugriffsbeschränkungen beschrieben wurden, überarbeitet.

Nach anschließender Abstimmung in der Arbeitsgruppe "Internationaler Datenverkehr" des Düsseldorfer Kreises konnte im Jahr 2004 die Genehmigung erteilt und dem Bundesministerium des Innern zugeleitet werden. Das Bundesministerium des Innern wird die EU-Kommission und die anderen EU-Mitgliedstaaten entsprechend Art. 26 Abs. 3 EG-Datenschutzrichtlinie unterrichten.

Im anderen Fall hatte ein Konzern ein global ausgerichtetes Personalinformationssystem eingeführt. Hierzu wurden eine Konzernbetriebsvereinbarung und eine Datenschutzvereinbarung zwischen der deutschen Konzernzentrale und den globalen Koordinationsstellen für die Auslandsregionen getroffen. Die deutsche Muttergesellschaft bat um Bestätigung, dass damit die Voraussetzungen des § 4b Abs. 2 und 3 BDSG (angemessenes Datenschutzniveau) erfüllt seien. Alternativ bat sie um Genehmigung nach § 4c Abs. 2 BDSG. Aufgrund der Beratung durch die Aufsichtsbehörde wurden die Unterlagen überarbeitet, sodass im nächsten Tätigkeitsbericht über die abschließende Bewertung zu berichten sein wird.

4. Register der meldepflichtigen Verfahren nach § 4d BDSG

Die Aufsichtsbehörden führen nach § 38 Abs. 2 BDSG ein Register der nach § 4d BDSG meldepflichtigen automatisierten Verarbeitungen.

Im Laufe des Berichtsjahres wurden sieben Verfahren aus dem Melderegister gelöscht, weil die Unternehmen die meldepflichtige Tätigkeit aufgegeben hatten und eines neu eingetragen.

Am Ende des Berichtsjahres waren 87 Verfahren von 85 verantwortlichen Stellen im Melderegister eingetragen. Wie sich aus diesen Zahlen ergibt, haben nur zwei verantwortliche Stellen mehr als ein Verfahren gemeldet. Davon werden in 38 gemeldeten Verfahren geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung gespeichert (Adresshändler, Han-

dels- und Wirtschaftsauskunfteien, meldepflichtig nach § 4d Abs. 4 Nr. 1 BDSG). 49 der eingetragenen Verfahren dienen dem Zwecke der anonymisierten Übermittlung (Markt- und Meinungsforschung, meldepflichtig nach § 4d Abs. 4 Nr. 2 BDSG).

5. Ordnungswidrigkeitenverfahren

Im Berichtsjahr wurden vom Regierungspräsidium Darmstadt acht Verfahren nach dem Gesetz über Ordnungswidrigkeiten (OWiG) eingeleitet. Die Verfahren bezogen sich auf:

Grund:	**nach § 43**	**Rechtskraft:**	**Bußgeld**
Nichterteilung von Auskünften	Abs. 1 Nr. 10 BDSG	Ja	500 €
Nichterteilung von Auskünften	Abs. 1 Nr. 10 BDSG	Ja	1.000 €
Nichterteilung von Auskünften	Abs. 1 Nr. 10 BDSG	Ja	250 €
Nichtduldung einer Maßnahme	Abs. 1 Nr. 10 BDSG	Ja	800 €
Nichterteilung von Auskünften	Abs. 1 Nr. 10 BDSG	Nein	-
Nichtduldung einer Maßnahme	Abs. 1 Nr. 10 BDSG	Nein	-
Kein Datenschutzbeauftragter	Abs. 1 Nr. 2 BDSG	Ja	1.000 €
Unbefugte Verarbeitung	Abs. 2 Nr. 1 BDSG	Ja	2.000 €

In einem dieser Verfahren, das nach § 43 Abs. 1 Nr. 10 BDSG gegen einen gerichtlich bestellten Bausachverständigen wegen der Erteilung falscher Auskünfte an die Aufsichtsbehörde entgegen § 38 Abs. 3 Satz 1 BDSG eingeleitet wurde, hatte der von dem Beschuldigten eingelegte Einspruch Erfolg. Das zuständige Amtsgericht Darmstadt stufte die Schuld des Beschuldigten als gering ein und stellte das Verfahren nach § 47 Abs. 2 OWiG ein.

In einem weiteren Fall war der Eigentümer eines Mietshauses nicht zum angekündigten Ortstermin zur Überprüfung seiner Videoüberwachungsanlage erschienen, was zur Einleitung eines Bußgeldverfahrens wegen der Nichtduldung einer aufsichtsbehördlichen Maßnahme entgegen § 38 Abs. 4 Satz 1 BDSG nach § 43 Abs. 1 Nr. 10 führte. Infolge des Einspruchs des Beschuldigten gegen den erlassenen Bußgeldbescheid wurde das Verfahren zur Entscheidung an das Amtsgericht Darmstadt abgegeben. Das Gericht entschied, das Ordnungswidrigkeitsverfahren einzustellen und den Bußgeldbescheid aufzuheben, da nicht zweifelsfrei nachgewiesen werden könne, dass dem Hausbesitzer die Terminmitteilungen zur Überprüfung seiner Überwachungsanlage tatsächlich zugegangen seien.

In den sechs anderen durchgeführten Verfahren haben die erlassenen Bußgeldbescheide zwischenzeitlich Rechtskraft erlangt.

Die Verfahren gegen die Geschäftsführer von drei Daten verarbeitenden GmbH aus unterschiedlichen Branchen mit einer Bußgeldsummer von 1.750 € wurden zur Durchsetzung der Auskunftsansprüche der Aufsichtsbehörde nach § 38 Abs. 3 Satz 1 BDSG durchgeführt, nachdem die Erinnerungen an die Beantwortung der Fragen der Aufsichtsbehörde zuvor keinen Erfolg hatten. Nach Durchführung dieser Bußgeldverfahren wurden alle aufsichtsbehördlichen Fragen umgehend und detailliert beantwortet.

In einem Fall war der Geschäftsführer einer Vermögensverwaltungsgesellschaft nicht bereit, bei der angekündigten Überprüfung seiner Datenverarbeitung hinreichend mitzuwirken. Da ihm kein Zugang zu den Geschäftsräumen gewährt wurde, konnte ein Außendienstmitarbeiter der Aufsichtsbehörde die beabsichtigte datenschutzrechtliche Kontrolle nicht durchführen und musste den Ort unverrichteter Ding wieder verlassen. Gegen den Geschäftsführer wurde ein Bußgeldverfahren wegen der Nichtduldung einer aufsichtsbehördlichen Maßnahme entgegen § 38 Abs. 4 Satz 1 BDSG nach § 43 Abs. 1 Nr. 10 eingeleitet. Der Bußgeldbescheid in Höhe von 800 € ist inzwischen rechtskräftig, da der eingelegte Einspruch des Beschuldigten vom zuständigen Amtsgericht nach § 74 Abs. 2 OWiG verworfen wurde.

Ein kleines Dienstleistungsunternehmen aus der Datenverarbeitungsbranche wurde bereits vor Jahren im Rahmen einer Überprüfung darauf hingewiesen, dass es gesetzlich verpflichtet ist, einen betrieblichen Datenschutzbeauftragten zu bestellen. Bei einer anlässlich einer berechtigten Betroffeneneingabe durchgeführten Überprüfung des Unternehmens im Berichtsjahr wurde allerdings festgestellt, dass die Mitarbeiterin, die damals zur betrieblichen Datenschutzbeauftragten bestellt wurde, in der Zwischenzeit weder die nach § 4f

Abs. 2 BDSG erforderliche Fachkunde erworben hatte noch den gesetzlichen Aufgaben eines betrieblichen Datenschutzbeauftragten nachgekommen war. Sie kannte weder die rechtlichen Grundlagen des BDSG noch hatte sie überhaupt irgendeine Tätigkeit als Datenschutzbeauftragte entfaltet. Überprüfbare schriftliche Unterlagen dieser betrieblichen Datenschutzbeauftragten über ihre Tätigkeit und Aufgabenwahrnehmung konnten nach mehr als fünf Jahren in dieser Stellung nicht vorgelegt werden. Sie war in dieser Funktion offensichtlich komplett untätig. Eine inhaltliche Aufgabenerfüllung wurde ihr von der verantwortlichen Unternehmensleitung auch nicht abgefordert. Der Einspruch gegen den Bußgeldbescheid über 1.000 € gegen den Geschäftsführer nach § 43 Abs. 1 Nr. 2 BDSG wurde von den Bevollmächtigten des Unternehmens nach Akteneinsicht zurückgenommen, da die Aktenlage den Verstoß eindeutig belegen konnte.

Das Bußgeld zeigte Wirkung, denn bei der darauf erfolgenden Kontrolle konnte die Aufsichtsbehörde feststellen, dass die betriebliche Datenschutzbeauftragte an einem Qualifizierungsseminar teilgenommen und ihre gesetzlichen Aufgaben in Angriff genommen hatte (Erstellung eines Verfahrensverzeichnisses, Verpflichtung der Mitarbeiter auf das Datengeheimnis nach § 5 BDSG und Schulung der Mitarbeiter, Erarbeitung eines Datensicherheitskonzeptes).

Durch den Anruf einer Passantin wurde die Datenschutzaufsichtsbehörde auf eine Zahnärztin aufmerksam gemacht, die eine große Anzahl von Karteikarten aus dem Archiv der Arztpraxis mit personenbezogenen Patientendaten in der offenen und für Anwohner und Passanten frei zugänglichen Altpapiermülltonne entsorgen wollte, anstatt die Unterlagen einer datenschutzgerechten Vernichtung durch einen Datenträgervernichtungsbetrieb zuzuführen. Die Unterlagen wurden mithilfe der Polizei umgehend sichergestellt.

Die Inhaberin der Arztpraxis hatte mit ihrem Verhalten die Gesundheitsdaten der Patientinnen und Patienten einer unbekannten Anzahl unbefugter dritter Personen übermittelt (§ 3 Abs. 4 Nr. 3 BDSG) und dabei eine unrechtmäßige Nutzung oder Einsichtnahme billigend in Kauf genommen. Die Datenschutzaufsichtsbehörde leitete deshalb ein Bußgeldverfahren nach § 43 Abs. 2 Nr. 1 BDSG gegen die Ärztin ein, da diese durch das Einbringen der Patientenunterlagen im frei zugänglichen Altpapiermüll ohne Rechtsgrundlage und damit unbefugt personenbezogene Daten im Sinne des BDSG verarbeitete. Gegen das verhängte Bußgeld in Höhe von 2.000 € wurde zunächst Einspruch erhoben. Als sich für die Zahnärztin abzeichnete, dass das Gericht den Verstoß für sehr gravierend hielt und eher zu einem deutlich höheren Bußgeld neigte, wurde der Einspruch aber noch vor der Gerichtsverhandlung zurückgenommen.

Obwohl das Regierungspräsidium Darmstadt als Datenschutzaufsichtsbehörde immer wieder Verstöße gegen die Bestimmungen des BDSG und anderer datenschutzrechtlicher Regelungen feststellen musste, blieb die Einleitung von Verfahren nach dem Gesetz über Ordnungswidrigkeiten auch im Jahr 2003 die Ausnahme. Der weitaus überwiegende Teil der Daten verarbeitenden Stellen war bemüht, die festgestellten Fehler bei der Verarbeitung personenbezogener Daten zu beseitigen und die beanstandeten Verarbeitungen und Geschäftsprozesse unverzüglich datenschutzgerecht entsprechend den Anregungen und Hinweisen der Aufsichtsbehörde auszugestalten.

Das Regierungspräsidium Gießen hat im Berichtsjahr zwei Verfahren nach dem Gesetz über Ordnungswidrigkeiten betrieben. Ein Verfahren musste wegen fehlender örtlicher Zuständigkeit an eine andere Aufsichtsbehörde abgegeben werden, das zweite Verfahren war bei Redaktionsschluss dieses Berichts noch in der Bearbeitung.

Das Regierungspräsidium Kassel hat im Berichtsjahr keine Verfahren nach dem Gesetz über Ordnungswidrigkeiten eingeleitet. Soweit bei den Überprüfungen Verstöße gegen das Bundesdatenschutzgesetz festgestellt wurden, konnte aufgrund des einsichtigen Verhaltens der betroffenen Stellen nach Hinweisen auf die Rechtslage von der Einleitung von Ordnungswidrigkeitenverfahren abgesehen werden.

Einzelfälle

6. Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA)

6.1 Prüfung des Scoring-Verfahrens

Die SCHUFA hat durch das Statistische Beratungslabor am Institut für Statistik der Ludwig-Maximilian-Universität München ein Gutachten zur Wissenschaftlichkeit des SCHUFA-Scoring-Verfahrens (vgl. bereits 15. Bericht

der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, LT-Drucks. 15/4659, Nr. 10.2, und 16. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, LT-Drucks. 16/1680, Nr. 10.1) erstellen lassen.

Die Wissenschaftlichkeit eines Scoring-Verfahrens ist zwar keinesfalls alleiniger Maßstab für die datenschutzrechtliche Bewertung, sie ist jedoch durchaus von Bedeutung.

Wenn Scoring-Verfahren, die jeglicher wissenschaftlicher Grundlage entbehren und damit einer "Kaffeesatzleserei" gleichkommen, eingesetzt werden, um automatisierte Entscheidungen zu treffen, oder wenn sie ein erhebliches Gewicht für Entscheidungen haben, die den Betroffenen erheblich beeinträchtigen, dann besteht Grund zur Annahme, dass die schutzwürdigen Belange des Betroffenen gegenüber dem Interesse des Unternehmens an der Nutzung der Score-Werte überwiegen.

Die Aufsichtsbehörde führte deshalb eine Prüfung des Scoring-Verfahrens bei der SCHUFA durch und ließ sich dabei die Ergebnisse des Gutachtens von dessen wissenschaftlich verantwortlichem Verfasser erläutern. Im Anschluss an die Prüfung bat die Aufsichtsbehörde die SCHUFA um eine Kurzfassung des Gutachtens, die daraufhin durch das Statistische Beratungslabor erstellt und an die Mitglieder des Düsseldorfer Kreises verteilt wurde.

Die Gutachter kamen zu dem Ergebnis, dass das Scoring-Verfahren der SCHUFA wissenschaftlichem Standard entspricht. Dies betrifft sowohl die Auswahl des Verfahrens als auch dessen Durchführung. Das bei der Erstellung der Score-Karten verwendete Verfahren wird als "logistische Regression" bezeichnet und ist eine fundierte, seit langem praxiserprobte mathematisch-statistische Methode zur Prognose von Risikowahrscheinlichkeiten, die auch in der Ökonomie und der Medizin verwendet wird. Das Deutsche Krebsforschungszentrum in Heidelberg beabsichtigt beispielsweise, eine epidemiologische Studie zu Wachstum und Ausbreitung von Brustkrebs mithilfe des logistischen Regressionsmodells durchzuführen, die zur Verbesserung der Früherkennung und Behandlung von Brustkrebs dienen soll.

Das Verfahren der logistischen Regression hat aus wissenschaftlicher Sicht keinen "Black-Box"-Charakter, im Gegensatz zur Methodik der neuronalen Netze.

Eine Score-Ermittlung erfolgt nur, wenn zum Betroffenen keine Negativdaten vorliegen oder allenfalls solche Negativdaten gespeichert sind, die mindestens seit einem Jahr erledigt sind. Die SCHUFA-Score-Broschüre ist insoweit etwas missverständlich, denn danach erfolgt eine Score-Ermittlung nur, wenn sich der Kreditinteressent "bei anderen Geschäften bisher stets vertragstreu verhalten hat". Die Broschüre wird von der SCHUFA überarbeitet werden.

Für die Ermittlung des Score-Werts werden durch anonymisierte Auswertung der im SCHUFA-Datenbestand gespeicherten Daten Gruppenprofile erstellt, aus denen sich ableiten lässt, bei welcher Personengruppe mit zunächst positivem Datenbestand sich in der Vergangenheit welches Kreditausfallrisiko realisiert hat. Diese personengruppenbezogenen Vergangenheitswerte werden als Prognose auf die Zukunft übertragen, wobei davon ausgegangen wird, dass sich dieselbe Personengruppe auch in Zukunft gleich verhalten wird. Da das Kreditausfallrisiko ganz unterschiedlich sein kann, je nachdem, um welche Geschäfte mit kreditorischem Risiko es sich handelt, wird beim Scoring-Verfahren auch entsprechend differenziert, indem für verschiedene Branchen (z.B. Banken, Handelsunternehmen, Telekommunikationsunternehmen) eine separate Score-Berechnung erfolgt.

Bei der Entwicklung der Score-Karten werden diejenigen Parameter (Merkmale) herausgesucht, die am besten zu den beobachteten Ausfallrisiken passen, die also die größte Relevanz für die Prognose besitzen.

Bei der konkreten Score-Berechnung wird eine Auswahl aus den Merkmalen, die zu der betreffenden Person gespeichert und aus der Eigenauskunft ersichtlich sind, verwendet. Soweit für die Score-Karten und die Score-Berechnung zusätzliche Merkmale gebildet werden, erfolgt dies durch Kategorisierung und Transformation. Zum Beispiel wird das zusätzliche Merk-

mal "Anzahl der offenen Kredite" aus der Summe der Eintragungen von offenen Krediten gebildet. Die Merkmale beinhalten damit keine neuen, zusätzlichen Angaben gegenüber den aus der Eigenauskunft ersichtlichen.

Im Rahmen der Prüfung wurden der Aufsichtsbehörde die Faktoren (Parameter) mehrerer Score-Karten genannt.

Dabei hat die SCHUFA ausdrücklich bestätigt, dass derzeit nicht genutzt werden:

- die Einholung von Selbstauskünften,
- bestrittene Daten, auch nicht das Merkmal "bestrittene Daten in Prüfung",
- die Ausübung sonstiger datenschutzrechtlicher Rechte des Betroffenen, z.B. Berichtigung, Löschung; wenn Betroffene derartige Rechte geltend machen, wird dies zwar von der SCHUFA beachtet, aber die Tatsache der Geltendmachung als solche wird nicht im SCHUFA-Datensatz des Betroffenen gespeichert,
- Adresse; das SCHUFA-Scoring enthält keine soziodemographischen Komponenten, es wird also beispielsweise nicht ermittelt und nicht berücksichtigt, ob die Adresse dem sozialen Wohnungsbau zuzuordnen ist,
- Nationalität; wird als solche ohnehin nicht gespeichert, wäre evtl. aber aus dem Geburtsort ableitbar, dies geschieht jedoch nicht (vgl. bereits 16. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, LT-Drucks. 16/1680, Nr. 10.1).

Es erfolgt eine dauernde Kontrolle (permanentes Monitoring) anhand der tatsächlichen Entwicklung des Datenbestands. Mithilfe von Ex-post-Analysen lässt sich die Richtigkeit der Prognose überprüfen. Aufgrund des Monitorings werden also eine Validierung und gegebenenfalls auch eine Anpassung der Score-Karten, soweit dies beispielsweise aufrund der Änderung der wirtschaftlichen Gegebenheiten oder Verhaltensweisen der Menschen erforderlich ist, durchgeführt. Dadurch wird sichergestellt, dass die Score-Karten auch unter sich ändernden wirtschaftlichen Bedingungen ihre Gültigkeit behalten.

Das von der Aufsichtsbehörde nach der Prüfung um Stellungnahme gebetene Statistische Bundesamt erklärte, dass gegen das Gutachten aus theoretischer Sicht keine Einwände bestünden. Die Darstellung und Schlussfolgerungen seien aus Sicht des Statistischen Bundesamtes plausibel. Der wissenschaftlich verantwortliche Verfasser sei dem Statistischen Bundesamt als wissenschaftliche Autorität im Bereich der statistischen Methodik und das eingesetzte Verfahren der logistischen Regression ist als ein wissenschaftlich anerkanntes Verfahren bekannt. Die Verwendung des Verfahrens in dem dargestellten Kontext scheine zweckmäßig zu sein.

Aufgrund des Gutachtens bestehen daher keine Zweifel mehr an der Wissenschaftlichkeit des von der SCHUFA eingesetzten Scoring-Verfahrens.

6.2 Transparenz des Scoring-Verfahrens, Nutzung des Score-Werts durch Vertragspartner

Vor Redaktionsschluss dieses Berichts teilte die SCHUFA mit, dass die Umstellung auf das neue Datenverarbeitungssystem voraussichtlich bis Ende 2006 erfolge und den Betroffenen dann auch Auskunft über den an SCHUFA-Vertragspartner übermittelten Score-Wert gegeben werden könne. Derzeit erhalten Betroffene nur Auskunft über den tagesaktuellen Score-Wert.

Wie bereits im letzten Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden ausgeführt (vgl. LT-Drucks. 16/1680, Nr. 10.2), vertreten die Aufsichtsbehörden die Auffassung, dass gegenüber dem Betroffenen der tatsächlich übermittelte Score-Wert beauskunftet werden soll.

In der letzten Sitzung der Arbeitsgruppe "Auskunfteien/SCHUFA" des Düsseldorfer Kreises wurde im Hinblick auf die Transparenz des Verfahrens erörtert, ob dem Betroffenen gegenüber die in die Berechnung des Score-Werts einfließenden Faktoren in der Selbstauskunft anzugeben sind.

Angesprochen wurde auch die Möglichkeit, dass Banken den Score-Wert der SCHUFA erhalten und diesen mit eigenen weiteren Daten in einem eigenen

Score-System verwenden. Es bestand die Befürchtung, dass es zu fehlerhaften Berechnungen (Doppel-Berücksichtigung von Merkmalen) kommen könnte, wenn eine Bank die Faktoren, die in die Berechnung des SCHUFA-Scores einfließen, nicht kenne. Hierzu hatte die SCHUFA bereits im Rahmen der oben genannten Prüfung (siehe oben Nr. 6.1) mitgeteilt, dass sie Banken, die den SCHUFA-Score in eigene Score-Systeme einfügten, die berücksichtigten Faktoren bekannt gebe.

Bei der weiteren Erörterung des SCHUFA-Scoring-Verfahrens werden voraussichtlich auch die von anderen Auskunfteien angebotenen Scoring-Verfahren einbezogen werden.
Besonderes Augenmerk wird ebenfalls darauf zu richten sein, ob Vertragspartner, welche Score-Werte erhalten, die Vorgaben des § 6a BDSG beachten.

6.3 Filtertext bei Widerspruch gegen die Score-Berechnung

Betroffene können bei der SCHUFA Widerspruch gegen die Berechnung eines Score-Werts erheben, sodass für sie kein solcher Wert mehr berechnet wird. Widerspricht ein Betroffener der Score-Ermittlung und bleibt er auch nach Hinweisen der SCHUFA zum Score-Verfahren bei dieser Haltung, übermittelte die SCHUFA ihren Vertragspartnern, die nach dem Score-Wert fragen, den Text "Betroffener widerspricht Scoreberechnung". In der Arbeitsgruppe "Auskunfteien/SCHUFA" äußerten die beteiligten Aufsichtsbehörden jedoch Bedenken gegen diese Formulierung und forderten eine neutralere Formulierung. Die SCHUFA sagte dies zu.

Gegenüber der Aufsichtsbehörde bestätigte die SCHUFA nunmehr, dass diese Zusage mittlerweile umgesetzt wurde. Der ursprünglich bekannt gegebene Text "Betroffener widerspricht Score-Berechnung" erscheint nur noch in der Selbstauskunft, damit der Betroffene die Bestätigung erhält, dass sein Widerspruch beachtet wird. Vertragspartner erhalten den Text "über angefragte Person erfolgt keine Score-Ermittlung" angezeigt.

6.4 Erweiterung des Kreises der Vertragspartner der SCHUFA

Die SCHUFA wurde aufgefordert, sich zu einem Vorschlag der Arbeitsgruppe "Auskunfteien/SCHUFA" zu äußern, der das Verfahren für Wohnungsunternehmen betrifft. Der Vorschlag sieht im Wesentlichen eine Begrenzung auf eine "geschlossene Benutzergruppe" - ausschließlich Wohnungsunternehmen - vor. Eine Stellungnahme der SCHUFA zu dem Vorschlag der Arbeitsgruppe der Aufsichtsbehörden lag bis zum Redaktionsschluss dieses Berichts nicht vor.

Das Vorhaben, Sicherheitsunternehmen als Vertragspartner für das B-Verfahren zu gewinnen, wird von der SCHUFA nicht weiterverfolgt.

Die SCHUFA beabsichtigte, Versicherungsunternehmen die Möglichkeit zu eröffnen, Vertragspartner für das B-Verfahren zu werden. Die SCHUFA verwies insbesondere darauf, dass nach Ansicht der Versicherer ein Zusammenhang zwischen der Bonität und dem Schadensrisiko, dem Risiko, dass der Versicherungsfall eintritt, bestehe. Dies wurde von den Aufsichtsbehörden in der Arbeitsgruppe "Auskunfteien/SCHUFA" im Hinblick auf die Voraussetzungen des § 29 Abs. 2 BDSG kritisiert, da das Schadensrisiko grundsätzlich kein kreditorisches Risiko darstellt und nicht jedes finanzielle Risiko die Übermittlung von Bonitätsdaten rechtfertigt.

Die SCHUFA versicherte gegenüber der Arbeitsgruppe inzwischen, dass das B-Verfahren für Versicherer jedenfalls nicht umgesetzt werde, solange der Zusammenhang zwischen Bonität und Schadensrisiko nicht hinreichend wissenschaftlich nachgewiesen sei.

Die geplante und teilweise bereits realisierte Teilnahme von Inkassounternehmen am SCHUFA-Verfahren beurteilen die in der Arbeitsgruppe "Auskunfteien/SCHUFA" vertretenen Aufsichtsbehörden differenziert.

Wenn Inkassounternehmen als Erfüllungsgehilfen von Unternehmen tätig werden, die bereits Vertragspartner der SCHUFA sind, ist dies unproblematisch, weil es sich um keine echte Erweiterung des Kreises der SCHUFA-Vertragspartner handelt.

Unproblematisch ist auch die Teilnahme der Inkassounternehmen an dem neuen F-Verfahren, bei dem die Inkassounternehmen nur Schuldnerverzeichnisdaten und Insolvenzdaten der Insolvenzgerichte erhalten.

Differenzierter zu beurteilen ist die Teilnahme am B-Verfahren bei Inkassounternehmen, die Forderungen für solche Unternehmen einziehen, die nicht Vertragspartner der SCHUFA sind.
Die SCHUFA erklärte sich jedoch bereit, die Forderungen der Aufsichtsbehörde zu erfüllen, wonach

- nur rechtskräftig titulierte Forderungen gemeldet werden dürfen, die vorläufige Vollstreckbarkeit ist nicht ausreichend,
- die Forderungen erst sechs Wochen nach der Titulierung gemeldet werden dürfen, damit der Betroffene ausreichend Zeit erhält, die Zahlung vorzunehmen.

6.5 Personenverwechslungen

Im letzten Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden wurde ausführlich über die Problematik von Personenverwechslungen berichtet (vgl. LT-Drucks. 16/1680, Nr. 10.3). Auch im aktuellen Berichtsjahr wurden der Aufsichtsbehörde aufgrund der Beschwerden Betroffener einige Verwechslungsfälle bekannt.

In einigen Fällen waren Meldungen der SCHUFA-Vertragspartner ursächlich für die Verwechslungen. In anderen Fällen lag der Fehler bei der SCHUFA, z.B. wurde eine Negativmeldung falsch zugeordnet, weil die mit der Prüfung der Anfrage befasste SCHUFA-Mitarbeiterin bei einer Angabe von einem Schreibfehler ausging.

Die SCHUFA räumte gegenüber der Aufsichtsbehörde in diesen Fällen ein, dass offenkundig Zuordnungsfehler vorlagen, die durch eine Rückfrage bei dem einmeldenden Vertragspartner möglicherweise hätten vermieden werden können.

In einem anderen Fall war es schon einmal zu einer Verwechslung gekommen, weshalb ein Hinweis in beiden Datensätzen gespeichert wurde, dass keine Identität zwischen den beiden Personen besteht. Aufgrund einer Programmroutine im SCHUFA-System wurde der Nichtidentitätshinweis gelöscht und es kam erneut zu einer falschen Zuordnung. Die SCHUFA ersetzte in diesem Fall der betroffenen Person die bei der Aufklärung der Verwechslung entstandenen Aufwendungen.

Wie bereits im letzten Tätigkeitsbericht ausgeführt, hatte die SCHUFA im Jahr 2002 mit einer strukturierten Aufarbeitung der Verwechslungsproblematik begonnen. Die Aufsichtsbehörde ließ sich das abgestufte System der Prüfung bei unklarer Identität demonstrieren und die aufgrund der Analyse getroffenen bzw. geplanten Maßnahmen erläutern.

Geht von einem Vertragspartner eine Meldung ein, findet zunächst eine maschinelle Suche im gespeicherten Datenbestand der SCHUFA nach der betroffenen Person statt. Wenn keine automatisierte Zuordnung zu einem Datensatz einer Person möglich ist, erfolgt eine Aussteuerung an einen Arbeitsplatz zur manuellen Bearbeitung.

Zu den bereits getroffenen Maßnahmen gehört beispielsweise die Hervorhebung der Abweichungen und etwaiger Nichtidentitätshinweise zur deutlicheren Kenntlichmachung bei der manuellen Bearbeitung von Meldungen. Nichtidentitätshinweise werden nicht mehr automatisch gelöscht.

Die Arbeitsanweisungen für die Sachbearbeitung werden überarbeitet und sollen im Intranet der SCHUFA zur schnelleren Verfügbarkeit und besseren Suchmöglichkeit zur Verfügung gestellt werden. Außerdem werden Schulungskonzepte erarbeitet und die technischen Suchroutinen verbessert. Ferner wurde mit den Vertragspartnern eine Projektgruppe zur Verbesserung der Datenqualität gebildet.

Die Aufsichtsbehörde forderte die Vorlage der Arbeitsanweisungen und wird weiter beobachten, ob die Maßnahmen Erfolg haben oder weitere Maßnahmen erforderlich sind.

7. Banken
7.1 Spenden an gemeinnützige Organisationen

Die Arbeit von gemeinnützigen Organisationen kann nicht hoch genug eingeschätzt werden. Die Organisationen sind in der Regel auf Spenden angewiesen und daher berechtigterweise bestrebt, neue Spender zu gewinnen und auf Dauer zu behalten.

Wenn Spendenaufrufe in den Medien veröffentlicht werden, z.B. aus Anlass von Katastrophenfällen, gibt es erfahrungsgemäß viele spontane Spenden. Dass die gemeinnützigen Organisationen daran interessiert sind, die Adressen dieser Spender zu erfahren, um sich bei ihnen zu bedanken und sie nach gewisser Zeit erneut um eine Spende zu bitten, ist sehr verständlich.

Ein Direktmarketing-Dienstleister, der für eine oder mehrere Organisationen tätig war, teile der Aufsichtsbehörde mit, dass die Organisationen auf die Hilfe der Banken angewiesen seien. Die Banken würden oftmals keinerlei Angaben zu den Spendern übermitteln, oft würden wohl auch die Spender keine oder nur unvollständige Adressen angeben.

Das Marketing-Unternehmen beabsichtigte, ein Verfahren anzubieten, um die geschilderten Probleme der Organisationen zu beheben. Die gemeinnützige Organisation sollte die unklaren Adressen mit Kontonummern an diejenige Bank geben, bei der die Überweisung veranlasst wurde. Die Bank sollte der Kontonummer dann die jeweilige Adresse des Kontoinhabers zuordnen. Die gemeinnützige Organisation erhielte von der Bank nur die Adressen der Spender zurück und keine weiteren Bankdaten.

Nach der Feststellung der Aufsichtsbehörde enthalten die Überweisungsvordrucke der verschiedenen Organisationen stets folgenden Hinweis:

"Bitte geben Sie für die Spendenbestätigung Ihre Spenden-/Mitgliedsnummer oder Ihren Namen und Ihre Adresse an."

Der Hinweis ist jeweils links unten neben dem Feld für die Datumsangabe und die Unterschrift auf dem Vordruck angebracht. Die entsprechenden Angaben sind in den üblicherweise für die Angabe des Verwendungszweckes vorgesehenen zwei Zeilen einzutragen.

Wenn ein Spender hier keine Angaben macht, bringt er zum Ausdruck, dass er eine Spendenbestätigung nicht wünscht und anonym bleiben will.

Die Bank, bei der die Überweisung veranlasst wird, ist nur berechtigt, den Namen des Überweisenden, also des in der Zeile darunter einzutragenden Kontoinhabers bzw. Einzahlers, weiterzuleiten (vgl. § 676a Abs. 1 BGB). Die Weiterleitung weiterer Angaben wäre mit dem Bankgeheimnis nicht vereinbar und ist daher unzulässig (vgl. 13. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, LT-Drucks. 15/1539, Nr. 5.5).

Bereits die Weiterleitung der Kontonummer und Bankleitzahl der Kontoverbindung des Überweisenden an den Empfänger des Geldes ist danach unzulässig. Wenn die datenschutzrechtlichen Vorgaben beachtet werden, erfährt die gemeinnützige Organisation gar nicht, von wem die Überweisung stammt.

Wenn ein Spender in den für die Spendenbestätigung vorgesehenen Zeilen unvollständige Angaben macht, z.B. nur seinen Nachnamen ohne weitere Angaben einträgt, ist die Bank jedenfalls nicht berechtigt, die Angaben um den Vornamen und die Adresse zu ergänzen. Auch hier steht das Bankgeheimnis einer Übermittlung entgegen. Allenfalls bei ganz geringfügigen Unklarheiten, z.B. wenn die Hausnummer unleserlich geschrieben wurde, käme eine Korrektur bzw. Ergänzung in Betracht.

Nachfragen der Aufsichtsbehörde bei den betrieblichen Datenschutzbeauftragten zweier Banken im Aufsichtsbezirk ergaben, dass diese das Ansinnen des Direktmarketing-Unternehmens bereits zurückgewiesen hatten.

Ebenso wie die Banken auf das Vertrauen ihrer Kunden angewiesen sind, benötigen die gemeinnützigen Unternehmen das Vertrauen ihrer Spender. Dazu ist es unerlässlich, dass die Entscheidung eines Spenders, anonym bleiben zu wollen, respektiert wird. Letztlich wird sich die Einhaltung des Datenschutzes daher auch für die gemeinnützigen Organisationen auszahlen.

7.2 Elektronisches Lastschriftverfahren - Datenübermittlung trotz Kontosperre

Bei einem Hauseinbruch wurden sämtliche Kredit- und EC-Karten der Bewohner gestohlen. Die Betroffenen erstatteten sofort Strafanzeige und baten die Bank um Karten- bzw. Kontosperrung. Mit den gestohlenen Karten wurden in insgesamt 34 Fällen missbräuchlich Einkäufe getätigt. Die auf das Konto der Betroffenen eingereichten Lastschriften wurden aufgrund deren Widerspruchs storniert.

Die Betroffenen hatten die Bank hierbei jeweils ausdrücklich darauf hingewiesen, dass sie der Herausgabe ihrer Adressen an Dritte widersprechen. Die Bank versicherte, dass der Datenschutz beachtet werde. Die Betroffenen erhielten jedoch mehrere Mahnungen von Verbrauchermärkten und anderen Einzelhandelsgeschäften aufgrund der stornierten Lastschriften. Auf Nachfrage teilten diese mit, dass sie die Adressen von der Bank erhalten hatten.

Beim Einsatz der EC-Karte für das elektronische Lastschriftverfahren unterschreibt der Kunde zwar die unwiderrufliche Einwilligung, dass die Bank im Falle der Nichteinlösung der Lastschrift oder bei Widerspruch gegen die Lastschrift dem Unternehmen, bei dem mittels elektronischem Lastschriftverfahren bezahlt wurde, auf Aufforderung Namen und Anschrift mitteilen darf. Aber dies gilt nicht für den Fall der Sperrung des Kontos wegen Diebstahls der Karte. In diesem Fall ist nämlich gerade nicht von einer wirksamen Einwilligung des Betroffenen auszugehen, weil die Einwilligung nicht von ihm selbst unterzeichnet wurde, sondern eine Unterschriftenfälschung durch eine andere Person erfolgte.

Die Bank ist außerdem durch das Bankgeheimnis gehindert, die Daten des Karteninhabers herauszugeben. Hiergegen hatte die Bank verstoßen.

Sinnvoller wäre es gewesen, die 34 Buchungsvorgänge der ermittelnden Polizeidienststelle mitzuteilen, weil die Buchungen auch eine Spur zu den Tätern des Einbruchs darstellten.
Die Überprüfung durch die Aufsichtsbehörde ergab, dass bei der Bank eine Anweisung bestand, wonach bei Sperrung eines Kontos keine Daten der Adresse herausgegeben werden dürfen. Dass dies im vorliegenden Falle trotzdem geschah, führte die Bank auf einen menschlichen Fehler zurück. Die Bearbeiterin hatte offensichtlich den Vermerk der Kontosperre übersehen und überdies die Unterschriften nicht sorgfältig verglichen.

Die Bank nahm den Vorgang zum Anlass, sowohl die betreffende Mitarbeiterin als auch alle anderen im Kundenkontakt stehenden Mitarbeiter auf eine korrekte Vorgehensweise im Umgang mit Kundendaten hinzuweisen. Daher sah die Aufsichtsbehörde von weiteren Maßnahmen ab.

8. Inkassounternehmen

Zahlreiche Beschwerden richteten sich gegen den Datenverarbeitungshinweis eines Inkassounternehmens, der als Anhang zum Überweisungsvordruck dem Mahnschreiben beigefügt war.

Der Hinweis enthielt Formulierungen, die darauf schließen ließen, dass die Schuldnerdaten direkt an dritte Geschäftspartner übermittelt würden, wenn die Forderung nicht beglichen wird, damit diese die Zahlungswilligkeit bzw. Zahlungsfähigkeit der Schuldner einschätzen könnten. Die Proteste richteten sich sowohl dagegen, dass auch bestrittene Forderungen übermittelt werden könnten, als auch dagegen, dass die Übermittlung an willkürlich ausgewählte Empfänger erfolgen könnte.

Die Prüfung des Unternehmens vor Ort ergab jedoch, dass neben der Information an den konkret beteiligten Gläubiger allein die SCHUFA Empfänger der Schuldnerdaten war. Dabei wurden die entsprechenden Einmeldevorgaben der SCHUFA beachtet.

Die Aufsichtsbehörde forderte eine Abänderung des irreführenden Datenverarbeitungshinweises. Die SCHUFA unterbreitete dem Inkassounternehmen einen Formulierungsvorschlag, der von der Aufsichtsbehörde nur vorläufig akzeptiert wurde, weil noch vertragliche Details zwischen der SCHUFA und den Inkassounternehmen zu regeln sind, die möglicherweise auch eine Ab-

änderung des Hinweises zur Datenverarbeitung nach sich ziehen werden (siehe hierzu auch oben Nr. 6.4).

Fast genauso häufig beschwerten sich Betroffene über das Inkassounternehmen, weil sie auf ihre Auskunftsersuchen keine Antwort bekamen. Nicht selten wurde ihnen erst dann Auskunft über die zu ihrer Person gespeicherten Daten erteilt, wenn die Aufsichtsbehörde sich eingeschaltet hatte.

Die Prüfung in den Unternehmensräumen und die schleppende Zusammenarbeit mit der Aufsichtsbehörde machten ebenfalls deutlich, dass diese Probleme auch mit der nicht ordnungsgemäßen Tätigkeit des betrieblichen Datenschutzbeauftragten zusammenhingen, der sogar sein Desinteresse an dieser Tätigkeit betonte.

Die Aufsichtsbehörde forderte deshalb das Unternehmen auf, die Bestellung des alten Datenschutzbeauftragten zu widerrufen und einen zuverlässigen, fachlich geeigneten betrieblichen Datenschutzbeauftragten zu bestellen.

Das Unternehmen hat inzwischen einen neuen betrieblichen Datenschutzbeauftragten bestellt, dessen Tätigkeit die Aufsichtsbehörde beobachten wird.

Mehrere Eingaben erreichten die Aufsichtsbehörde auch wegen eines Fragebogens, der den Mahnschreiben, die über eine kooperierende Rechtsanwaltskanzlei versandt wurden, angehängt war.

Dieser Fragebogen enthielt zahlreiche detaillierte Fragen zu den Familienverhältnissen, einschließlich Name, Beruf und Einkommen des Ehepartners und der eigenen finanziellen Verhältnisse sowie eine Anerkenntniserklärung, eine Einzugsermächtigung und eine Abtretungserklärung hinsichtlich etwaiger Ansprüche auf Lohn, Gehalt, Arbeitnehmersparzulage, Arbeitlosengeld- und -hilfe, Krankengeld und Renten.

Am Ende des Fragebogens wurde die Unterschrift des Absenders bzw. bei Lastschrift des Kontoinhabers gefordert. Das Mahnschreiben war zudem mit dem Hinweis versehen, dass der Fragebogen vollständig ausgefüllt und unterschrieben in der festgesetzten Frist zurückgeschickt werden müsse, um weitergehende Maßnahmen und damit verbundene Kosten zu vermeiden.

Das Inkassounternehmen berief sich darauf, dass die Mehrzahl der Schuldner die Angaben freiwillig mitteile, indem sie die Fragebogen ausfüllen und zurücksenden würden. Es läge insoweit eine wirksame Einwilligung in die Erhebung, Verarbeitung und Nutzung der Daten vor.

Diese Argumentation hielt die Aufsichtsbehörde schon aufgrund des drohenden Hinweises auf dem Mahnschreiben für nicht akzeptabel, weil sich daraus ein faktischer Zwang ergab, die Fragen in dem Fragebogen zu beantworten, ganz gleich ob die Forderung bestritten wurde, bereits beglichen worden war oder aufgrund des Mahnschreibens umgehend vollständig beglichen werden sollte.

An keiner Stelle des Mahnschreibens oder des Fragebogens befand sich ein Hinweis darauf, dass alle Angaben gegenüber dem Inkassounternehmen freiwillig seien und in den genannten Ausnahmefällen ohnehin nicht benötigt würden. Es wurde so der Eindruck vermittelt, der Fragebogen sei in jedem Fall zu beantworten, um mögliche Nachteile zu vermeiden. Die erforderliche Freiwilligkeit der Erklärung war aufgrund dieser Umstände nicht anzunehmen.

Die Aufsichtsbehörde forderte das Inkassounternehmen auf, den Fragebogen grundlegend abzuändern und die Schuldner ordnungsgemäß nach § 4 Abs. 3 BDSG zu informieren.

9. Aspekte internationaler Datenverarbeitungen

9.1 Übermittlung von Schuldnerverzeichnisdaten nach Indien

Für Wirtschaftsauskunfteien stellen die Daten der bei den Amtsgerichten geführten Schuldnerverzeichnisse (eidesstattliche Versicherung, Haftbefehl wegen Nichterscheinen zur Abgabe der eidesstattlichen Versicherung etc.) eine der wichtigsten Datenquellen dar.

Das Einpflegen und die Zuordnung dieser Daten zum vorhandenen Datenbestand der Auskunftei stellen eine personalaufwendige Arbeit dar, welche

eine international tätige Wirtschaftsauskunftei mit rechtlich selbstständiger Niederlassung im Rhein-Main-Gebiet nach Indien auslagern wollte. Die britische Niederlassung dieser Auskunftei hatte bereits gute Erfahrungen mit dem indischen Dienstleister gemacht.

Der indische Dienstleister sollte seinerseits einen Dienstleister ("Unterauftragnehmer") in Nordrhein-Westfalen einschalten, der die Daten aus den Schuldnerverzeichnissen nach Indien transferiert. Soweit die Daten von den Gerichten in Papierform geliefert werden (insgesamt ca. 30 v.H.), sollten sie von diesem zunächst elektronisch erfasst (gescannt) werden. Der indische Dienstleister sollte die Daten nach der Verarbeitung an die Muttergesellschaft der Wirtschaftsauskunftei in den USA übermitteln, da sich dort der zentrale Server der gesamten Auskunftei befindet.

Die US-Muttergesellschaft der Auskunftei ist nach den Safe-Harbor-Regelungen zertifiziert, wodurch insoweit ein angemessenes Datenschutzniveau im Sinn des § 4b Abs. 2 und Abs. 3 BDSG gewährleistet ist. Problematisch war jedoch die Auslagerung der Datenverarbeitung nach Indien, weshalb die Auskunftei die Aufsichtsbehörde um Auskunft zur Rechtslage und Beratung bat.

Es bestand Einigkeit, dass der Ausnahmekatalog des § 4c Abs. 1 BDGS nicht einschlägig ist, insbesondere der gesetzliche Ausnahmetatbestand des § 4c Abs. 1 Satz 1 Nr. 6 BDSG nicht erfüllt ist, weil die Schuldnerverzeichnisse nicht der gesamten Öffentlichkeit, sondern nur solchen Personen zur Einsichtnahme offen stehen, die ein berechtigtes Interesse nachweisen können. Der indische Dienstleister hat kein berechtigtes Interesse im Sinne der maßgeblichen Vorschriften der Schuldnerverzeichnisse.

Daher wurde dem Unternehmen empfohlen, den EU-Standardvertrag vom 27. Dezember 2001 mit dem indischen Dienstleister abzuschließen. Dieser Standardvertrag wurde speziell für die Fälle konzipiert, in denen Daten an ein im Drittstaat ansässiges Unternehmen transferiert werden, das als untergeordneter und weisungsgebundener Auftragsverarbeiter fungiert, also keine eigenen Entscheidungsbefugnisse bezüglich der personenbezogenen Daten erhält. Bei wörtlicher Verwendung des Standardvertrages im Sinn des Art. 26 Abs. 4 EG-DSRL entfällt die bei individuellen Verträgen ansonsten nach § 4c Abs. 2 BDSG erforderliche Genehmigung (vgl. 15. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, LT-Drucks. 15/4659, Nr. 7.2).

Die Auskunftei folgte dem Rat der Aufsichtsbehörde. In den Anlagen zum Standardvertrag wurden die Datenverarbeitung und die Datensicherheitsmaßnahmen, insbesondere die notwendige Verschlüsselung der Daten, konkret beschrieben. Trotz der Genehmigungsfreiheit äußerte die Auskunftei den Wunsch nach einer förmlichen Genehmigung durch die Aufsichtsbehörde. Diesem Wunsch konnte jedoch nicht entsprochen werden. Hilfsweise bat das Unternehmen, eine Abstimmung im Düsseldorfer Kreis herbeizuführen.

Das besondere Interesse an einer Genehmigung oder zumindest einer behördlichen Bescheinigung der Zulässigkeit der Datenverarbeitung in Indien beruhte darauf, dass die Auskunftei darum besorgt war, die notwendigen Daten ohne Probleme von den Gerichten zu erhalten. Die Auskunftei hatte zunächst von sämtlichen zuständigen Amts- und Landgerichtspräsidenten im Bundesgebiet eine Bewilligung zum laufenden Bezug von Abdrucken aus den Schuldnerverzeichnissen erhalten und beabsichtigte nun, die Gerichtspräsidenten über die geplante Auslagerung der Datenverarbeitung nach Indien zu informieren.

Da die Gerichtspräsidenten in ihrer Entscheidung über den Bezug von Abdrucken aus dem Schuldnerverzeichnis datenschutzrechtliche Erwägungen anzustellen haben, ging die Auskunftei davon aus, dass die Gerichtspräsidenten die für ihren Gerichtsbezirk zuständige Aufsichtsbehörde um Stellungnahme bitten würden.

Daher initiierte die Aufsichtsbehörde eine Abstimmung im Düsseldorfer Kreis. Diese führte zu der übereinstimmenden Bewertung, dass die Auskunftei durch die Verwendung der Standardvertragsklauseln ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweisen kann und somit die Anforderungen

des § 4c Abs. 2 BDSG erfüllt sind. Zugleich bestand jedoch Einigkeit, dass die Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich zur Frage, unter welchen Voraussetzungen die Gerichtspräsidenten die Datenlieferung an die Auskunftei bewilligen dürfen, mangels Zuständigkeit keine Aussage treffen können.

Die zahlreichen Anfragen von Gerichtspräsidenten wurden von der Aufsichtsbehörde unter Bezugnahme auf die Abstimmung im Düsseldorfer Kreis beantwortet. Dazu gab die Aufsichtsbehörde den Hinweis, dass nach dieser Auffassung der Datentransfer von der Datenschutzaufsichtsbehörde nur beanstandet werden kann, wenn Erkenntnisse vorliegen, dass die Vertragsbedingungen nicht eingehalten werden. Eine Prüfung in Indien hat die Aufsichtsbehörde nicht vorgenommen, sie ist vom Bundesdatenschutzgesetz auch nicht vorgeschrieben.

Wie den späteren Informationsschreiben der Gerichtspräsidenten zu entnehmen war, haben diese der Auskunftei weiterhin die Bewilligungen zum Bezug der Abdrucke aus den Schuldnerverzeichnissen erteilt.

9.2 Übermittlung von Fluggastdaten an die Zoll- und Grenzschutzbehörde der USA

Nach den Terroranschlägen des 11. September 2001 trat in den USA eine Reihe von Gesetzen und Verordnungen in Kraft, die Fluggesellschaften bei Flügen in ihr Hoheitsgebiet dazu verpflichten, den US-Behörden personenbezogene Daten über einreisende oder ausreisende Fluggäste und Besatzungsmitglieder zu übermitteln. Insbesondere müssen die Fluggesellschaften dem US Bureau of Customs and Border Protection (US CBP - Zoll- und Grenzschutzbehörde der Vereinigten Staaten) bei Flügen in die, aus den und durch die USA elektronischen Zugang zu den im so genannten Passenger Name Record (PNR) enthaltenen Fluggastdaten gewähren. Fluggesellschaften, die diesen Forderungen nicht nachkommen, müssen mit hohen Geldstrafen oder sogar dem Entzug der Landerechte, ihre Passagiere mit Verspätungen bei der Ankunft in den USA rechnen.

Mit der Problematik der Vereinbarkeit dieser Regelungen mit dem europäischen Datenschutzrecht hat sich die Art.-29-Gruppe (Vertreter der europäischen Datenschutzaufsichtsbehörden) mehrfach befasst und kritische Stellungnahmen abgegeben (vgl. Arbeitspapiere 78, 87 und 95, abrufbar im Internet unter: http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2004/wpdocs04_de.htm).

Die Europäische Kommission führte intensive Verhandlungen mit US-Regierungsvertretern, bei denen unter anderem erreicht wurde, dass die Speicherfrist von den am Anfang vorgesehenen 50 Jahren auf eine Frist von drei Jahren und sechs Monaten reduziert wurde.

Angesichts der von US-Seite abgegebenen Datenschutz-Verpflichtungserklärung hat die Europäische Kommission trotz Kritik des EU-Parlaments nach Zustimmung der Art.-31-Gruppe (Vertreter der europäischen Regierungen) am 14. Mai 2004 die Feststellung nach Art. 25 Abs. 6 EG-DSRL getroffen, dass bezüglich der Verarbeitung der Fluggastdaten ein angemessenes Datenschutzniveau in den USA gewährleistet ist (im Internet abrufbar unter: http://europa.eu.int/comm/internal_market/privacy/adequacy_de.htm.

Weil damit nur die Drittstaatenproblematik behandelt wurde, nicht aber die Frage, ob überhaupt eine Rechtsgrundlage für die Übermittlung von Daten durch die Fluggesellschaften aus dem EU-Raum besteht ("Zwei-Stufen-Prüfung", vgl. 15. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, LT-Drucks. 15/4659, Nr. 7.4), verhandelte die EU-Kommission außerdem über ein bilaterales Abkommen nach Art. 300 Abs. 2 Unterabs. 1 Satz 1, Abs. 3 EG-Vertrag. Der Rat der Europäischen Union stimmte mit Beschluss vom 17. Mai 2004 dem Abschluss des Abkommens zu, das am 28. Mai 2004 unterzeichnet wurde.

Das Europäische Parlament hat sowohl gegen die von der EU-Kommission am 14. Mai 2004 getroffene Feststellung eines angemessenen Datenschutzniveaus als auch gegen am 17. Mai 2004 beschlossene Zustimmung des Rats zur Unterzeichnung des Abkommens mit den USA beim Europäischen Gerichtshof Nichtigkeitsklage nach Art. 230 EG-Vertrag erhoben.

Betroffene Bürger, die sich an die Aufsichtsbehörde wandten, weil sie mit der Lufthansa in die USA reisen wollten, wurden nach allgemeinen Hinweisen an die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen verwiesen, da sich der Sitz der Lufthansa in Köln befindet.

Aufgrund von Eingaben gegen die deutsche Niederlassung einer französischen Fluggesellschaft, insbesondere wegen der Frage der ausreichenden Aufklärung der Flugpassagiere, nahm die Aufsichtsbehörde zunächst Kontakt mit der deutschen Niederlassung auf und unterrichtete die französische Aufsichtsbehörde, die bereits Gespräche mit der Zentrale der Fluggesellschaft aufgenommen hatte. Im Hinblick auf diese Gespräche und weil die deutsche Niederlassung der Fluggesellschaft bei Flugbuchungen mittlerweile einen - wenn auch verbesserungsbedürftigen - Aufklärungstext aushändigte, sah die Aufsichtsbehörde von weiteren Maßnahmen ab.

Im Rhein-Main-Gebiet befinden sich auch Niederlassungen von US-Fluggesellschaften. Obwohl es sich um rechtlich unselbstständige Niederlassungen handelt und sich der Unternehmenssitz in den USA befindet, haben diese nach § 1 Abs. 5 Satz 2 BDSG das deutsche Datenschutzrecht zu beachten, soweit sie in Deutschland Daten erheben und verarbeiten.

Daher wandte sich die Aufsichtsbehörde bereits im Februar 2003 an die Niederlassungen der US-Fluggesellschaften und bat um Auskunft, ob den US-Behörden Zugriff auf die Buchungs- und Reservierungsdaten gegeben wird. Da dies bejaht wurde, forderte die Aufsichtsbehörde die Airlines auf, für eine frühestmögliche Unterrichtung der Passagiere zu sorgen.

Nach § 4 Abs. 3 BDSG sind die betroffenen USA-Reisenden bereits bei der Erhebung der Buchungs- und Reservierungsdaten über die Zweckbestimmung der Verarbeitung und Nutzung sowie die Kategorien von Empfängern der Daten zu unterrichten. Aus der Unterrichtung müssen die Betroffenen erkennen können, welche Risiken mit der Übermittlung an US-Behörden verbunden sind. Dazu ist insbesondere darüber aufzuklären, dass mit den Passdaten, den Buchungs- und Flugreservierungsdaten auch Angaben über Reiseweg und Aufenthalt in den USA übermittelt werden.

Im Hinblick darauf, dass im Einzelfall auch besondere Arten personenbezogener Daten im Sinn des § 3 Abs. 9 BDSG in den Servicedaten enthalten sein können, müssen die Passagiere entscheiden können, ob sie in Kenntnis einer Übermittlung an US-Behörden auf Angaben solcher Art verzichten wollen. Relevant ist dies beispielsweise bei Angaben über eine Schwerbehinderung oder die Wahl eines bestimmten Menüs, soweit dieses Rückschlüsse auf die religiöse Überzeugung ermöglicht (z.B. koscheres Essen, kein Schweinefleisch).

Die rechtliche Situation bei den US-Airlines unterscheidet sich von derjenigen der europäischen Fluggesellschaften. Die Passagierdaten werden bereits zur Abwicklung des Transportvertrages in die USA übermittelt. Was dann in den USA mit den Daten geschieht, unterliegt nicht dem BDSG. Aber die Unterrichtungspflicht besteht in jedem Fall, da davon auszugehen ist, dass die Daten in Europa erhoben werden.

Zur gesamten Thematik fand im Mai 2003 ein Abstimmungsgespräch im Bundesministerium des Innern statt, an dem auch andere Aufsichtsbehörden und Stellen, unter anderem die Lufthansa und der Deutsche Reisebüroverband, beteiligt waren.

Die US-Airlines waren zahlreich vertreten, auch über US-Verbandssprecher (Air Transport Association) und erklärten ihre Bereitschaft, die Forderungen der Aufsichtsbehörden umzusetzen. Ein Vertreter der Botschaft der USA hatte die Koordination angeboten und unterstützte bei der Übersetzung.

Unter Federführung des US-Luftfahrtverbandes entwarfen die Airlines sodann einen Unterrichtungstext. Im Interesse einer möglichst einheitlichen Handhabung, die zu Recht auch vom deutschen Reisebüroverband gefordert worden war, wurde der US-Luftfahrtverband gebeten, sich mit der Lufthansa auf einen gemeinsamen Text zu verständigen, der noch stärker an den von den Aufsichtsbehörden bereits akzeptierten Unterrichtungstext der Lufthansa angelehnt sein sollte.

Während diese Abstimmung begann, erfolgte zugleich auf europäischer Ebene über die Art.-29-Gruppe der Versuch, sich auf einen gemeinsamen Text zu einigen. Im Zuge der Verhandlungen der EU-Kommission mit den US-Vertretern nahm sich die EU-Kommission auch dieses Themas an. Hieran anknüpfend, allerdings mit einigen Ergänzungen bzw. Korrekturen an dem Text der EU-Kommission, waren in der Art.-29-Gruppe vor Redaktionsschluss dieses Berichtes erneut Gespräche mit dem Ziel einer Verständigung auf einen gemeinsamen europäischen Unterrichtungstext geplant.

Sollte eine Einigung auf einen europäischen Text nicht zustande kommen, wird die Aufsichtsbehörde die Gespräche mit den US-Airlines wieder aufnehmen, damit wenigstens für Deutschland ein einheitlicher Text verwendet wird.

9.3 Übermittlung von Daten deutscher Wirtschaftsprüfer in die USA

Als Reaktion auf die vergangenen Bilanz- und Wirtschaftsskandale, insbesondere den Fall "Enron", hat der amerikanische Gesetzgeber den Sarbanes-Oxley Act 2002 erlassen. Ziel ist es, den Schutz der Anleger zu stärken und effizientere Kontrollen von Unternehmen einzuführen. Die Regelungen richten sich unter anderem an die Unternehmen selbst, aber auch an Rechtsanwälte und Wirtschaftsprüfer.

Zur Regulierung der Tätigkeit von Wirtschaftsprüfern wurde das Public Company Accounting Oversight Board ("PCAOB") eingerichtet. Dieses ist zwar privatrechtlich organisiert und hat keinen Behördenstatus. Es soll jedoch der Wirtschaftsprüferkammer vergleichbare Aufsichtstätigkeiten übernehmen. Zu diesem Zweck wurde unter anderem eine Registrierungspflicht auch für ausländische Wirtschaftsprüfer bzw. Wirtschaftsprüfungsgesellschaften eingeführt.

Zum Zwecke der Registrierung ist es für die Wirtschaftsprüfungsgesellschaften notwendig, auf elektronischem Wege ein Formular auszufüllen, in dem weitreichende Angaben gemacht werden müssen, die auch personenbezogene Daten über die für die jeweiligen Wirtschaftsprüfungsgesellschaften tätigen Einzelpersonen einschließen. Unter anderem sind sämtliche noch laufenden oder während der vergangenen fünf Jahre abgeschlossenen Strafverfahren zu nennen, unabhängig davon, ob diese einen Bezug zur Berufstätigkeit haben oder nicht. Lediglich einige Verkehrsdelikte sind nicht anzugeben.

Anhand der Angaben entscheidet das PCAOB über die Registrierung. Sämtliche im Rahmen der Registrierung von den Wirtschaftsprüfungsgesellschaften gemachten Angaben werden grundsätzlich veröffentlicht. Eine vertrauliche Behandlung muss in jedem Einzelfall beantragt und begründet werden.

Bestimmte Angaben können verweigert werden, soweit die Übermittlung solcher Angaben gegen ausländisches Recht, also z.B. deutsches Recht, verstößt, dies von der Wirtschaftsprüfungsgesellschaft mit einem Rechtsgutachten unter Angabe der entsprechenden Rechtsvorschriften belegt wird und die antragstellende Wirtschaftsprüfungsgesellschaft glaubhaft darlegen kann, dass sie versucht hat, eventuell zulässige Einwilligungserklärungen einzuholen, ihr dies jedoch nicht gelungen ist.

Daher beauftragten die Deutsche Wirtschaftsprüfungskammer (WPK) mit Sitz in Berlin und das Institut der Deutschen Wirtschaftsprüfer (IDW) mit Sitz in Düsseldorf ein Rechtsanwaltsbüro mit der Erstellung entsprechender Gutachten. Das Anwaltsbüro kam zu dem Ergebnis, dass die Übermittlung der Angaben an das PCAOB aufgrund der gesetzlichen Erlaubnistatbestände des Bundesdatenschutzgesetzes entweder eindeutig unzulässig oder jedenfalls doch sehr zweifelhaft sei. Auch eine Einwilligung der betroffenen Wirtschaftsprüfer könne keine wirksame Grundlage sein.

Da die meisten von einer Registrierung nach dem Sarbanes-Oxley Act betroffenen Wirtschaftsprüfungsgesellschaften ihren Sitz in Frankfurt am Main haben, bat die Rechtsanwaltskanzlei die zuständige Aufsichtsbehörde um eine Stellungnahme.

Nach Abstimmung im Düsseldorfer Kreis konnte den Rechtsanwälten mitgeteilt werden, dass die Aufsichtsbehörden einhellig die gutachterliche Bewertung teilen.

Der Sarbanes-Oxley Act ist als ausländische Rechtsnorm keine "andere Rechtsvorschrift" im Sinne von § 4 Abs. 1 BDSG. Der Erlaubnistatbestand des § 28 Abs. 1 Nr. 1 BDSG greift nicht ein, weil Fragen eines Arbeitgebers an einen Arbeitnehmer nach Strafverfahren in Übereinstimmung mit der europäischen und deutschen Rechtsprechung zum Fragerecht eines Arbeitgebers individualvertraglich nicht zulässig sind und der Sarbanes-Oxley Act derartige Angaben in nahezu unbegrenztem Umfang verlangt, ohne ausreichende Garantien für eine vertrauliche Behandlung durch das PCAOB zu geben.

Im Rahmen der Interessenabwägung nach § 28 Abs. 1 Nr. 2 sowie § 28 Abs. 3 Nr. 1 BDSG gibt es schwerwiegende Gründe zur Annahme, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Übermittlung an das PCAOB überwiegt. Hierfür spricht zunächst die arbeitsrechtliche Unzulässigkeit. Die Preisgabe der angefragten Angaben kann sehr schwerwiegende Konsequenzen für den Betroffenen haben im Hinblick auf sein Beschäftigungsverhältnis oder seine Zulassung sowie seine Befähigung zur Berufstätigkeit in den USA. Eine vertrauliche Behandlung dieser sensitiven Informationen ist wegen der grundsätzlich vorgesehenen Veröffentlichung nicht gewährleistet. Schließlich werden Strafverfahren für einen Zeitraum abgefragt, für den innerhalb von Deutschland aufgrund des Bundeszentralregistergesetzes zumindest teilweise keine Auskünfte mehr erteilt würden bzw. der Betroffene trotz einer früheren Verurteilung angeben dürfte, dass er nicht vorbestraft ist. Dieses Recht würde im Hinblick auf eine Veröffentlichung der Angaben durch das PCAOB umgangen. Schließlich scheint die unbegrenzte Anfrage nicht verhältnismäßig und entspricht nicht den Grundsätzen der Datenvermeidung und Datensparsamkeit, da teilweise Daten ohne jeglichen Bezug zu Prüfungstätigkeiten oder ersichtliche Relevanz für die Registrierung der Wirtschaftsprüfungsgesellschaften abgefragt werden.

Dies gilt umso mehr, als die Registrierungspflicht sehr weit gefasst ist und auch deutsche Wirtschaftsprüfer erfasst, die in Deutschland Unternehmen prüfen, die in irgendeiner Weise einem Konzernverbund mit Unternehmen angehören, deren Aktien an einer US-amerikanischen Börse zum Handel zugelassen sind.

Außerdem unterliegt das PCAOB weder den Safe-Harbor Regelungen noch sind irgendwelche vertragliche Verpflichtungen zur Einhaltung eines angemessenen Datenschutzniveaus in Kraft. Die Voraussetzungen der §§ 4b, 4c BDSG liegen daher nicht vor.

Die übrigen gesetzlichen Erlaubnistatbestände sind in jedem Fall nicht einschlägig.

Entsprechende Bedenken bestehen auch gegen die Übermittlung einiger weiterer Daten, die im Registrierungsformular anzugeben wären.

Die Einholung von Einwilligungen der Wirtschaftsprüfer ist kein gangbarer Weg, da eine Einwilligung nach § 4a Abs. 1 Satz 1 BDSG auf der freien Entscheidung der Betroffenen beruhen, also ohne Zwang erteilt worden sein muss.

Zu dieser Problematik hat die Europäische Art.-29-Datenschutzgruppe in ihrer Stellungnahme 8/2001 die Auffassung geäußert, "dass es in den Fällen, in denen ein Arbeitgeber zwangsläufig aufgrund des Beschäftigungsverhältnisses personenbezogene Daten verarbeiten muss, irreführend ist, wenn er versucht, diese Verarbeitung auf die Einwilligung der betroffenen Person zu stützen. Die Einwilligung der betroffenen Person sollte nur in den Fällen in Anspruch genommen werden, in denen der Beschäftigte eine echte Wahl hat und seine Einwilligung zu einem späteren Zeitpunkt widerrufen kann, ohne dass ihm daraus Nachteile erwachsen."

Genau an diesen Voraussetzungen fehlt es jedoch. Die betroffenen Wirtschaftsprüfer stehen in einem rechtlichen und faktischen Abhängigkeitsverhältnis zu den Wirtschaftsprüfungsgesellschaften. Die Angelegenheit betrifft auch den Kernbereich des Arbeitsverhältnisses, da eine Registrierung beim PCAOB faktisch eine Voraussetzung für die Erbringung eines beträchtlichen Teils der Arbeit der betroffenen Wirtschaftsprüfungsgesellschaften darstellt. Eine Widerrufbarkeit der Einwilligung ist nicht gegeben, da einmal gemachte Angaben nicht zurückgenommen werden können.

Besonders kritisch ist die Einwilligungslösung auch im Hinblick auf den Drittstaatentransfer zu bewerten. Eine Übermittlung von personenbezogenen Daten in ein Bestimmungsland ohne angemessenes Schutzniveau ist vor allem in Fällen, in denen der spätere Widerruf der Einwilligung Probleme verursachen könnte, auch nach Ansicht der Art.-29-Datenschutzgruppe äußerst zweifelhaft. Im Ergebnis wären Einwilligungen daher unwirksam.

Die französische Datenschutzaufsichtsbehörde ist im Jahr 2004 zu einem entsprechenden Ergebnis in Bezug auf das französische Datenschutzrecht gekommen.

Die Gesamtproblematik ist auch Gegenstand politischer Bemühungen auf europäischer Ebene. Es bleibt zu hoffen, dass eine Lösung durch gegenseitige Anerkennung der jeweiligen nationalen Kontrollinstitutionen und -mechanismen für die Tätigkeit der Wirtschaftsprüfer erzielt wird.

10. Teledienste, Neue Medien, Internet-Provider

10.1 Auskunftserteilung auch bei fehlender Verantwortung für die Datenspeicherung?

Im Zusammenhang mit der ständig weiter ansteigenden Flut von unverlangten Werbezusendungen per Telefax und E-Mail versuchten viele Betroffene, ihre datenschutzrechtlichen Ansprüche geltend zu machen. In der Regel verlangten die Betroffenen zunächst Auskunft über die zu ihrer Person gespeicherten Daten sowie über deren Herkunft und über mögliche Empfänger. Verantwortliche Stellen im Sinne des § 3 Abs. 7 BDSG bzw. Diensteanbieter nach § 2 Nr. 1 TDDSG sind nach den Regelungen des § 34 Abs. 1 Nr. 1 BDSG und des § 4 Abs. 7 TDDSG gesetzlich verpflichtet, den Betroffenen mitzuteilen, welche Daten bei ihnen gespeichert sind, woher diese Daten stammen und an welche Stellen die Daten übermittelt wurden. Die Auskunftserteilung stellt nach § 6 Abs. 1 BDSG ein unabdingbares Recht der von einer Datenverarbeitung oder -nutzung betroffenen Personen dar, ohne dessen Realisierung die Rechte auf Berichtigung, Löschung oder Sperrung der Daten (§ 35 BDSG) ins Leere laufen würden.

Leider geben sich die Versender solcher unerwünschten Werbezusendungen in vielen Fällen nicht zu erkennen oder fälschen sogar die Angaben über den vermeintlichen Absender, um den Betroffenen und den Aufsichtsbehörden keinen Ansatzpunkt für ein datenschutzrechtliches Vorgehen zu geben. So werden z.B. in Telefaxen, die für betrügerische Angebote im WWW werben oder die zur Anwahl von teueren ausländischen Telefon- oder Telefaxnummern verleiten sollen, falsche Namen und Firmenbezeichnungen mit deutschen Anschriften als Absender angegeben. Bei der Versendung unverlangter Werbe-E-Mails ist es mittlerweile sogar die Regel, dass die Angaben über den Absender der E-Mail gefälscht werden. In einigen Fällen werden dabei auch die Daten real existierender Unternehmen missbraucht und als Absender angegeben, um die Seriosität und Glaubwürdigkeit des unerwünschten Angebots zu erhöhen.

Die datenschutzrechtlichen Auskunftsersuchen der belästigten Bürgerinnen und Bürger richten sich in diesen Fällen unverlangter Werbung mit gefälschten Absenderangaben an Unternehmen, die für diese unzulässigen Datennutzungen zu Werbezwecken nicht verantwortlich sind und die mit den unseriösen Anbietern in keiner Form zusammenarbeiten. Bei den Firmen befinden sich auch keinerlei Daten über die Betroffenen, über die im Sinne der oben angegebenen Vorschriften Auskunft erteilt werden könnte. Die gesetzliche Verpflichtung nach § 34 BDSG zur umfassenden Auskunftserteilung erfordert jedoch grundsätzlich auch, dem Antragsteller entsprechende Nachricht zu geben, wenn zu seiner Person keine durch das Bundesdatenschutzgesetz geschützten Daten gespeichert sind. Auch dies ist eine Form der Auskunft (Simitis, Kommentar zum Bundesdatenschutzgesetz, 5. Auflage, Mallmann zu § 34 Rdnr. 14). Es ist selbstverständlich, dass die SCHUFA, Handelsauskunfteien und sonstige verantwortliche Stellen auf Auskunftsersuchen auch dann antworten müssen, wenn zu der betreffenden Person keine Daten gespeichert sind.

Die geschilderte Fallgruppe ist allerdings insoweit etwas anders gelagert, als die Unternehmen, an die sich die Anfragen richten, gar nicht verantwortliche Stellen für die Datenverarbeitung und -nutzung sind, welche zu der Anfrage führte, sondern sich insoweit in einer "Opferrolle" befinden. Dennoch ist den betroffenen Unternehmen in solchen Fällen gefälschter Absenderangaben zu raten, den Anfragern eine entsprechende Antwort darüber

zukommen zu lassen, dass keine personenbezogenen Daten gespeichert waren bzw. sind und daher auch keine Auskunft über Herkunft und mögliche Empfänger erteilt werden kann. Wenngleich eine Auskunftsverpflichtung nach § 34 BDSG in solchen Fällen nicht offensichtlich ist, spricht die grundsätzlich gebotene extensive Auslegung des § 34 Abs. 1 BDSG (Bergmann/Möhrle/Herb, BDSG, § 34 Rdnr. 7) dafür, dass den Anfragern eine derartige Antwort zu geben ist.

Die Aufsichtsbehörde konnte aufgrund einer Beschwerde über die Nichtbeantwortung eines solchen Auskunftsersuchens durch einen südhessischen Teledienstеanbieter feststellen, dass das Unternehmen wirklich keinerlei Daten über den Betroffenen gespeichert hatte und auch nicht der Absender der unverlangten Werbung sein konnte. Dass das Unternehmen die Anfrage des Petenten zunächst nicht beantwortete, erweckte allerdings bei dem Betroffenen den Eindruck, man habe auf Unternehmensseite etwas zu verheimlichen. Letztlich festigte sich hierdurch die Auffassung des Beschwerdeführers, das Unternehmen würde versuchen, seinen Umsatz durch unzulässige Marketingmaßnahmen zu steigern, was dann auch zur Eingabe bei der Datenschutzaufsichtsbehörde führte.

Auch bei solchen Konstellationen sollte Betroffenen also Auskunft über die gespeicherten personenbezogenen Daten gegeben werden, selbst wenn ihnen lediglich mitgeteilt werden kann, dass eben keine Daten gespeichert sind. Nur so wird den Betroffenen die Möglichkeit eröffnet, weiter nach den wirklichen Versendern der unverlangten Werbung zu forschen, um ihre weitergehenden datenschutzrechtlichen Ansprüche bei den tatsächlich verantwortlichen Stellen geltend machen zu können. Zudem kann es gerade in solchen Fällen betrügerischer Angebote zu einer erheblichen Rufschädigung für betroffene Unternehmen kommen, wenn auf Auskunftsersuchen nach § 34 Abs. 1 BDSG nicht reagiert wird. Die Betroffenen fühlen sich dadurch in ihrer - an sich falschen - Beurteilung der Sachlage bestätigt, dass die Unternehmen sehr wohl verantwortlich für die unzulässigen Datennutzungen zu Werbezwecken seien, obwohl deren Firmendaten eigentlich von den echten aber in der Regel unbekannten Versendern als Absenderangaben missbraucht wurden.

10.2 Verwendung von Pseudonymen beim Whois-Dienst der DENIC e.G.

Die Zulässigkeit der Veröffentlichung personenbezogener Daten im Internet über den Whois-Server der DENIC e.G. in Frankfurt am Main, die zentrale deutsche Vergabestelle für Internet-Domains unterhalb der Top-Level-Domain "de", wurde im 13. und 15. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden für die Jahre 1999 und 2001 (LT-Drucks. 15/1539, Nr. 9.2 und LT-Drucks. 15/4659, Nr. 8.7) bereits ausführlich dargestellt. Obwohl die Zahl der Eingaben über diese Veröffentlichungen der DENIC e.G. seither rückläufig ist, gehen immer noch vereinzelte Beschwerden von Domain-Inhabern bei der zuständigen Aufsichtsbehörde ein. Diese verfügen zwar über zumeist umfangreiche Homepages im WWW, haben aber in der Regel keine Kenntnisse über die Funktion der weltweit in so gut wie allen Ländern vorhandenen nationalen Domainvergabestellen und die Veröffentlichungspraxis der jeweiligen Whois-Dienste. Sie wenden sich daher mit der Bitte um Abhilfe an die für die DENIC e.G. zuständige Aufsichtsbehörde.

Im Rahmen der Bearbeitung einer solchen Eingabe bat ein Beschwerdeführer - nachdem er zuvor von der Datenschutzaufsichtsbehörde über die Zulässigkeit der Veröffentlichung seiner Daten durch die DENIC e.G. in Kenntnis gesetzt wurde - um Unterstützung bei der Durchsetzung seines Wunsches, dass künftig nicht mehr sein wirklicher Vor- und Nachname beim Whois-Dienst der DENIC e.G. abgefragt werden kann, sondern stattdessen ein Pseudonym veröffentlicht wird. Unter diesem Pseudonym, das auch beim Finanzamt angemeldet sei, publiziere er als freier Schriftsteller auf seiner Homepage einige Texte. Er wollte auf diese Weise verhindern, dass seine Veröffentlichungen über die Angaben bei der DENIC e.G. ihm persönlich zugeordnet werden können. Das Pseudonym habe für ihn die Funktion eines "Künstlernamens", der nach andauernder Nutzung von mindestens zehn Jahren nach dem Pass- oder Personalausweisgesetz schließlich auch in den Ausweis eingetragen werden könne.

Die Aufsichtsbehörde konnte dem Ansinnen des Petenten allerdings nicht folgen. Die bei der DENIC e.G. registrierten und in der Whois-Abfrage ersichtlichen Daten eines Domain-Inhabers sind erforderlich, um den Domain-

Inhaber eindeutig zu bestimmen (vgl. 13. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, LT-Drucks. 15/1539, Nr. 9.2). Die veröffentlichten Daten bieten Anknüpfungspunkte unter anderem für Fragen des Lizenz-, Namens-, und Urheberrechtes und tragen erheblich zur Förderung der Rechtssicherheit im Sinne des Verbraucherschutzes im Internet bei. Es wäre nicht akzeptabel, wenn ein Domain-Inhaber für die Domainregistrierung einfach einen Phantasienamen benutzen würde, da in diesem Fall die eindeutige und beweisbare Zuordnung zu der dahinter stehenden Person nicht gewährleistet wäre und damit z.B. auch Klagezustellungen kaum noch möglich wären.

Auf die Verwendung eines Pseudonyms könnte nur dann ein Anspruch bestehen, wenn dieses Pseudonym eindeutig und für Dritte klar erkennbar mit der betreffenden Person dauerhaft verknüpft ist, also von ihr möglichst umfassend verwendet wird und ausreichend "gefestigt" ist. Schließlich erfolgt auch die Eintragung in den Personalausweis nach zehn Jahren nur dann, wenn eine gewisse Bekanntheit unter diesem Künstlernamen besteht, die den zuständigen Behörden in diesen Fällen zuvor auch nachgewiesen werden muss.

Der Petent trug das Pseudonym allerdings ausschließlich auf seiner Internet-Seite. Dieser "Künstlername" wurde zudem weder zehn Jahre lang andauernd benutzt noch erfreute er sich einer größeren Bekanntheit - er war im Gegenteil öffentlich vollkommen unbekannt.

Obwohl die Datenschutzaufsichtsbehörde daher im vorliegenden Fall keinen Rechtsanspruch auf den Eintrag des "Künstlernamens" in die Whois-Datenbank der DENIC e.G. anerkennen konnte, wurde dem Beschwerdeführer eine Möglichkeit aufgezeigt, sein Geheimhaltungsinteresse zu wahren, indem er anstelle seiner eigenen Daten den Namen und die Anschrift eines Vertretungsberechtigten bei der Domainregistrierung eintragen lässt. Dabei muss es sich nicht immer um einen Rechtsanwalt oder Notar handeln, da die DENIC e.G. es auch akzeptiert, wenn die Eintragung auf eine andere Person (z.B. aus der Verwandtschaft oder dem Bekanntenkreis) vorgenommen wird, die dann im Sinne eines Treuhänders als Domaininhaber bzw. als "admin-c:" bei der Whois-Abfrage auftritt.

10.3 WWW-Veröffentlichungen und Suchmaschinen-Ergebnisse

Ein Petent wandte sich mit einer Beschwerde gegen einen großen südhessischen Internet-Provider an die Datenschutzaufsichtsbehörde. Er hatte festgestellt, dass die Inhalte seiner bei diesem Provider gehosteten Homepage über die WWW-Suchmaschine "Google" auffindbar sind. Er ging davon aus, dass sein Internet-Provider, dessen Speicherplatz er für die Erstellung seiner eigenen privaten Homepage im WWW nutzt, ohne ihn zu informieren oder seine Einwilligung einzuholen, umgehend die Inhalte seiner Seiten an die Suchmaschine übermittelt habe, und bat darum, dem Unternehmen diese Übermittlungen zu untersagen. Er wolle selbst bestimmen, wo seine Inhalte auffindbar sein sollen, wie das bei anderen WWW-Verzeichnissen und Web-Katalogen üblich sei.

Zunächst wurde der Petent darauf hingewiesen, dass Suchmaschinen selbstständig mithilfe so genannter "Web-Crawler" das Internet nach veröffentlichten Inhalten durchsuchen, diese anhand von Schlagwörtern sammeln, mittels einer anspruchsvollen Ranking-Technik bewerten und den Suchenden dann die Treffer präsentieren. Ein aktiver Eintrag von Inhalten in deren Datenbank ist nicht immer erwünscht und auch nur sehr bedingt möglich. Hierin unterscheiden sich Internet-Suchmaschinen ganz wesentlich von WWW-Verzeichnissen, Web-Katalogen oder auch inhaltlich orientierten Web-Portalen. Dort ist es in der Regel notwendig, aktiv einen Eintrag vorzunehmen, wenn man gefunden werden möchte. Diese Kataloge suchen aber auch - anders als eine Suchmaschine - bei ihrer Inanspruchnahme nicht das gesamte Internet ab, sondern liefern lediglich Ergebnisse aus ihrer eigenen lokalen Datenbasis. Beispielsweise erfolgt ein "Google-Treffer" nicht, weil der Host-Provider den Petenten bzw. seine Inhalte dorthin gemeldet habe, sondern weil "Google" selbst die von dem Petenten veröffentlichten Inhalte gefunden hat.

Aus datenschutzrechtlicher Sicht ist zudem nicht der Host-Provider für die von seinen Kunden auf deren privaten Homepages veröffentlichten Inhalte verantwortlich. Das Unternehmen bietet hierfür im Rahmen seiner üblichen Tarife seinen Kunden lediglich Speicherplatz an und tritt in dieser Konstella-

tion als Anbieter von fremden Inhalten auf. Wenn sich ein Kunde entschließt, selbst eine eigene Homepage auf dem ihm zur Verfügung stehenden Speicherplatz ins WWW zu stellen, wird er aus datenschutzrechtlicher Sicht selbst zum Anbieter im Sinne des § 3 Nr. 1 Teledienstegesetz (TDG) und ist für diese Veröffentlichungen nach § 8 Abs. 1 TDG selbst verantwortlich. Der Beschwerdeführer hat es als Anbieter also selbst in der Hand zu bestimmen, was auf seiner Homepage veröffentlicht werden soll und was eben nicht. Wer Inhalte im WWW veröffentlicht, macht diese einer unbekannten Anzahl von Empfängern allgemein zugänglich.

In der Praxis haben die Betroffenen allerdings mehrere Möglichkeiten, hierauf Einfluss zu nehmen. Sie können ihre Homepage z.B. mit einer Passwortabfrage ausstatten, was dazu führt, dass nur bestimmte Nutzer, denen das Passwort bekannt ist, an die Inhalte gelangen können (geschlossene Benutzergruppe). Wen es stört, dass veröffentlichte Inhalte von Suchmaschinen wie z.B. "Google" gefunden werden, kann allerdings durchaus eine Indizierung und Archivierung seiner WWW-Seiten durch Suchmaschinen verhindern oder sogar rückgängig machen. Entsprechende Hinweise sind üblicherweise auf den Suchmaschinen-Seiten - auch bei "Google" - abrufbar. Mit einem ergänzenden Hinweis auf "WWW.robotstxt.org/wc/robots.html", wo zusätzliche weiterführende Informationen zu dem Standardprotokoll vorhanden sind, mit dem die von Suchmaschinen eingesetzten "Web-Crawler" arbeiten und mit dem man Webseiten aus einem Suchmaschinenindex entfernen oder die Aufnahme verhindern kann, konnte der Beschwerdeführer letztlich zufrieden gestellt werden.

11. Private Bildungseinrichtungen

Zwei Fälle aus dem privaten Bildungswesen zeigen, dass in diesem Bereich die datenschutzrechtliche Zulässigkeit von Veröffentlichungen und Übermittlungen nicht immer ausreichend geprüft wird.

In einem Fall veröffentlichte eine private branchenspezifische Bildungseinrichtung die Klausurergebnisse ihrer Studenten mit vollem Namen am schwarzen Brett in der Eingangshalle. Damit wurden diese Informationen für jegliche Dritte, also alle Mitstudenten, Dozenten, Gasthörer, Kunden und sonstigen Personen zugänglich gemacht. Bei einer Prüfung vor Ort wurde die Bildungseinrichtung aufgefordert, die Notenaushänge nur noch mit Kennziffern vorzunehmen, damit unbefugte Dritte keine Kenntnis von den Personenbezügen erhalten.

Eine andere nicht öffentliche Bildungseinrichtung übersandte allen Teilnehmern und Referenten von Seminaren die vollständigen Adresslisten der Seminarteilnehmer sowie die Auswertungen der Referentenbeurteilungen, die die Seminarteilnehmer abgegeben hatten.
Auch hier musste die Aufsichtsbehörde anmahnen, dass solche Übermittlungen ohne eine wirksame Einwilligung der Betroffenen unterbleiben müssen.

12. Weitergabe gebrauchter Mobiltelefone

Die mobile Kommunikation über Handys ist mittlerweile aus dem Alltagsleben nicht mehr wegzudenken. Die Betreiber der Mobilfunkfunknetze versuchen, durch günstige Sonderangebote immer mehr Kunden zu gewinnen, teilweise werden hochwertige Handys bei Abschluss eines neuen Vertrages oder bei der Vertragsverlängerung sogar an die Kunden verschenkt. Als Nebeneffekt dieses Verhaltens gibt es in Deutschland mittlerweile Millionen gebrauchter Alt-Handys, die von den ehemaligen Besitzern in vielen Fällen auch an andere Personen weitergegeben werden.

Vor diesem Hintergrund muss auch eine Anfrage gesehen werden, die im Berichtsjahr an die Aufsichtsbehörde gerichtet und in der um eine datenschutzrechtliche Beurteilung gebeten wurde, ob die Weitergabe eines Handys im Falle des Verkaufs oder der Spende an eine gemeinnützige Organisation zulässig ist, wenn in dem Gerät noch Daten (Telefonnummern, Adressen usw.) von Kommunikationspartnern des ehemaligen Handy-Besitzers gespeichert sind, die dieser Übermittlung ihrer Daten nicht zugestimmt und auch keine Kenntnis davon haben.
Die Aufsichtsbehörde wies darauf hin, dass die in einem Handy gespeicherten Daten anderer Personen (Namen, Telefonnummern, Adressen usw.) sowie die Listen der eingegangen, ausgegangenen und entgangenen Anrufe und auch die gespeicherten MMS- und SMS-Nachrichten nach § 3 Abs. 1

BDSG als personenbezogene Daten zu beurteilen sind. Bei der Erhebung und Nutzung dieser Daten durch den Handy-Besitzer kann davon ausgegangen werden, dass es sich um eine familiäre oder persönliche Tätigkeit des Handy-Besitzers handelte. Somit wäre die Anwendung des Bundesdatenschutzgesetzes nach § 1 Abs. 2 Nr. 3 für diese Verarbeitung personenbezogener Daten grundsätzlich ausgeschlossen.

Das gilt allerdings nicht uneingeschränkt für die Weitergabe des Handys an Dritte. Mit der Weitergabe könnten das Handy und damit auch die gespeicherten Daten den persönlichen bzw. familiären Bereich verlassen. Das Gesetz wäre dann voll anwendbar. Bei der Weitergabe würden personenbezogene Daten übermittelt. Diese Übermittlung wäre ohne Einwilligung der Betroffenen unzulässig, da es keine andere Rechtsgrundlage im Bundesdatenschutzgesetz hierfür gibt. Auch der ansonsten für Nutzungen und Übermittlungen einschlägige § 28 BDSG kann in diesem Fall nicht als Rechtsgrundlage für eine Übermittlung herangezogen werden, da die schutzwürdigen Interessen der von einer Übermittlung betroffenen Nummerninhaber deutlich überwiegen. Sämtliche im Handy gespeicherten personenbezogenen Daten müssen daher vom Eigentümer eines Handys vor der Weitergabe des Geräts an kommerzielle Händler oder auch an gemeinnützige Organisationen gelöscht werden.

Ein Händler oder eine sonstige verantwortliche Stelle nach § 3 Abs. 7 BDSG, die Handys direkt von den Eigentümern sammelt oder aufkauft, um diese dann weiterzugeben oder zu verkaufen, aus kommerziellen oder auch mildtätigen Gründen, sollte ihrerseits diese Eigentümer zuvor darauf hinweisen, dass alle internen Speicher des Geräts zuvor zu löschen sind und sich die Löschung dieser Daten auch schriftlich vom Alt-Eigentümer bestätigen lassen. Es ist dieser Stelle zudem zu empfehlen, zusätzlich zu den erfolgten Hinweisen an die Alt-Eigentümer der Mobiltelefone mit angemessenem Aufwand nachzuprüfen, ob die entsprechenden Speicher der Geräte wirklich gelöscht sind oder noch Daten enthalten. Falls entdeckt wird, dass noch Daten vorhanden sind, sind diese zu löschen, da ansonsten eine datenschutzrechtlich unzulässige Übermittlung personenbezogener Daten zu befürchten wäre, die den Bußgeldtatbestand des § 43 Abs. 2 Nr. 1 BDSG erfüllen kann.

Auf die Anfrage wurde ferner mitgeteilt, dass auch beim Verschenken des Handys innerhalb der Familie oder an persönliche Freunde und Bekannte die Privatsphäre der betroffenen Rufnummerninhaber grundsätzlich beachtet werden sollte, selbst wenn hier das Bundesdatenschutzgesetz nicht angewandt werden kann. Nicht nur die Persönlichkeitsrechte der Betroffenen, deren Angaben im Handy gespeichert sind, werden durch eine Datenübermittlung gefährdet. Auch der Besitzer des Handys würde mit der Weitergabe des Geräts ohne vorherige Datenlöschung einen Teil seines Kommunikationsverhaltens und seine gespeicherten Kommunikationspartner offenbaren. Schon aus diesem Grund ist es nach Auffassung der Aufsichtsbehörde auch ohne gesetzlichen Grund nahe liegend, sämtliche Daten des eigenen Mobiltelefons vor der Weitergabe - an wen auch immer - zu löschen.

13. Werbung, Direktmarketing

13.1 Leitfaden des Deutschen Direktmarketingverbandes (DDV)

Der DDV mit Sitz in Wiesbaden hat im Jahr 2001 einen Leitfaden zu den Auswirkungen der BDSG-Novelle auf das Direktmarketing erstellt.

Wie bereits im 16. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden (LT-Drucks. 16/1680, Nr. 16.1) ausgeführt, fand hierzu ein intensiver Meinungsaustausch zwischen dem DDV und der Aufsichtsbehörde statt, die ihrerseits alle obersten Aufsichtsbehörden im Bundesgebiet informierte.

Die im September 2002 vom DDV herausgegebene zweite Auflage des Leitfadens berücksichtigte die Kritik der Aufsichtsbehörden zum Teil, wurde jedoch vom DDV erfreulicherweise erneut als "offener Diskussionsbeitrag" bezeichnet. Der Dialog wurde fortgesetzt und im März 2004 erschien eine dritte überarbeitete Auflage des Leitfadens, der - ebenso wie die Vorauflagen - auch Nichtmitgliedern zugänglich ist.
Wenngleich nicht in allen Punkten volle Übereinstimmung mit der Auffassung der Aufsichtsbehörden besteht, enthält diese dritte Auflage doch eine weitgehende Angleichung der Standpunkte.

13.2 Internationalisierung der Werbewirtschaft

Neu ist in vielen Fällen der hohe Ermittlungsaufwand bis die verantwortliche Stelle gefunden ist - hier wirkt sich die Internationalisierung der Werbewirtschaft aus.

Es zeigt sich einmal mehr die Bedeutung des § 28 Abs. 4 Satz 2 BDSG, wonach der Betroffene bei der Ansprache zum Zwecke der Werbung auch über die verantwortliche Stelle zu informieren ist. Diese Information kann nicht nur für den Verbraucher, sondern auch für die Aufsichtsbehörde sehr hilfreich sein.

Ein Beispiel ist hier der Fall eines Unternehmens, das mit Gewinnzusagen wirbt. In personalisierten Werbezusendungen wendet es sich mit einer Mitteilung über einen Gewinn an den Adressaten. Durch die Gestaltung dieser Zusendung wird der Eindruck erweckt, der Preis sei bereits gewonnen und stehe schon zur Entgegennahme bereit.

Nach Recherchen der Aufsichtsbehörde ist der vermeintliche Firmenname jedoch nur eine Produktbezeichnung. Die angegebene Adresse des Unternehmens ist nur eine Postfachadresse. Es gibt außerdem ein "Service-Telefon-Deutschland", das mit einer 0180-Nummer angewählt werden kann. Dahinter verbirgt sich aber ein Call-Center, das jegliche Auskunft über seinen Auftraggeber verweigerte. Es wird deutlich, wie schwierig hier die Suche nach den Verantwortlichen ist.

Der Beschwerdeführer hatte keine Auskunft über die Herkunft seiner Daten erhalten. Auf dem Werbematerial fehlte der Widerspruchshinweis. Auf seine Beschwerde, die der Betroffene an die Postfachadresse gerichtet hatte, erhielt er von einem Unternehmen in Frankreich zwar die Auskunft, seine Daten seien für weitere Werbezusendungen gesperrt, aber keine Auskunft über die Herkunft seiner Daten.

Da trotz umfangreicher Nachforschungen kein Nachweis für die Existenz einer Niederlassung in Deutschland gefunden werden konnte, war nach § 1 Abs. 5 Satz 1 BDSG von der Geltung französischen Datenschutzrechts auszugehen.

Nachdem die hessische Aufsichtsbehörde keine weitere Möglichkeit gesehen hatte, den Fall in Deutschland aufzuklären, musste die zuständige französische Aufsichtsbehörde eingeschaltet werden, welche - mit dem Einverständnis des Beschwerdeführers - die weitere Bearbeitung der Beschwerde übernahm.

Wiesbaden, 14. Februar 2005

Der Hessische Ministerpräsident:
Koch

Der Hessische Minister des Innern und für Sport:
Bouffier