17. Wahlperiode

Drucksache **17/663**

HESSISCHER LANDTAG

16. 09. 2008

Vorlage
der Landesregierung

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

Vorgelegt mit der Stellungnahme zum Sechsunddreißigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten (Drucks. 16/8377) nach § 30 Abs. 2 des Hessischen Datenschutzgesetzes in der Fassung vom 7. Januar 1999.

Eingegangen am 16. September 2008 · Ausgegeben am 23. September 2008
Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

Überblick und Statistiken

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

1.1 Bearbeitung von aktuellen Eingaben und Beschwerden

Das Regierungspräsidium Darmstadt überprüft als Aufsichtsbehörde für den nicht öffentlichen Bereich nach § 38 Abs. 1 BDSG die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz in Hessen, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln.

Im Berichtsjahr wurden von der Aufsichtsbehörde in 658 Fällen (im Vorjahr: 603) Überprüfungen von nicht öffentlichen Stellen vorgenommen, die Datenverarbeitung nach § 28 BDSG für die Erfüllung eigener Geschäftszwecke betreiben oder personenbezogene Daten nach §§ 29, 30 und § 6b BDSG zur personenbezogenen oder anonymisierten Übermittlung speichern und nutzen.

Telefonische Eingaben, die durch telefonische Beratung erledigt werden konnten, wurden dabei bis auf wenige Ausnahmen ebenso wenig erfasst wie solche, die durch die Versendung von Informationsmaterial und Orientierungshilfen erledigt werden konnten.

Die 658 Überprüfungen aufgrund von Eingaben, Beschwerden und Pressemeldungen durch das Regierungspräsidium Darmstadt betrafen:

- in 138 Fällen eine große Auskunftei,
- in 87 Fällen Telemedienanbieter (Anbieter von Internetdiensten und -inhalten, unverlangte E-Mail-Werbung),
- in 66 Fällen Stellen und Unternehmen der Direktmarketing- und Werbewirtschaft,
- in 56 Fällen Banken, Kreditinstitute und EDV-Dienstleister im Zahlungsverkehr,
- in 48 Fällen (andere) Handels- und Wirtschaftsauskunfteien,
- in 42 Fällen Inkassounternehmen,
- in 34 Fällen den Datenschutz in Arbeitsverhältnissen und bei Arbeitsvermittlern,
- in 31 Fällen die Videoüberwachung von Grundstücken, Häusern und Wohnungen,
- in 20 Fällen das Gesundheitswesen (Ärzte, Krankenhäuser, Senioren- und Pflegeheime),
- in 18 Fällen Unternehmen der Freizeit-, Touristik- und Reisebranche,
- in 17 Fällen Unternehmen des Groß- und Einzelhandels,
- in 16 Fällen Versicherungsgesellschaften,
- in 11 Fällen Vermieter sowie Wohnungs- und Immobilienverwaltungsfirmen,
- in 9 Fällen Kreditkartenunternehmen,
- in 8 Fällen Vereine (Sport, Soziales, Kultur) sowie deren Landes- und Bundesverbände,
- in 8 Fällen den Verlags- und Medienbereich,
- in 5 Fällen Unternehmen der Versandhandelsbranche,
- in 4 Fällen Adresshandelsunternehmen,
- in 4 Fällen die Auslandsdatenverarbeitung,
- in 4 Fällen Markt- und Meinungsforschungsunternehmen,
- in 2 Fällen Anwaltskanzleien,
- in 30 Fällen sonstige Stellen (z.B. politische Parteien, Briefzusteller)

Bei ca. 17 v.H. der Beschwerden konnte zeitnah festgestellt werden, dass diese begründet waren. In insgesamt 108 Fällen wurden bei den Nachforschungen der Aufsichtsbehörde unzulässige Verarbeitungen personenbezogener Daten und andere Verstöße gegen Vorschriften des Datenschutzrechts und des Rechts der Telemedien festgestellt, die zu Beanstandungen der jeweiligen Verarbeitungsverfahren bei den betroffenen Stellen führten.

Die bei den Überprüfungen beanstandeten 108 Verstöße gegen Datenschutzbestimmungen wurden festgestellt:

- in 23 Fällen bei Auskunfteien (22 Fälle betrafen diesselbe Auskunftei),
- in 15 Fällen bei Anbietern von Telemedien im Internet (Content-Provider und Versender von Werbe-E-Mails),

- in 19 Fällen bei Unternehmen der Direktmarketing- und Werbebranche,
- in 12 Fällen bei Kreditinstituten und Banken (davon war in einem Fall ein Vertragspartner der Bank ursächlich),
- in 12 Fällen bei der Videoüberwachung,
- in 6 Fällen bei der Verarbeitung von Arbeitnehmer- und Bewerberdaten,
- in 4 Fällen bei Unternehmen der Freizeit-, Touristik- und Reisebranche,
- in 3 Fällen bei der Auslandsdatenverarbeitung,
- in 3 Fällen im Groß- und Einzelhandel,
- in 2 Fällen bei der Markt- und Meinungsforschung,

sowie in jeweils einem Fall bei einem Inkassounternehmen, einem Kreditkartenunternehmen, bei einem Verein, einer Versicherungsgesellschaft, einem Unternehmen im Verlags- und Medienbereich sowie bei vier sonstigen Stellen.

Ein Teil der eingeleiteten Überprüfungen konnten im Berichtsjahr noch nicht abgeschlossen werden. Die Erledigung dieser Fälle 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 160 Fälle abgeschlossen. Die Beurteilung dieser in der Regel nur mit hohem Ermittlungsaufwand aufklärbaren Eingaben durch das Regierungspräsidium ergab, dass davon 66 Eingaben begründet waren. Damit musste die Aufsichtsbehörde bei mehr als 40 v.H. dieser Fälle einen Datenschutzverstoß feststellen.

Die beanstandeten 66 Verstöße gegen Datenschutzbestimmungen wurden festgestellt:

- in 18 Fällen bei Anbietern von Telemedien (Internetprovider, WWW-Anbieter),
- in 11 Fällen bei Unternehmen der Freizeit-, Touristik- und Reisebranche,
- in 5 Fällen bei Arbeitgebern und Arbeitsvermittlern,
- in 5 Fällen bei Unternehmen der Werbewirtschaft und werbenden Einzelhändlern,
- in 5 Fällen bei der Videoüberwachung,
- in 4 Fällen im Gesundheitswesen,
- in 4 Fällen im Groß- und Einzelhandel,
- in 4 Fällen bei einer Auskunftei,
- in 3 Fällen bei Vereinen und Verbänden,

sowie in jeweils einem Fall bei einem Adresshändler, bei der Auslandsdatenverarbeitung, bei einer Bank, einem Kreditkarten- und einem Versicherungsunternehmen, bei einem Vermieter sowie bei einem Sicherheitsunternehmen.

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

Die Aufsichtsbehörde entscheidet nach pflichtgemäßem Ermessen, wann und in welchem Unternehmen eine Kontrolle vor Ort durchgeführt wird.

Einen besonderen Schwerpunkt bildete - auch aufgrund zahlreicher Anfragen und Eingaben - die Überprüfung von Videoüberwachungseinrichtungen. Insgesamt wurden im Berichtsjahr 31 Kontrollen vor Ort durchgeführt.

Diese betrafen folgende Branchen/Bereiche:

- Videoüberwachungssysteme	17
- Ärztliche Praxen/Kliniken/Laboratorien/Verrechnungsstellen	4
- Vereine/Verbände	2
- Inkasso-Unternehmen	2
- Sonstige	6

Dabei wurden folgende Mängel am häufigsten festgestellt:

1. Voraussetzungen des § 6b Abs. 1, Abs. 3 - 5 BDSG bei der Videoüberwachung nicht erfüllt,

2. Voraussetzungen des § 6b Abs. 1, Abs. 3 - 5 BDSG bei der Videoüberwachung erfüllt, aber die erforderliche Information zur Videoüberwachung fehlte (§ 6b Abs. 2 BDSG),
3. Fahrlässiger Umgang mit sensiblen Unterlagen hinsichtlich der Löschung dieser Unterlagen,
4. Fehlendes oder inhaltlich unzureichendes Verfahrensverzeichnis,
5. Fehlende Vorabkontrolle,
6. Mangelnde Fachkunde der zum Datenschutzbeauftragten bestellten Personen.

Darüber hinaus bestand oftmals weiterer Anlass für Beanstandungen, wie auch in den vorangegangen Tätigkeitsberichten bereits aufgezeigt wurde.

Bezüglich Einzelheiten bei der Durchführung der Vorortkontrollen wird auf die ausführliche Darstellung unter Ziffer 1.3 des 20. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden (Drucks. 16/7646) verwiesen.

2. Bearbeitung von Anfragen zu datenschutzrechtlichen Problemstellungen und Beratungstätigkeit

2.1 Anfragebearbeitung und datenschutzrechtliche Beratung

Das Regierungspräsidium Darmstadt hatte im Berichtsjahr erneut eine hohe Anzahl von Anfragen und Beratungsersuchen zu bearbeiten. In 289 Fällen (im Vorjahr: 294 Fälle) erfolgte die Beratung und Information von Unternehmen, Vereinen und Verbänden, Bürgerinnen und Bürgern sowie Arbeitnehmerinnen, Arbeitnehmern und Betriebsräten aktenmäßig. 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 statistische Auswertung der 289 Fälle ergab folgende inhaltliche Schwerpunkte:

56 Anfragen zu Kredit-, Handels- und Wirtschaftsauskunfteien
Allgemeine Fragen zu deren Verfahren, insbesondere Erhebung von Gebühren, Rechte der Betroffenen, Fragen zur Speicherung, Aufbewahrung und Löschung von Daten; Beratung zur Implementierung verschiedener Verifikations- und Sicherungsverfahren; Fragen zur Ermittlung des Score-Werts; Aufnahme als Vertragspartner der Auskunftei; Anfrage wegen Gebührenrückerstattung bei falschen Daten in der Selbstauskunft; Angebot von Wirtschaftsauskünften und Bonitätsbewertungen über das Internet; Informationen zum weiteren Vorgehen bei einer Benachrichtigung über die Datenspeicherung (siehe hierzu Ziffer 7.7); Anfragen zu den Voraussetzungen für die Speicherung von Daten und für die Erteilung von Bonitätsauskünften; Stellungnahme zum Antrag einer Auskunftei für den Bezug von Abdrucken aus dem Schuldnerverzeichnis.

33 Anfragen zum Datenschutz im Internet
Speicherung von Daten bei einem Online-Spiel; Suche von Personen und Namen mittels spezialisierter Suchmaschine (siehe hierzu Ziffer 9.3); Anlegen eines Stammbaums auf der eigenen Homepage mit Namen, Geburtsdaten und den Geburtsorten der Verwandten; Personenbeziehbarkeit der Kfz-Fahrgestellnummer im Rahmen einer Online-Datenbank; Abrufbarkeit eines Zwangsversteigerungstermins auf diversen Webseiten, obwohl Zwangsversteigerung abgewendet werden konnte; Abo- und Kostenfallen - Frage nach Drohung mit Auskunftei-Einträgen (siehe hierzu Ziffern 9.2 und 7.5); Datenverarbeitung eines Vereins für ehrenamtliche Betreuer in einer geschlossenen Benutzergruppe im Internet; Datenerhebung auf der Homepage eines Unternehmens – Beratung zum Datenschutzhinweis; Hinweise der Denic e. G. zum Datenschutz beim Who-is-Dienst; Ausgestaltung und Transparenz der Vertreterreglung bei der Domainregistrierung; Voraussetzung der Anwendung von Google-Analytics; Zulässigkeit der Speicherung von IP-Logdateien zur Gewährleistung der Datensicherheit; Aufzeichnung von Inhaltsdaten von Telefongesprächen zur Fehler- bzw. Störungsbeseitigung in der Telekommunikationsanlage; Zertifizierung der Löschung aller Daten auf den Datenträgern bei Verwertung alter PCs.

31 Anfragen zum Arbeitnehmerdatenschutz
Fragen im Zusammenhang mit einer Whistleblowing-Hotline (siehe hierzu Ziffer 10.1 des 20. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde (Drucks. 16/7646); Rufnummernanzeige bei TK-Anlagen; Sprachaufzeichnung von Telefongesprächen; Offenlegung von Benutzerkennungen und Passwörtern; diverse Fragen zum Archivieren von E-Mails; permanente Öffnung und Inhaltskontrolle von persönlichen E-Mail-Konten der Mitarbeiter; Durchsuchung von Servern in den USA nach nicht genehmigten privaten E-Mails; Software zur Überwachung des E-Mail Verkehrs; Empfehlungen zur Einrichtung eines Telearbeitsplatzes; Beratung hinsichtlich einer Online-Jobbörse; Veröffentlichung von Mitarbeiterbildern auf der Homepage des Unternehmens; Veröffentlichung von Arbeitnehmerdaten sowie Mitarbeiter- und Patientenfotos im Internet; Gewährleistung des Datenschutzes bei der Personaldatenverarbeitung auf Laptops; Umgang mit Bewerbungsunterlagen; Nutzung eines Fragebogens zur Erhebung von Mitarbeiterdaten (hier Erforderlichkeit der z. T. detaillierten Fragen); Auskunftspflicht eines Arbeitnehmers bei Personalfragebögen; Weitergabe von Informationen zu Mitarbeitern an Kaufinteressenten eines Unternehmens und Umgang mit Mitarbeiterdaten bei Veräußerung; Überprüfung einer Einwilligungserklärung zur Übermittlung der Ergebnisse von Einstellungstests von Ausbildungsplatzbewerbern an Mitglieder einer Handwerksinnung; Datenübermittlung des Arbeitgebers an eine Gesellschaft, die die betriebliche Altersversorgung in einem Unternehmen einführen und verwalten möchte; Einsatz eines digitalen Fahrtenschreibers in Firmen-LKW; Kopieren und Aufbewahren der Führerscheine der Mitarbeiter bei Nutzung von Firmen-PKW; Versehen des Führerscheins mit einer elektronischen Plakette zur Führerscheinkontrolle; Erforderlichkeit der Nutzung eines elektronischen Tachographen bei Rettungsdiensten; Nutzung einer in den USA befindlichen und administrierten Datenbank, die die Kompetenzprofile von Mitarbeitern weltweit verfügbar machen soll.

23 Anfragen aus dem Gesundheitssektor
Anfrage, ob ein Sachbearbeiter der Krankenkasse den Bericht des Medizinischen Dienstes der Krankenkasse zur Pflegestufe erhalten darf; Anfrage, ob ein angebotenes Praxisanalyse-Verfahren bekannt und zulässig ist; Überprüfung eines neuen Vertragsmodells über eine überörtliche Teilgemeinschaftspraxis; Voraussetzungen für die Einrichtung einer externen Telefonzentrale für Arztpraxen; elektronische Fallakten zur einrichtungsübergreifenden Kooperation; Notwendigkeit eines von der Anmeldung getrennten Wartezimmers; Richtlinien zur datenschutzrechtlichen Ausbildung von Arztfachhelferinnen; Einführung einer elektronischen Patientenakte in einem Klinikum; Veröffentlichung von Namen in einer "Babygalerie" eines Krankenhauses; Zulässigkeit der Auskunft durch eine Klinik an Gläubiger von Patienten über den Aufenthalt oder die Entlassungsanschrift; Information an Eltern über Suchtmittelprobleme ihres Kindes; Erarbeitung eines Konzepts für Sozialarbeiter zur regelmäßigen schriftlichen Rückmeldung der zu betreuenden Kinder an deren Ärzte; Durchführung einer Nachfolgestudie unter den ehemaligen Teilnehmern einer Arzneimittelstudie; Übermittlung des Geburtsdatums im Rahmen einer medizinischen Studie; Anforderung von Diagnosen durch ein Fitnessstudio; Weitergabe von Gesundheitsdaten durch den Arzt nach einem Verkehrsunfall ohne Personenschaden.

22 Anfragen zur Datenverarbeitung im Ausland
Anfrage zur Verarbeitung von Mitarbeitergesprächsdaten durch Datenverarbeitungsdienstleister in einem Drittstaat; Unterrichtung der Fluggäste über die Übermittlung von Fluggastdaten; Fragen zur Meldepflicht im Zusammenhang mit dem Auslandsdatentransfer; Fragen zu den EU-Standardverträgen (Genehmigungspflicht, Anzeigepflicht usw.); Sicherstellung des datenschutzgerechten Umgangs mit Kundendaten in den USA; Anfrage zu den Voraussetzungen für Datenübermittlungen in ein Drittland, insbesondere zur Datenübermittlung an unselbständige Niederlassungen in Drittstaaten; Fragen zu Safe Harbor (siehe hierzu Ziffer 10.1 und 10.2); Zusammenfassung der globalen Datenverarbeitungstätigkeiten eines Unternehmens in seinen Rechenzentren in den USA; Beratung hinsichtlich eines konzernweit gültigen Datenschutzkonzepts für einen Konzern mit Hauptsitz in den USA; Implementierung eines Supportsystems für Kundenanfragen an mehreren länderübergreifenden Standorten mit zentraler Datenhaltung in den USA durch ein hessisches Unternehmen.

19 Anfragen zum Datenschutz bei Banken
Zulässigkeit des Anfertigens einer Kopie des Ausweises eines Kunden; Anfrage bezüglich Angriffen auf Kreditkartenunternehmen zum Ausspähen der Kartendaten von Kunden; Übertragung eines Kredits nach finanziellen Schwierigkeiten der Bank auf eine andere Bank (siehe hierzu Ziffer 8); Nutzung eines falschen Kopfbogens; Geldtransfer durch einen Anbieter von Bargeldtransfers; Kreditvermittlung über Einzelhandel; Vereinbarkeit der Tätigkeiten des betrieblichen Datenschutzbeauftragten und des Geldwäschebeauftragten; Übermittlung der personenbezogenen Daten von Kreditkartenkunden an Strafermittlungsbehörden; Herausgabe von Adress- und Ausweisdaten bei Transaktionen; Datenübermittlung durch SWIFT (siehe hierzu Ziffer 8.1 des 20. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde (Drucks. 16/7646), Sprachaufzeichnung bei der Kunden-Hotline einer Bank.

18 Anfragen zum betrieblichen Datenschutzbeauftragten
Aufgaben, Rechte und Pflichten des Datenschutzbeauftragten; Möglichkeit der externen Vergabe der Stelle als Datenschutzbeauftragter an Mitarbeiter der externen IT-Betreuung; Informationen zum Verfahrensverzeichnis; Frage zu erforderlichen Schulungen für Datenschutzbeauftragte; Interessenkonflikte bei einem internen Datenschutzbeauftragten, Frage zur Erforderlichkeit der Bestellung eines Datenschutzbeauftragten; Fragen zur rechtssicheren Gestaltung des Aufgabenbereichs im Unternehmen; Mindestbestelldauer eines externen Datenschutzbeauftragten; Fragen zur Erforderlichkeit der Vorabkontrolle.

16 Anfragen zur Datenverarbeitung durch Vereine und Dachverbände
Stadionverbote und Datenschutz; Erhebung von Besteller- und Besucherdaten auf einem Web-Portal zum Verkauf von Tickets; Fragen zur Datenverarbeitung bei Kindergärten u.a. Auskunftsrecht des Kindesvaters gegenüber einem Kindergarten (e.V.); Weitergabe von personenbezogenen Daten durch den Dachverband; Unterscheidung zwischen Trainingsdaten und medizinischen Daten; Übersendung von Befunden und Berichten per Fax; Möglichkeit der Ausgabe der Mitgliederliste an alle Mitglieder; Meldung aller Einsteller eines Reitvereins an die Hessische Tierseuchenkasse; Aushang einer Anwesenheitsliste (Name, Trainingsbeginn, Saunanutzung) in einem Sportverein; Zulässigkeit der Veröffentlichung von Spielerstrafen durch Sportverein/-verband im Internet; weitere Verwendung der im Rahmen des Volksbegehrens zum Nichtraucherschutz-Gesetz erhobenen Daten.

15 Anfragen zur Videoüberwachung
Zulässigkeit der Videoüberwachung auf einem Privatparkplatz; rechtliche Bewertung des Einbaus einer bereits durch die Eigentümergemeinschaft beschlossenen Videoüberwachungsanlage; Fotoaufnahmen zur Wiedererkennung von Personen zur Wahrnehmung des Hausrechts; Überwachung der Außenmauer des Grundstücks durch privaten Grundstückseigentümer; Sprechanlage mit Videofunktion in einer Hochhausanlage; Videoüberwachung in Spielhallen; Überwachung auf städtischem Gelände durch privates Unternehmen; Anfrage über den Einsatz von Außenkameras zur Absicherung eines Firmengebäudes; Installation von Kameras auf oder in Straßenbahnen, um Bilder in Echtzeit auf eine Homepage zu stellen; Installation einer Videokamera an einem Lichtmast der Gemeinde zur Überwachung des Firmengeländes.

6 Anfragen zur Werbewirtschaft und dem Adresshandel
Allgemeine Fragen zum Thema Direktmarketing (siehe auch Ziffer 2.2); Informationen zum Thema "Ethno-Marketing"; Anfragen zu Anrufen diverser Call-Center, die personenbezogene Daten nutzen, Zusendung unerwünschter Werbung; Beratung zum weiterem Vorgehen, wenn ein Unternehmen die Auskunft zu gespeicherten Personendaten verweigert; Anfrage zur Robinson-Liste.

6 Anfragen zum Einzelhandel
Beratung zur datenschutzgerechten Datenverarbeitung beim Einzelhandel; Hinweis auf möglichen Fehler im Impressum; Erhebung der vollständigen Adresse des Kunden bei einem Umtausch; Weitergabe von Energieverbrauchsdaten durch ein Energieversorgungsunternehmen an Gebäudeeigentümer (Energieeinsparverordnung).

5 Anfragen zur Versicherungsbranche
Versicherung fordert Akteneinsicht beim Hausarzt; Bewertung eines Verfahrens, bei dem eine Kfz-Versicherung nur in dem Umfang bezahlt wird, in dem auch das Fahrzeug genutzt wird (Pay as you drive); Beratung bezüglich der datenschutzkonformen Gestaltung des Datenaustauschs in einem Versicherungskonzern; Weiterverkauf des Datenbestands von einem Versicherungsmakler an einen anderen.

5 Anfragen zu Inkassounternehmen
Inkassounternehmen bittet durch Aufsprache auf Anrufbeantworter von Schuldnern um Rückruf; Rechtmäßigkeit der Beauskunftung bestimmter Angaben.

3 Anfragen aus dem Bereich Miete und Wohnen
Einblicksrecht einer Wohnungseigentümergemeinschaft in die Lohnunterlagen des Hausmeisters; Zugrundelegung des Energieverbrauchs ehemaliger Mieter für den Energieverbrauchsausweis bei Neuvermietungen; Zulässigkeit der statistischen Auswertung von bei einem Gewinnspiel erhobenen Stromverbrauchsdaten.

3 Anfragen zur Markt- und Meinungsforschung
Anfrage zur Nutzung von Kundendaten für Marktforschungszwecke; Überprüfung eines verwendeten Fragebogens.

28 Anfragen aus unterschiedlichen Wirtschafts- und Lebensbereichen
Aufbewahrung von Bescheinigungen über die Vernichtung und Löschung von Daten; Aufbewahrungsfrist für Geschäftsunterlagen; Notwendigkeit der Löschung der Daten in einer Anwaltskanzlei nach Beendigung des Streitfalls; Einsichtsrecht eines Gesellschafters einer Immobilien-Anlagegesellschaft in Treugeberverzeichnis; Vorlage von Ausweiskopien zur Einlasskontrolle; Überwachung der Route eines Segelflugzeugs durch ein Antikollisionsgerät; diverse Fragen zum Datenschutz bei Kreditkarten.

2.2 Vorträge, Informationsmaterial und Orientierungshilfen

Im Berichtsjahr lud das Regierungspräsidium Darmstadt zu einer Vortrags- und Informationsveranstaltung zum Datenschutz ein. Nach einer Darstellung der historischen Entwicklung sowie der aktuellen Bedeutung des Datenschutzes im nicht öffentlichen Bereich durch Herrn Regierungsvizepräsidenten Matthias Graf wurden die Tätigkeitsbereiche der Datenschutzbehörde vorgestellt und über die Themen "Auskunfteien", "Datenschutz im Internet" und "betriebliche Überprüfungen" informiert. Darüber hinaus hatten interessierte Bürgerinnen und Bürger die Möglichkeit einer persönlichen Beratung an Informationsständen. Dort konnten sich Interessierte auch noch einige Wochen nach der Veranstaltung auf den ausgestellten Schautafeln über den Datenschutz informieren.
Die Veranstaltung wurde vom Datenschutzdezernat in Zusammenarbeit mit dem Europäischen Informationszentrum im Regierungspräsidium Darmstadt durchgeführt und war Teil einer Veranstaltungsreihe zu europarelevanten Themen. Der Europarat hat im Jahr 2007 erstmals den Europäischen Datenschutztag ausgerufen, um das Bewusstsein für den Datenschutz in ganz Europa zu erhöhen. Diesem Zweck diente auch die Informationsveranstaltung des Regierungspräsidiums Darmstadt.

Darüber hinaus haben Vertreterinnen und Vertreter der Aufsichtsbehörde - wie in den vergangenen Jahren - im Rahmen von Informationsveranstaltungen diverser Veranstalter wieder Fragen zum Datenschutz beantwortet und Vorträge gehalten.

Sowohl an der Frühjahrs- als auch der Herbsttagung des Erfahrungsaustauschkreises Hessen der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. nahm die Aufsichtsbehörde teil und beantwortete die Fragen der anwesenden betrieblichen Datenschutzbeauftragten.

Auch in einer Sitzung des Erfahrungsaustauschkreises Hessen des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V. war die Aufsichtsbehörde vertreten und hielt einen Vortrag zum Thema "Videoüberwachung".

Dem an die Aufsichtsbehörde herangetragenen Wunsch, im Rahmen von Datenschutzfachveranstaltungen über aktuelle Fragestellungen des internationalen Datenverkehrs zu informieren, wurde ebenfalls entsprochen. Diese Fragestellungen und deren Bewertung sind im letzten Tätigkeitsbericht ausführlich behandelt (siehe Ziffer 9 des 20. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde, Drucks. 16/7646). Der Düsseldorfer Kreis (Abstimmungsgremium der obersten Datenschutzaufsichtsbehörden in Deutschland) hat im April 2007 einen entsprechenden Beschluss gefasst sowie ein Positionspapier und eine Handreichung verabschiedet (siehe Ziffer 6). Diese Unterlagen sind auch von der Website der Aufsichtsbehörde abrufbar (http://www.rp-darmstadt.hessen.de , Pfad: Sicherheit & Ordnung/ Datenschutz/Auslandsdatenverkehr).

Der von der Hochschule Darmstadt im Juni 2007 veranstaltete 3. Darmstädter Informationsrechtstag hatte das "Recht der Mediengesellschaft" zum Thema. Hierbei wurden unter anderem Rechtsfragen im Zusammenhang mit der Fußball-Weltmeisterschaft 2006 behandelt. Ein Vertreter der Aufsichtsbehörde war gerne bereit, über die RFID-Technik, die bei der Fußball-Weltmeisterschaft 2006 zum Einsatz gekommen ist, zu referieren. Wie bereits in den letzten Tätigkeitsberichten dargestellt, hatte sich die Aufsichtsbehörde in den Vorjahren eingehend mit der Thematik beschäftigt (siehe Ziffer 11.1.3 des 18. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde, Drucks. 16/4752).

Seit mehreren Jahren besteht schon ein regelmäßiger Kontakt mit der Hochschule Darmstadt. Studenten des Studiengangs "Informationswissenschaft" unter Leitung von Herrn Prof. Dr. Erd besuchen jeweils im Sommersemester die Aufsichtsbehörde, um sich über deren Tätigkeit und aktuelle Themen aus der Aufsichtspraxis zu informieren.

Auch beim Girls´ Day am 25. April 2007 wirkte die Aufsichtsbehörde mit und erläuterte interessierten Mädchen ihre Arbeit anhand bestimmter Themen, zu denen die Mädchen aufgrund ihrer eigenen Lebenserfahrung einen Bezug haben (zum Beispiel Gefahren der Internetnutzung, Selbstschutz, Mobilfunkgebühren und Tätigkeit von Auskunfteien).

Das Angebot an Informationsmaterial, das die Datenschutzaufsichtsbehörde zu unterschiedlichsten Fragestellungen des Datenschutzrechts bereithält, wurde wieder gut angenommen. Im Berichtsjahr wurde das Informationsmaterial vor allem um ein Merkblatt zum Thema Werbewirtschaft ergänzt. Dieses Thema und hier insbesondere die Problematik der unerwünschten Werbung war auch im Berichtsjahr ein Schwerpunkt der Arbeit der Aufsichtsbehörde. Wie bereits in den vorangegangenen Jahren erreichten die Aufsichtsbehörde wieder zahlreiche Beschwerden von Betroffenen, die Schwierigkeiten bei der Durchsetzung ihres Auskunfts- oder Widerspruchsrechts nach dem BDSG hatten (siehe Ziffer 1).
Problematisch ist hier die Abgrenzung des Datenschutzrechts zu anderen Rechtsgebieten wie z.B. dem Wettbewerbsrecht und dem BGB. So ist das Datenschutzrecht im Bereich des E-Mail-, Telefon- und FAX-Marketing grundsätzlich nur von sekundärer Bedeutung, hingegen bei persönlich adressierter postalischer Werbung grundsätzlich allein einschlägig.
Häufig gestellte Fragen Betroffener zu diesem Themenkomplex hat die Aufsichtsbehörde zusammengefasst und in Form des diesem Tätigkeitsbericht beiliegenden Merkblatts "Werbung (un)erwünscht" strukturiert beantwortet (siehe Anlage 1). Dadurch wird dem interessierten und dem betroffenen Bürger eine Orientierungshilfe gegeben, Rechtsbegriffe werden geklärt und Handlungswege aufgezeigt.
Das Merkblatt ist auch von der Website der Aufsichtsbehörde abrufbar (http://www.rp-darmstadt.hessen.de, Pfad: Sicherheit & Ordnung/Datenschutz/-Werbung). Hier sind außerdem weitere Informationsmaterialien zum Thema Werbung verfügbar.

3. Genehmigungsverfahren nach § 4c Abs. 2 BDSG und Abstimmungsverfahren betreffend verbindliche Unternehmensregelungen zum Drittstaatentransfer

Im Berichtsjahr wurde kein konkreter Genehmigungsantrag gestellt. Nach eingehender Beratung durch die Aufsichtsbehörde entschlossen sich die

Unternehmen in aller Regel zur wörtlichen Verwendung der EU-Standardvertragsklauseln, bei der keine Genehmigungspflicht besteht. Vertragsbeitritte zu den Standardvertragsklauseln sowie geringfügige Änderungen oder Ergänzungen, die ausschließlich zugunsten der betroffenen Personen erfolgten, wurden von der Aufsichtsbehörde als nicht genehmigungspflichtig bewertet (siehe Ziffer 9.2 und 9.4 des 20. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde, Drucks. 16/7646).

Lediglich ein Unternehmen, das an die Aufsichtsbehörde herangetreten war und um Beratung und Prüfung eines komplexen Vertragswerkes gebeten hatte, konnte sich nicht zur wörtlichen Verwendung der Standardvertragsklauseln entschließen. Das Vertragswerk ist zwar teilweise an den Standardvertrag angelehnt, weicht aber doch in erheblichem Umfang von diesem ab, sodass nach derzeitiger Bewertung von einem Genehmigungserfordernis auszugehen ist. Da das in Hessen ansässige Unternehmen zu einer internationalen Unternehmensgruppe gehört und der Vertrag als Grundlage für Datenübermittlungen innerhalb dieser Gruppe dienen sollte, wies die Aufsichtsbehörde, wie in vielen vergleichbaren Fällen, auf die folgenden Schwierigkeiten hin. Unabhängig von der Frage der inhaltlichen Genehmigungsfähigkeit des Vertrags hat eine Genehmigungserteilung durch die Hessische Datenschutzaufsichtsbehörde keine Bindungswirkung für andere europäische Datenschutzbehörden, d.h. die Unternehmensgruppe trägt das Risiko, dass die Genehmigungen für die Drittstaatenübermittlungen aus anderen Ländern der Europäischen Union unter Umständen nicht erteilt würden, obwohl sie auf der Grundlage des gleichen Vertragswerks erfolgen, bzw. dass die Datenschutzaufsichtsbehörden in Europa unterschiedliche Forderungen bzgl. einer Modifikation des Vertragswerks stellen.

Eine europaweite Koordination zwischen den Datenschutzaufsichtsbehörden ist bislang nur für verbindliche Unternehmensregelungen zum Datenschutz (sog. Binding Corporate Rules - BCR) vorgesehen, mit denen konzernweit für ein angemessenes Datenschutzniveau gesorgt wird und somit die datenschutzrechtlichen Voraussetzungen für den weltweiten Austausch von personenbezogenen Daten erfüllt werden (siehe Arbeitspapier 107 der Art. 29-Gruppe).
Im konkreten Fall bestand Einigkeit mit den Vertretern der Unternehmensgruppe, dass das Vertragswerk nicht als verbindliche Unternehmensregelung im Sinne des Arbeitspapiers 107 einzustufen ist.

Die Bearbeitung des Vorgangs ist noch nicht abgeschlossen, bei Redaktionsschluss für diesen Bericht war ein weiteres Beratungsgespräch geplant.

Im Berichtsjahr war die Aufsichtsbehörde darüber hinaus in drei Koordinierungsverfahren auf deutscher und europäischer Ebene betreffend verbindliche Unternehmensregelungen einbezogen und hat hierzu ihre Stellungnahme abgegeben.

4. Register der meldepflichtigen Verfahren nach § 4d BDSG

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

Am Ende des Berichtsjahres waren 103 Verfahren von 95 verantwortlichen Stellen im Melderegister eingetragen. Nur vier verantwortliche Stellen haben mehr als ein Verfahren gemeldet.

Davon werden in 56 gemeldeten Verfahren geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung gespeichert (Adresshändler, Handels- und Wirtschaftsauskunfteien, meldepflichtig nach § 4d Abs. 4 Nr. 1 BDSG). Die weiteren 47 der eingetragenen Verfahren dienen dem Zwecke der anonymisierten Übermittlung (Markt- und Meinungsforschung, meldepflichtig nach § 4d Abs. 4 Nr. 2 BDSG).

5. Ordnungswidrigkeitenverfahren

Von drei noch offenen Verfahren aus 2006 wurden zwei mit einem rechtskräftigen Bußgeldbescheid beendet. Ein Verfahren, in dem mehrere Verstöße gegen das BDSG begangen wurden, ist noch beim Amtsgericht anhängig.

Im Berichtsjahr wurden vom Regierungspräsidium Darmstadt acht Verfahren nach dem Ordnungswidrigkeitengesetz (OWIG) eingeleitet.

Verstoß	Grund	Rechtskraft/Bußgeldhöhe
§ 43 Abs. 1 Nr. 1 und § 43 Abs. 1 Nr. 2	Verstoß gegen die Meldepflicht Nichtbestellung eines Datenschutzbeauftragten	Noch anhängig
§ 43 Abs. 1 Nr. 2	Nichtbestellung eines Datenschutzbeauftragten	Noch anhängig
§ 43 Abs. 1 Nr. 10	Nichterteilen von Auskünften	Rechtskräftig (Bußgeld 1000 €)
§ 43 Abs. 1 Nr. 10	Nichterteilen von Auskünften	Verfahren eingestellt nach § 47 I OWIG Empfänger verstorben
§ 43 Abs. 1 Nr. 10	Nichterteilen von Auskünften	Verfahren eingestellt nach § 47 I OWIG, Empfänger abgemeldet nach Frankreich
§ 43 Abs. 1 Nr. 10	Nichterteilen von Auskünften	Noch anhängig
§ 43 Abs. 1 Nr. 10	Nichterteilen von Auskünften	Noch anhängig
§ 43 Abs. 2 Nr. 3	Unbefugte Beschaffung von Daten	Noch anhängig

Wie sich aus der Übersicht ersehen lässt, beruhen die meisten eingeleiteten Ordnungswidrigkeitenverfahren auf Verstößen gegen § 38 Abs. 3 BDSG. In diesen Fällen wurden der Aufsichtsbehörde die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte nicht oder nicht unverzüglich erteilt. In diesen Fällen ist die Einleitung eines Ordnungswidrigkeitenverfahrens geboten, um für die Zukunft ein gesetzeskonformes Verhalten zu erreichen.
Ein Verfahren wurde im pflichtgemäßen Ermessen der Verfolgungsbehörde nach § 47 Abs. 1 Ordnungswidrigkeitengesetz eingestellt, da der Verfahrensbeteiligte verstorben war. Das Verfahren befand sich noch in der Anhörungsphase, sodass die Verfolgungsbehörde das Verfahren im Rahmen ihres Ermessens einstellen konnte. Ein anderes Verfahren wurde ebenfalls eingestellt, da der Beschuldigte sich nach Frankreich abgemeldet hatte und eine weitere Verfolgung einen unangemessenen Aufwand bedeutet hätte.

In einem noch anhängigen Verfahren hatten Mitarbeiterinnen und Mitarbeiter eines Unternehmens bei mehreren Verlagshäusern und Zeitungen Kontaktanzeigen aufgegeben. Diese Anzeigen aus dem Bereich der Partnersuche waren so gestaltet, dass deren Verfasserinnen und Verfasser als Privatpersonen auftraten, eine vermeintlich private Postanschrift verwendeten und keinerlei Hinweise auf eine gewerbliche Tätigkeit gaben. Auf diese also scheinbar von Privatpersonen formulierten Anzeigen sollten Interessierte über Chiffre an den Verlag antworten. Da die Anzeigen als private Kontaktanzeigen aufgegeben und veröffentlicht wurden, unterblieb eine Kennzeichnung des Inserates durch den Hinweis "gewerblich" oder ähnliche Hinweise. Die Interessenten antworteten deshalb in der Annahme, mit Partner suchenden Privatpersonen zu korrespondieren und nicht mit einem gewerblichen Unternehmen.

Tatsächlich aber wurden die in den Antworten der Partnersuchenden enthaltenen Adressen und weitere Informationen soweit angegeben (Telefon- und Mobiltelefonnummern, Berufsbezeichnungen) in das Datenverarbeitungssystem des Unternehmens eingegeben. Für diese Firma tätige Vermittler erhielten monatlich Listen mit diesen Adressen, um über eine Kontaktaufnahme Leistungen des Unternehmens zu vermitteln. Es wurden somit ohne Rechtsgrundlage personenbezogene Daten, die nicht allgemein zugänglich sind, für eine automatisierte Nutzung und Verarbeitung beschafft und erhoben. Den Betroffenen wurde die Möglichkeit genommen, zu entscheiden, ob und welche Daten preisgegeben werden sollten. Unter anderem hatten die Betroffenen in ihren Antwortschreiben auch Daten, die einem besonderen Schutz unterliegen (ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen) offenbart. Die Aufsichtsbehörde geht davon aus, dass die Betroffenen in Kenntnis der tatsächlichen Gegebenheiten diese Daten nicht bekannt gegeben hätten.
Der Ausgang des Verfahrens beim Amtsgericht bleibt abzuwarten.

6. Teilnahme an bundesweiten Arbeitsgruppen des "Düsseldorfer Kreises"

Auch im Berichtsjahr hat sich das Regierungspräsidium Darmstadt wieder an der Arbeit des "Düsseldorfer Kreises" (bundesweites Abstimmungsgremium der Datenschutzaufsichtsbehörden) und den von diesem gebildeten Arbeitsgruppen beteiligt (siehe Ziffer 6 des 20. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde, Drucks. 16/7646).

Seit November 2006 veröffentlicht der Düsseldorfer Kreis die von ihm gefassten Beschlüsse auf der Website des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (http://www.bfdi.bund.de (Pfad: Datenschutz/Entschließungen/Düsseldorfer Kreis)).

Einmal im Jahr treffen sich die Aufsichtsbehörden zu einem Workshop, um sich zu Fragen der praktischen Durchführung der Aufsichtstätigkeit (z. B. Durchführung der Kontrollen vor Ort) auszutauschen. Auch hieran hat die Aufsichtsbehörde wieder teilgenommen.

Ausgesuchte Probleme und Einzelfälle

7. Auskunfteien

7.1 Novelle des Bundesdatenschutzgesetzes/Scoring

Bereits im vorletzten Tätigkeitsbericht hat die Aufsichtsbehörde es begrüßt, dass sich der Bundestag und die Bundesregierung mit der Auskunfteienthematik befassen.
Insbesondere bezüglich der Scoring-Problematik und der sehr weit gefassten generalklauselartigen Abwägungstatbestände erscheint auch aus Sicht des Regierungspräsidiums Darmstadt eine klarere gesetzliche Regelung im BDSG wünschenswert (siehe Ziffer 6.1 des 19. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Drucks. 16/5892).

Im Herbst 2007 hat das Bundesministerium des Innern einen im Schwerpunkt auf den Auskunfteienbereich zielenden Entwurf zur Änderung des Bundesdatenschutzgesetzes erarbeitet und den obersten Aufsichtsbehörden sowie diversen Wirtschafts- und Interessenverbänden zur Stellungnahme zugeleitet. Das Ministerium des Innern und für Sport hat auf der Grundlage eines entsprechenden Berichts des Regierungspräsidiums Darmstadt eine umfangreiche Stellungnahme als oberste Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich in Hessen abgegeben.
Auch im Düsseldorfer Kreis wurde der Gesetzentwurf behandelt. Der Düsseldorfer Kreis begrüßte im November 2007 die Gesetzesinitiative zu Auskunfteien und Scoring. Der diesbezügliche Beschluss ist auf der Homepage des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit veröffentlicht (a.a.O. siehe Ziffer 6). Darin wird die Initiative gewürdigt, die Rechte der Betroffenen zu stärken und insbesondere mehr Transparenz zu gewährleisten. Allerdings bedarf der Entwurf nach Auffassung der obersten Aufsichtsbehörden einer grundlegenden Überarbeitung, damit die Erstellung von umfassenden Persönlichkeitsprofilen vermieden wird, und die Einholung von Bonitätsauskünften auch zukünftig an das Vorliegen eines finanziellen Ausfallrisikos geknüpft bleibt.
Darüber hinaus sollte nach Ansicht der obersten Aufsichtsbehörden klar gestellt werden, dass nur vertragsrelevante Daten in die Berechnung eines Score-Werts einbezogen werden und die Auskunftsrechte der Betroffenen nicht durch die pauschale Berufung auf ein Geschäftsgeheimnis vereitelt werden dürfen.

Nach Beobachtung der hessischen Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich scheint der Trend zum Einsatz von Scoring-Systemen zumindest vor dem Abschluss von Massen-Kreditgeschäften ungebrochen zu sein.

Dem entsprechend ist die Zahl von schriftlichen und telefonischen Anfragen und Beschwerden von Betroffenen zur Berechnung ihrer Score-Werte durch Auskunfteien und Kreditgeber, wie in den vergangenen Jahren, unvermindert hoch.

Die größte Anzahl von Fällen betraf die größte in Hessen ansässige Auskunftei, die Bonitätsauskünfte über Verbraucher erteilt.

Die Auskunfteien verweigern sich nach wie vor der Forderung nach größerer Transparenz, welche, wie im vergangenen Jahr dargestellt (siehe Ziffer 7.4 des 20. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Drucks. 16/7646), zu ausgewogeneren Ergebnissen führen könnte.

Die der Aufsichtsbehörde bekannt gewordenen Sachverhalte deuten auch darauf hin, dass die Bezieher der Score-Werte teilweise aus wirtschaftlichen Erwägungen immer weniger Vorkehrungen treffen, die dazu beitragen könnten, die individuelle Situation von Betroffenen ausreichend zu würdigen.

Die Forderung an Score-Entwickler und Verwender, mehr Ausgewogenheit in ihren Scoring-Verfahren herzustellen, ist daher aufrecht zu erhalten. Nach Ansicht der Aufsichtsbehörde könnte Transparenz im Rahmen gesetzlicher Änderungen vor allem dadurch gefördert werden, dass die Betroffenen Auskunft darüber erhalten, welche Faktoren ihren Score-Wert entscheidend prägen. Zugleich sollte die Möglichkeit der Berufung auf Geschäftsgeheimnisse seitens der Score-Entwickler und Verwender gesetzlich klar und eng definierte Grenzen erfahren.

7.2 Bonitätsauskünfte an Versandhandelsunternehmen

Im letzten Tätigkeitsbericht wurde dargestellt, dass die Versandhändler, welche Vertragspartner einer bestimmten Auskunftei sind, unter dem Merkmal "Versandhauskonto" fortlaufend Nachmeldungen über neue Eintragungen ihrer Kunden beziehen konnten (siehe Ziffer 7.1 des 20. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde, Drucks. 16/7646).

In der Diskussion der Aufsichtsbehörden mit den Vertretern der Auskunfteienbranche und dem Versandhandelsverband stellte sich heraus, dass die undifferenzierte fortlaufende Erteilung von Bonitätsauskünften über Versandhandelskunden ein allgemeines Problem im Datenaustausch zwischen Auskunfteien und Versandhändlern ist (vgl. auch den 4. Tätigkeitsbericht des Innenministeriums Baden-Württemberg - Datenschutz im nichtöffentlichen Bereich (2007) Ziffer 3.4 und den 18. Datenschutz- und Informationsfreiheitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (2007) Ziffer 7.5).

Nachdem sich das BDSG und die technischen und geschäftlichen Möglichkeiten der Abruf- und Meldeverfahren weiter entwickelt haben, ist das Nachmeldeverfahren des Versandhandels gegenüber der Anfang der 90er Jahre bestehenden Rechtsansicht differenzierter zu bewerten.
Ist das Rechtsgeschäft zwischen dem Versandhändler und dem Versandhandelskunden nach der Abwicklung des einzelnen Kaufgeschäfts abgeschlossen, besteht für fortlaufende Nachmeldungen oder sonstige Bonitätsauskünfte kein berechtigtes Interesse mehr. Nachmeldungen oder sonstige Beauskunftungen sind dann datenschutzrechtlich unzulässig.

Die Versandhändler dürfen also nur noch Bonitätsauskünfte beanspruchen, wenn ein Ratenzahlungskredit vereinbart wurde oder so lange noch ein offener Saldo besteht. Dementsprechend müssen die Auskunfteien ihre Verfahren so umstellen, dass Bonitätsauskünfte nur noch unter den vorgenannten Bedingungen erteilt werden.

Im Rahmen einer Sondersitzung der Arbeitsgruppe Auskunfteien, an der verschiedene zuständige Aufsichtsbehörden sowie Vertreter der Auskunfteienbranche und des Versandhandels teilnahmen, wurde den anwesenden Wirtschaftsvertretern nochmals diese einheitliche Rechtsauffassung der Aufsichtsbehörden verdeutlicht. Es wurde auch klar gestellt, dass beide Vertragsseiten, das heißt sowohl das abfragende Unternehmen als auch das übermittelnde Unternehmen, datenschutzrechtlich verantwortlich sind.

Die Wirtschaftsvertreter haben zwischenzeitlich angekündigt, ihre Verfahren bis spätestens Ende September 2008 umzustellen.

Die Aufsichtsbehörden werden nach Ablauf dieser Frist prüfen, ob die Umstellung tatsächlich erfolgt ist oder Maßnahmen gegenüber verantwortlichen Stellen zu ergreifen sind.

7.3 Kreditanfragen/Konditionenanfragen

Seit längerem hatte die Aufsichtsbehörde die Verwendung des Merkmals "Anfrage Kredit" durch eine Auskunftei kritisiert, wenn nicht sicher festgestellt war, dass der Betroffene tatsächlich einen Kreditvertrag mit dem anfragenden Kreditinstitut abschließen, sondern möglicherweise nur die Konditionen für eine Kreditvergabe erfahren wollte (siehe Ziffer 6.1 des 19. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Drucks. 16/5892).

Danach wurde zwar das Merkmal "Kreditkonditionen" eingeführt, zu bemängeln blieb jedoch, dass offensichtlich bei den Banken mangels eindeutiger Festlegungen Unsicherheiten über dessen Abgrenzung zum Merkmal "Anfrage Kredit" bestanden (siehe Ziffer 7.3 des 20. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Drucks. 16/7646).

Im Berichtsjahr wurde die Problematik daher in einer gemeinsamen Sondersitzung der Arbeitsgruppen Kreditwirtschaft und Auskunfteien behandelt. Dabei wurden Abgrenzungskriterien und Voraussetzungen für die künftige Einmeldepraxis der Kreditinstitute festgehalten.

Nur wenn Kreditsuchende im rechtlichen Sinne einen Kreditantrag stellen, also eine verbindliche Willenserklärung auf Abschluss eines Kreditvertrages abgeben, darf das bisherige Merkmal "Kreditanfrage" verwandt werden, das zur Verdeutlichung "Kreditantrag" heißen sollte.
In allen anderen Fällen, in denen die Kreditsuchenden keinen verbindlichen Kreditantrag stellen, ist das Merkmal "Konditionenanfrage" zu verwenden. Dieses Merkmal wird dann nicht an die Vertragspartner übermittelt und fließt auch nicht in die Score-Berechnung der Auskunftei ein. Daher bedarf es für dessen Übermittlung an die Auskunftei lediglich der Befreiung vom Bankgeheimnis, welche auch mündlich vom Betroffenen erklärt werden kann.

Im Berichtjahr hatte die Aufsichtsbehörde noch einzelne Beschwerden zu verzeichnen, in denen sich mehrere Anfragen zu Kreditkonditionen im Datensatz der Betroffenen als fälschliche Anfragen "Kredit" negativ auf den errechneten Score-Wert ausgewirkt zu haben schienen.

Es bleibt zu hoffen, dass mit einer klaren Abgrenzung entsprechend den oben genannten Kriterien solche Beschwerden künftig vermieden werden.

7.4 Unzulässige Anfrage des Vermieters

Nachteilig wirkte sich für einen Beschwerdeführer die missbräuchliche Nutzung eines Auskunftei-Systems durch einen Vermieter aus. Dieser hatte nämlich als Inhaber eines Autohauses - unter Vortäuschung einer Kreditanfrage - bei einer Bank die Einholung einer Auskunft über den wohnungssuchenden Petenten bei der Auskunftei veranlasst. Mit der negativen Auskunft begründete er dann seine ablehnende Entscheidung bei der Wohnungsvergabe. Die Bank nahm den Vorfall zum Anlass, den Autohändler unter Hinweis auf die Anfragevoraussetzungen wegen seiner unzulässigen Anfrage zu rügen. Die Aufsichtsbehörde ahndete das datenschutzwidrige Verhalten des Autohändlers mit einer Geldbuße.

Erstaunt war ein anderer Beschwerdeführer, als er eine Anfrage des Handels, veranlasst durch eine Baustoffhandlung, in seiner Eigenauskunft bemerkte. Offenbar hatte eine Baustoffhandlung mit Sitz in einem anderen Bundesland eine Anfrage zu seiner Person an die Auskunftei gerichtet. Die Erläuterungsversuche zu dem Eintrag, er würde vielleicht gerade ein Haus bauen oder renovieren, konnten ihn nicht überzeugen. Er war sich sicher, dass all dies auf ihn nicht zutraf und er keinesfalls Geschäftsverbindungen zu diesem Unternehmen eingegangen war oder hätte eingehen wollen. Im Zuge der Ermittlungen stellte sich dann heraus, dass der Geschäftsführer der anfragenden GmbH gleichzeitig der Vermieter des Petenten war. Aus den Angaben im Mietvertrag zu der Person des Vermieters war dies für den Mieter jedoch nicht zu erkennen gewesen. Der Vermieter hatte offenbar

kurzerhand den für den Baustoffhandel bestehenden Online-Anschluss an die Auskunftei genutzt, um eine Bonitätsauskunft über den Mietinteressenten einzuholen. Auf Nachfrage gab das Unternehmen an, die Anfrage versehentlich für den Immobilienbereich gestellt zu haben.

Die Auskunftei wies ihren Geschäftspartner nochmals auf die Anfragevoraussetzungen hin und stellte durch eine vertragliche Ergänzung sicher, dass zukünftig Anfragen nur für den zugelassenen Geschäftszweck getätigt werden. Inwieweit das Verhalten des Vermieters auch hier bußgeldrechtliche Konsequenzen nach sich ziehen würde, war durch die zuständige Aufsichtsbehörde des anderen Bundeslandes zu klären.

7.5 Vermeintliche Auskunftei

Die starke Zunahme der Beschwerden gegen ein im Aufsichtsbezirk gemeldetes Inkassounternehmen war darin begründet, dass dieses vorgab, im Internet ein für jedermann zugängliches Schuldnerverzeichnis zu betreiben.

Das Unternehmen verfügt über eine gerichtliche Inkassoerlaubnis und ist per Generalinkassovollmacht befugt, offene Forderungen beizutreiben. Gegen die Inkassotätigkeit als solche bestanden grundsätzlich keine datenschutzrechtlichen Bedenken. Allerdings führt das Unternehmen auch ein Inkasso für angebliche Forderungen aus fragwürdigen Internetangeboten durch. Bezüglich der insoweit bestehenden datenschutzrechtlichen Problematik wird auf die Ausführungen unter Ziffer 9.2 verwiesen. Die Beschwerden richteten sich jedoch im Wesentlichen gegen die Drohung mit dem Eintrag in ein "Schuldnerverzeichnis". Das Führen einer Art Schuldnerverzeichnis, in das auch Dritte Einsicht nehmen können, wäre unzulässig gewesen. (Zur datenschutzrechtlichen Bewertung von Internetauskunfteien und Prangerseiten siehe Ziffer 8.1 des Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde, Drucks. 15/4659).

Trotz der Hinweise auf die Veröffentlichung von Schuldnerdaten auf der Internetseite des Unternehmens und im Schriftverkehr mit den Schuldnern, in dem auf die negativen Folgen eines Eintrags bei dem im Internet geführten "Schuldnerverzeichnis" verwiesen wurde, ist ein solches Verfahren allerdings nicht praktiziert worden. Einzig der jeweilige Betroffene konnte unter Angabe des nur ihm bekannten Geschäftszeichens des Inkassounternehmens und eines weiteren Merkmals Einsicht in den Verlauf seines eigenen Verfahrens nehmen.
Solange also mit der Verarbeitung nur gedroht wird, sie aber tatsächlich gar nicht stattfindet, kann die Aufsichtsbehörde nicht von einer unzulässigen Datenverarbeitung ausgehen und somit auch keine aufsichtsbehördlichen Maßnahmen einleiten.

Dennoch war das Unternehmen im Rahmen einer erfolgten Überprüfung nach § 38 BDSG darauf zu verweisen, dass seinem Hinweis im Impressum des Internetauftritts folgend, es würde die Geschäfte einer Auskunftei betreiben, auch die entsprechenden datenschutzrechtlichen Maßstäbe an die Zulässigkeit eines solchen Geschäftszweckes anzulegen wären. Nachdem das Unternehmen über die datenschutzrechtlichen Voraussetzungen für die Inbetriebnahme der Geschäfte einer Auskunftei belehrt worden war, änderte es das Impressum sowie die entsprechende Passage in den Anschreiben an die Schuldner.

Aber auch nachdem der Internetauftritt geändert worden war, wurden zuletzt erneut Beschwerden gegen das Unternehmen erhoben. Im Mittelpunkt der neuerlichen Beschwerden stand nun eine andere von dem Unternehmen betriebene Internetseite. Auf dieser Seite sollten potentielle Schuldner sich über die neuesten Rechtsprechungen in "vergleichbaren Fällen" informieren können. Insbesondere wurde auf ein Amtsgerichtsurteil verwiesen, das zugunsten des Unternehmens ergangen war. Zur Untermauerung dieses Urteils stellte ein für das Unternehmen tätiger Rechtsanwalt seinen mit den betroffenen bzw. möglichen Schuldnern geführten vertraulichen Schriftverkehr zur Ansicht in die Seite ein. Leider waren die personenbezogenen Daten der Betroffenen nur zum Teil geschwärzt. So waren in vereinzelten Schriftsätzen auch die Geschäftszeichen des Inkassounternehmens und die Anschriften der Betroffenen aufgrund der unzureichenden Schwärzung lesbar. Somit konnte jeder Besucher dieser Internetseite mittels der auf diese Weise in Erfahrung

gebrachten Kennwörter sich Zugang zu den persönlichen Bereichen der im Internet geführten Schuldnerdatei verschaffen.

Nach Bekanntwerden dieses neuerlichen Verstoßes gegen datenschutzrechtliche Bestimmungen wurden seitens des Unternehmens die Akten der Betroffenen in dieser Schuldnerdatei geschlossen. Ein weiterer Zugriff war damit unterbunden. Im Zuge dieser Beschwerden änderte das Unternehmen nochmals seinen Internetauftritt, sodass auf der ursprünglich bekannten Internetseite keine Anmelde-Möglichkeit mehr gegeben ist.
Die Aufsichtsbehörde wird die Tätigkeit des Unternehmens weiterhin kritisch beobachten.

7.6 Sperrdatei für Lastschriftverfahren

Ein bisher vor allem als Dienstleister im Inkassobereich tätiges Unternehmen plant die Errichtung eines neuartigen Frühwarn- und Schutzsystems in Bezug auf Lastschriftverfahren und bat die Aufsichtsbehörde hierzu um Beratung. Mit dem Produkt soll den Spezifika des Zahlungsverfahrens per Lastschrift Rechnung getragen und den damit verbundenen Risiken begegnet werden. Zu diesem Zweck ist die zentrale Speicherung und Beauskunftung von Rücklastschriftinformationen bei nicht eingelösten Lastschriften beabsichtigt. Den beteiligten Vertragspartnern sollen Informationen gegeben werden, um sie vor Forderungsausfällen durch Rücklastschriften zu schützen und ihnen gleichzeitig die Möglichkeit eröffnen, den Kunden bei der missbräuchlichen Inanspruchnahme seiner Daten vor weitergehenden Forderungen, insbesondere durch Dritte, zu bewahren. Darüber hinaus soll das System helfen, die Bankrücklastschriftkosten der Vertragspartner, insbesondere bei wiederkehrenden Lastschrifttransaktionen, z.B. bei Abonnements, Monatsrechnungen, zu reduzieren. Im Wesentlichen handelt es sich um eine spezielle Art von "Sperrdatei". Auch eine Selbstsperrung durch den Kontoinhaber ist möglich.

Derzeit gibt es bereits eine Reihe von Unternehmen, die "Sperrdateien" im Bereich des Lastschriftverfahrens anbieten. Diese beziehen sich nach den vorliegenden Erkenntnissen in der Regel nur auf den stationären Handel (sog. Point-of-Sales-Systeme), d. h. auf die Bezahlung mittels EC-Karte in einem Ladengeschäft unter Einsatz eines entsprechenden Lesegeräts.

Das geplante Auskunftssystem soll jedoch nicht auf Lastschriftverfahren im Rahmen des stationären Handels beschränkt sein. Vielmehr sollen als Vertragspartner grundsätzlich alle Unternehmen in Betracht kommen, die Lastschriftverfahren als Bezahlart anbieten. Hierunter können Unternehmen fallen, bei denen die Lastschriftermächtigung schriftlich gegeben wurde, z.B. Energieversorgungsunternehmen. In Betracht kommen aber auch Unternehmen, bei denen der Kunde telefonisch Waren oder Dienstleitungen bestellen und auch telefonisch die Bankverbindungsdaten zwecks Lastschrift angeben kann. Vor allem kommen Unternehmen mit Internetangeboten in Betracht. Da hier keine EC-Karte vorgelegt wird, ist das Risiko einer missbräuchlichen Nutzung des Lastschriftverfahrens für die Unternehmen besonders hoch.

Aber auch für die Kunden bzw. Nutzer ist die Gefahr, dass ein unbefugter Dritter die eigenen Kontoverbindungsdaten missbräuchlich nutzt, grundsätzlich höher als beim stationären Handel. Zwar kann der Kontoinhaber die Lastschrift widerrufen, ohne dass ihm Gebühren entstehen, aber er muss die Kontoauszüge sorgfältig kontrollieren und den Widerruf tatsächlich ausüben. Für die als Vertragspartner in Betracht kommenden Unternehmen besteht beim Lastschriftverfahren nicht nur das Risiko eines Forderungsausfalls. Vielmehr werden sie bei einer Rücklastschrift in jedem Fall, also unabhängig davon, ob die Forderung doch noch beglichen wird, von den Banken mit der Rücklastschriftgebühr von 8 € belastet. Ein berechtigtes Interesse an einem speziellen Schutzsystem kann daher durchaus anerkannt werden. Entscheidend ist jedoch, dass sich die Einmeldung und die Beauskunftung der Daten auf das erforderliche Maß beschränken sowie Vorkehrungen getroffen werden, um den schutzwürdigen Belangen der Betroffenen Rechnung zu tragen.

Die Aufsichtsbehörde hat hierzu eine eingehende Beratung vorgenommen und über das entsprechend modifizierte Konzept auch die anderen Aufsichtsbehörden im Bundesgebiet im Rahmen der Arbeitsgruppe Auskunfteien informiert. Aufgrund deren Stellungnahmen wurden weitere kleine Änderungen vorgenommen.

Konkret sieht die Produktbeschreibung nun vor, dass im Gegensatz zur Praxis bei den meisten Wirtschaftsauskunfteien keine Forderungen, Namen und Anschriften des Kunden beauskunftet werden sollen, sondern ausschließlich Informationen zu Rücklastschriften (Grund der Rücklastschrift und unter Umständen das Datum der Rücklastschrift). Das Vorhaben ist daher mit einer herkömmlichen Wirtschaftsauskunftei nicht vergleichbar. Von den Vertragspartnern werden lediglich der Name des Kunden, soweit dem Vertragspartner bekannt und wie vom Kunden bei der Lastschriftermächtigung angegeben, sowie Datum und Grund der Rücklastschrift eingemeldet. Der Name wird jedoch nicht beauskunftet. Bei der Abfrage in der Datenbank hat der anfragende Vertragspartner lediglich die Bankverbindung, die der Kunde in der Lastschriftermächtigung angibt, zu nennen, nicht aber den Namen.

Bei den meisten Rücklastschriftgründen, z.B. "Konto erloschen", "Kontonummer falsch", geht es nicht darum, den betreffenden Kunden ein vertragswidriges Verhalten vorzuwerfen; darum wird auch der Name des Kunden nicht beauskunftet. Die Sperrdatei ist, wie bereits ausgeführt, grundsätzlich nicht mit einer Bonitätsauskunftei vergleichbar, denn es geht hier nur darum, ob das Konto für eine Lastschrift verwendet werden kann. Wenn also beispielsweise der Kunde eines Online-Shops zwecks Lastschrift eine bestimmte Kontonummer nebst Bankleitzahl zur Bezahlung eines Films, eines Musikstücks oder einer Software angegeben hat, dann ist es völlig berechtigt, dass der Online-Shop sich vergewissern will, ob diese Bankverbindung für das Lastschriftverfahren geeignet ist, bevor er den Film, das Musikstück oder die Software zum Download freigibt. Eine entsprechende Abfrage bei der Auskunftei ohne Nennung des Kundennamens ist gerechtfertigt.

Es spielt keine Rolle, ob bei dem Lastschriftvorgang, der die Einmeldung auslöste, eine für das Lastschriftverfahren unbrauchbare Kontoverbindung absichtlich oder versehentlich durch den Betroffenen angegeben wurde. Wenn die Kontoverbindung unbrauchbar ist, dann rechtfertigt allein diese Tatsache die Einmeldung und Abfrage. Der Vertragspartner wird den betroffenen Kunden zu Recht auffordern, eine andere Bankverbindung anzugeben.

Wenn der Einmeldung in die Sperrdatei ein telefonischer Bestellvorgang zugrunde lag und der Vertragspartner die Kontoverbindung falsch notierte, sodass die Bank eine Rücklastschrift vorgenommen hat, die zu einer entsprechenden Einmeldung führte, dann ist der Kunde dadurch bei den oben genannten und ähnlichen Rücklastschriftgründen nicht belastet. Denn abgesehen davon, dass er wohl kaum den Fehler des alten Vertragspartners bei seinem neuen Bestellvorgang selbst wiederholen, d.h. selbst die gleichen falschen Daten eingeben wird, wäre es bei entsprechender Falschangabe völlig gerechtfertigt, wenn der Vertragspartner diese Bankdaten nicht für das Lastschriftverfahren akzeptiert. Derartige Fehler wären also unerheblich.

Selbst wenn auch andere Fehler nicht völlig ausgeschlossen sind, die dazu führen, dass einem Kunde möglicherweise in einer bestimmten Situation unberechtigt die Zahlung mittels Lastschriftverfahren verweigert wird, erscheint dieses Restrisiko als hinnehmbar, da eine Aufklärung möglich ist - hierfür sind entsprechende Verfahren vorgesehen - und zudem kein Rechtsanspruch auf Zahlung mittels Lastschriftverfahren besteht sowie andererseits der Vertragspartner gerade beim nichtstationären Einsatz des Lastschriftverfahrens ein besonderes Ausfallrisiko trägt. Letzteres gilt in besonderem Maße, wenn es sich um Online-Anbieter handelt, deren "Ware" unmittelbar online zur Verfügung gestellt wird, sodass eine "Rückforderung" der "Ware" sinnlos bzw. unmöglich ist, wie bei den oben genannten Beispielen ersichtlich ist. Ein Musikstück, Bilder oder Filme, die über das Internet zum Anhören bzw. Anschauen angeboten werden, können nicht "zurückgefordert" werden, wenn sich der Kunde diese unmittelbar nach der Angabe seiner Kontodaten zwecks Zahlung mittels Lastschrift heruntergeladen und angehört bzw. angeschaut hat.

Besondere Betrachtung erfordert jedoch der Rücklastschriftgrund "wegen Widerspruchs". Hierzu ist zu erläutern, dass nach den Zahlungsbedingungen der Banken der Kontoinhaber eine Lastschrift ohne jede Begründung widerrufen kann. Er hat dadurch auch keinerlei Kosten, vielmehr hat das Unternehmen, bei dem mittels Lastschrift bezahlt werden sollte, wie bereits oben ausgeführt, gegenüber der Bank eine Gebühr zu zahlen. Der Rücklastschriftgrund "wegen Widerspruchs" hat also per se nichts mit einem Bestreiten der Forderung zu tun, sondern kann quasi willkürlich erfolgen. Der Begriff "wegen Widerspruchs" ist insofern missverständlich, wird aber von den

Banken verwendet und ist insofern korrekt. In der Sache geht es darum, dass ein Zahlungsvorgang - aus welchen Gründen auch immer - auf Veranlassung des Kontoinhabers gestoppt wird.

Natürlich kann der Grund für einen Widerspruch sein, dass der Kontoinhaber die Forderung als unbegründet ansieht, möglicherweise ist dies sogar der häufigste Grund. Da in diesem Fall seine schutzwürdigen Belange berührt sind, wurden von der Aufsichtsbehörde hier besondere Anforderungen gestellt. Insbesondere darf keine Einmeldung erfolgen, wenn die Forderung bestritten ist. Wird die Forderung nachträglich bestritten, muss der Vertragspartner eine Korrekturmeldung vornehmen. Die Beauskunftung dieses Widerrufsgrunds darf nur erfolgen, wenn mehrere solcher Rücklastschriften vorliegen.

Nicht unproblematisch war die Absicht des Unternehmens, gespeicherte Rücklastschriftgründe nicht sofort zu löschen, wenn die Forderung nachträglich beglichen wird, sondern die Rücklastschriftgründe noch eine gewisse Zeit weiter zu speichern und zu beauskunften. Hier war jedoch nach der Art der Rücklastschriftgründe zu differenzieren. Wie bereits oben ausgeführt, gibt es Rücklastschriftgründe, wie "Konto erloschen", die nur eine Aussage über die Tauglichkeit einer Kontoverbindung für das Rücklastschriftverfahren geben. Da eine Beauskunftung ja nur erfolgt, wenn genau diese Kontodaten wieder abgefragt werden und an der Richtigkeit der Aussage, dass die Kontoverbindung für das Lastschriftverfahren untauglich ist, sich nichts ändert, auch wenn eine Forderung beglichen wird, erscheint eine weitere Speicherung für einen gewissen Zeitraum gerechtfertigt.

Bei anderen Rücklastschriftgründen, z.B. "mangels Deckung" und "wegen Widerspruchs", ist hingegen nicht zu verkennen, dass diese implizit eine gewisse Aussage über die Verlässlichkeit des Kunden für dieses Zahlverfahren beinhalten, daher ist die weitere Speicherung nach Begleichung der Forderung hier problematischer. Zu berücksichtigen ist allerdings, dass Unternehmen beispielsweise gerade dadurch ein Schaden entstehen kann, dass Kunden Zahlungen verzögern, indem sie bewusst, z.B. am Monatsende, zunächst eine Lastschrift widerrufen, ohne die Forderung als solche zu bestreiten, und dann später doch bezahlen. Daher ist auch hier eine weitere Speicherung für eine gewisse Zeit, die allerdings kürzer sein muss als bei den anderen Rücklastschriftgründen, gerechtfertigt. Dies allerdings nur unter der Maßgabe, dass bzgl. der Beauskunftung die oben genannten weitere Anforderung beachtet wird.

Aus Sicht der Aufsichtsbehörde bestehen gegen das in der aktuellen Produktbeschreibung dargestellte Vorhaben keine Bedenken. Durch die besonderen Vorkehrungen wird den schutzwürdigen Belangen der Betroffenen Rechnung getragen.
Daher ist sowohl die Einmeldung in den Datenpool als auch die Abfrage aus diesem grundsätzlich durch die gesetzlichen Erlaubnistatbestände gedeckt (§ 28 Abs. 1 Nr. 1 bzw. Nr. 2 und § 28 Abs. 3 Nr. 1 BDSG). Es genügt daher ein Hinweis nach § 4 Abs. 3 BDSG.
(Ebenso: Hinweise des Innenministeriums Baden-Württemberg Nr. 37 vom 18. Januar 1999 (Nr. 3.1)).

Hiervon bestehen jedoch Ausnahmen. Soweit § 3 Abs. 9 BDSG einschlägig ist, ist eine Einwilligung erforderlich. Dies ist bei Erotik-Angeboten relevant. Darüber hinaus ist generell bei Online-Angeboten eine Einwilligung erforderlich. Da es sich bei Waren- und Dienstleistungsangeboten im Internet um Telemedien im Sinne von § 1 Abs. 1 Telemediengesetz (TMG) handelt, sind im Online-Bereich die strengen Zweckbindungsvorschriften der §§ 12 Abs. 1, 2 TMG und § 14 Abs. 1 TMG bezüglich der erhobenen Bestandsdaten zu beachten. Die Einmeldung in den Sperrpool und die möglicherweise anschließende Beauskunftung an weitere Vertragspartner ist nicht mehr zur "inhaltlichen Ausgestaltung des konkreten Vertragsverhältnisses" zwischen dem Vertragspartner und dessen Endkunden erforderlich und ist deshalb auch nicht mehr durch § 14 Abs. 1 TMG abgedeckt. Daher bedarf es hierfür einer informierten Online-Einwilligung des Betroffenen nach § 13 Abs. 2, 3 TMG. Das Unternehmen hat entsprechende Formulierungen vorgelegt.

Selbstverständlich wird das Verfahren weiter zu beobachten sein, ggf. wird bei neuen Erkenntnissen eine Neubewertung erforderlich sein.

7.7 Benachrichtigung der Betroffenen, Auskunft über Herkunft und Empfänger der Daten

"Sehr geehrter Empfänger,
nach § 33 Abs. 1 Bundesdatenschutzgesetz setzen wir Sie hiermit davon in Kenntnis, dass wir zu Ihrer Person gespeicherte Daten erstmals übermittelt haben."
Diese Zeilen ließen so manchen Beschwerdeführer regelrechte Verschwörungstheorien oder Verfolgungsszenarien entwickeln. Viele Bürger wendeten sich schriftlich oder telefonisch an die Aufsichtsbehörde, da sie die Rechtmäßigkeit der Auskunfteien-Tätigkeit trotz der - hier nur auszugsweise zitierten - schriftlichen Benachrichtigung grundsätzlich anzweifelten, nicht zuletzt wegen entsprechender Beiträge in einschlägigen Internet-Foren.

Die Aufsichtsbehörde hatte das Unternehmen bereits im Jahr 2004 eingehend geprüft und war zu dem Ergebnis gelangt, dass die Datenverarbeitung nicht zu beanstanden ist (siehe Ziffer 8.3 des 18. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde, Drs. 16/4752).

Auch im Berichtszeitraum gingen jedoch zahlreiche Anfragen und Beschwerden bezüglich des Unternehmens ein. Anlass war einmal mehr die in § 33 Abs. 1 BDSG vorgeschriebene oben erwähnte Benachrichtigung der Betroffenen durch die betreffende Auskunftei, die sich im Wesentlichen auf Adressermittlungen spezialisiert hat. Die Ermittlungen erfolgen in der Regel durch Anfrage beim zuständigen Einwohnermeldeamt oder über öffentliche Verzeichnisse. Die Auskunftei übermittelt die aktuellen Adressdaten der Betroffenen ausschließlich an Unternehmen, überwiegend aus den Branchen Banken, Versicherungen, Telekommunikation und Dienstleistungen, die ein berechtigtes Interesse daran glaubhaft dargelegt haben. Die Adressdaten werden nicht zu Werbezwecken weitergegeben.

Häufig klärte die Aufsichtsbehörde die Anfragenden nochmals über ihr Auskunftsrecht nach § 34 BDSG auf, sodass diese sich dann selbst an das Unternehmen wenden konnten um zu erfahren, welche personenbezogenen Daten konkret gespeichert und an wen übermittelt wurden.
Die Pflicht zur Beauskunftung erstreckt sich auf die zu der Person gespeicherten Daten, den Zweck der Datenspeicherung sowie die Empfänger und die Datenherkunft.
Die Datenschutzaufsichtsbehörden im Bundesgebiet vertreten einhellig die Meinung, dass Auskunfteien nur beim Bestehen besonderer Umstände die Auskunft verweigern dürfen. Auf entsprechende Auskunftsersuchen sind daher im Regelfall auch Datenherkunft und Datenempfänger zu benennen (siehe Ziffer 7 des 19. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde, Drucks. 16/5892). Gleichwohl wurde auch von einigen Petenten Beschwerde wegen unzureichender Beauskunftung vorgetragen. Diese Beschwerden bezogen sich allerdings hauptsächlich nur auf den Umstand, dass das Unternehmen nicht in dem vom Petenten gesetzten Zeitrahmen geantwortet hatte.

Erfreulicherweise war das Unternehmen gegen Ende des Berichtszeitraums bereit, sowohl sein Benachrichtigungsschreiben an die Betroffenen als auch das Beauskunftungsschreiben zu überarbeiten. Nun wird nicht mehr ausschließlich in abstrakter Form auf die bestehenden rechtlichen Vorgaben hingewiesen, was möglicherweise auch dazu beigetragen hatte, dass für viele Adressaten die durchaus zutreffenden Ausführungen teilweise nur schwierig zu verstehen waren oder deren Rechtmäßigkeit trotz Angabe der einschlägigen gesetzlichen Bestimmungen in Zweifel gezogen worden waren.

Der jetzt verwendete Text für das Beauskunftungsschreiben beschreibt vielmehr im Anschluss an die Nennung der gespeicherten Daten sowie des anfragenden Unternehmens (Datenempfänger) in einer verständlichen Sprache die möglichen Hintergründe für die Datenerhebung und führt aus, welche Wirtschaftsbranchen üblicherweise zu den Auftraggebern des Unternehmens gehören. Außerdem wird noch explizit darauf verwiesen, dass die gespeicherten Daten keinesfalls zu Werbezwecken oder an sonstige Dritte übermittelt werden.

Auch für das Standard-Benachrichtigungsschreiben wurde der Aufsichtsbehörde eine Überarbeitung angekündigt, die allerdings bei Redaktionsschluss für diesen Bericht noch nicht vorlag.

8. Banken - Verkauf von Krediten

Im Berichtszeitraum wurde die Öffentlichkeit durch Berichte in Fernsehen und Presse über ein bis dahin eher unbekanntes Geschäftsfeld der Kreditinstitute informiert. Der Verkauf von grundpfandrechtlich gesicherten Darlehensforderungen an einen Investor rückte in den Fokus der Verbraucher und Bankkunden.

Wenn Kredite notleidend werden, muss ein Kreditinstitut grundsätzlich die Entscheidung treffen, ob es die Engagements in den eigenen Büchern behalten und die Abwicklung bzw. Sanierung selbst übernehmen will. Alternativ dazu bietet sich der Kreditverkauf an.

Das Kreditvolumen der Bank ist abhängig von deren haftenden Eigenkapital. Durch den Verkauf von Krediten wird das haftende Eigenkapital entlastet, der Bank fließt Liquidität zu und steht für das Neugeschäft zur Verfügung. Die Bank ist daher interessiert, sich von notleidenden Krediten zu trennen, denn diese binden Kapital und sind unrentabel. Notleidende Kredite binden darüber hinaus auch Personal, denn sie erfordern eine intensive Bearbeitung.

Der Verkauf von Kreditportfolios ist für die Banken ein Instrument der Risiko- und Kapitalsteuerung. Als Refinanzierungsmittel werden auch Kredite, die vertragsnach von den Kreditnehmern bedient werden, in Paketen an Investoren verkauft. Hier darf die veräußernde Bank die personenbezogenen Daten der Kreditnehmer nicht ohne deren Einwilligung an den Forderungserwerber übermitteln.

Der Bundesgerichtshof (BGH) hat mit Urteil vom 27. Februar 2007 (XI ZR 195/05) entschieden, dass der wirksamen Abtretung von Darlehensforderungen eines Kreditinstituts weder das Bankgeheimnis noch das BDSG entgegensteht. Die Instanzgerichte hatten diese Frage bislang uneinheitlich entschieden. Der BGH hält die Abtretung einer notleidenden Darlehensforderung an ein anderes Kreditinstitut für wirksam. Er trennt deutlich das dingliche Geschäft der Abtretung von der schuldrechtlichen Seite und zieht den Schluss, dass sich weder aus dem Bankgeheimnis noch aus dem BDSG ein Abtretungsverbot nach § 399 BGB ergibt. Auch ein eventueller Verstoß gegen datenschutzrechtliche Bestimmungen oder das Bankgeheimnis berühren die Wirksamkeit des dinglichen Verfügungsgeschäfts der Forderungsabtretung nicht. Der BGH stellt jedoch klar, dass ein solcher Fall zu einer zivilrechtlichen Schadensersatzpflicht auf schuldrechtlicher Ebene führen kann. Darüber hinaus sieht das Gericht durch die Bußgeld- und Strafvorschriften der §§ 43, 44 BDSG datenschutzrechtliche Verstöße ausreichend sanktioniert.

Gegen diese Entscheidung des BGH wurde Verfassungsbeschwerde eingelegt. Die Beschwerdeführer rügten die Verletzung ihres Rechts auf informationelle Selbstbestimmung. Diese hat das Bundesverfassungsgericht mangels Erfolgsaussichten nicht zur Entscheidung angenommen (1 BvR 1025/07).Einen Verstoß gegen das Grundrecht sieht das Gericht nur als Ausnahmefall.

Mit der datenschutzrechtlichen Bewertung des Verkaufs von Kreditportfolios befasste sich die Arbeitsgruppe Kreditwirtschaft des Düsseldorfer Kreises in der Sitzung im April 2007. Dabei waren die Aufsichtsbehörden einheitlich der Auffassung, dass eine Übermittlung von Daten des Forderungsschuldners in ein Land innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig ist, sofern es sich um eine sogenannte notleidende Forderung handelt. Dies ist der Fall, wenn der Forderungsschuldner seinen vertraglichen Pflichten nicht hinreichend nachgekommen ist. Die Übermittlung von Daten im Zusammenhang mit nicht notleidenden Forderungen ist dagegen nur dann zulässig, wenn der Forderungsschuldner darin eingewilligt hat.

Soweit die Forderung an eine Stelle außerhalb der EU bzw. des EWR übertragen werden soll, ist die damit verbundene Datenverarbeitung nur unter der weiteren Voraussetzung zulässig, dass in dem betreffenden Land ein angemessenes Datenschutzniveau besteht oder Vorkehrungen nach § 4c Abs. 2 BDSG getroffen worden sind.

Zwischenzeitlich greifen einige Kreditinstitute aktiv die Problematik auf und versichern ihren Kunden schriftlich, Kreditverkäufe nicht vorzunehmen. Auch die Bundesregierung sieht Regelungsbedarf und möchte im Rahmen des "Risikobegrenzungsgesetzes" die Materie behandeln. Es bleibt zu hoffen, dass bei der gesetzlichen Regelung auch die Fragen des Datenschutzes und des Bankgeheimnisses ausreichend berücksichtigt werden.

Durch die Anfrage eines Kreditnehmers wurde der Aufsichtsbehörde ein Sachverhalt bekannt, der sich durch Sensibilität gegenüber den personenbezogenen Daten des Kunden auszeichnet.
Eine Hypothekenbank die im Rahmen der Umstrukturierung und Neuorganisation den Geschäftsbereich des Privatkundengeschäfts sukzessive an andere Kreditinstitute übertragen wollte, wählte das mit Rundschreiben vom 19. März 1997 durch das Bundesaufsichtsamt für das Kreditwesen (heute BaFin) vorgeschlagene Modell zu Asset Backed Securities (ABS)-Transaktionen als Leitbild zur Umsetzung der Maßnahme.

Die Bankkunden wurden schriftlich von der beabsichtigten Übertragung des Hypothekendarlehens an eine niederländische Bank mit deutscher Niederlassung informiert. Sie wurden um Zustimmung zu der Darlehensübertragung und der Weitergabe der persönlichen Daten gebeten. Es erfolgte der Hinweis, dass im Falle der verweigerten Zustimmung die Übertragung der Darlehensforderung nicht berührt wird. Für diesen Fall hatte die Hypothekenbank ein Treuhandmodell in Anlehnung an das ABS-Modell der BaFin eingerichtet. Ein Notar fungiert als Datentreuhänder. Er besitzt die Daten über den Kunden, das Darlehen und das beliehene Objekt. Der Forderungskäufer erhält einen anonymisierten Datensatz, sowie Angaben zum Darlehen wie Zinssatz und Anfangsbetrag. Er erhält keine Beleihungsobjektdaten. Die Hypothekenbank ist weiterhin Vertragspartner und führt weiterhin die Bearbeitung des Kredits durch. Sie leitet auch die Annuitäten an den Forderungskäufer weiter.
Auch bei Ablauf der Zinsfestschreibung bleibt die Hypothekenbank auf Wunsch des Kunden weiterhin Vertragspartner, prolongiert das Darlehen und führt das Engagement bis zur vollständigen Rückzahlung im Treuhandmodell weiter.

9 Telemedien

9.1 Unerwünschte Veröffentlichung personenbezogener Daten im WWW

Eine Reihe von Beschwerdeführern bat die Datenschutzaufsichtsbehörde um Unterstützung gegenüber Seitenbetreibern, auf deren Internetseiten gegen den Willen der Betroffenen Daten zu deren Person veröffentlicht wurden.

Als Anbieter von Telemedien nach § 2 Nr. 1 TMG waren die Stellen entweder im Rahmen des § 7 TMG für die angebotenen eigenen Inhalte selbst verantwortlich oder zumindest als Anbieter fremder Inhalte, sog. Host-Provider wie z. B. Foren-Anbieter, nach § 10 für die Veröffentlichung der Daten eingeschränkt verantwortlich. Da das TMG allerdings nur das Rechtsverhältnis zwischen dem Anbieter und den Nutzern eines Internetangebots regelt, gilt nach § 4 Abs. 1 BDSG für den Umgang mit personenbezogenen Inhaltsdaten von WWW-Seiten das BDSG. Es war also in jedem Einzelfall zu prüfen, ob das Vorhalten der personenbezogenen Daten als Inhalt von öffentlich zugänglichen WWW-Seiten auf der Grundlage von § 28 Abs. 1 Nr. 1 - 3 oder § 29 BDSG erfolgen durfte oder ob dem ein anzuerkennendes schutzwürdiges Interesse gegenübersteht, das eine Verarbeitung der Daten im Rahmen eines öffentlichen WWW-Angebots aus datenschutzrechtlichen Gründen verbietet.

Bei den Eingaben handelte es sich um verschiedenste Sachverhalte und Datenarten.

Mehrfach wandten sich Petenten gegen die Nennung ihres Realnamens oder ihrer E-Mail-Adresse in alten Forenprofilen oder in Forenbeiträgen zu Hobby-Themen, die sie vor Jahren selbst geschrieben hatten und auf die sie aktuell u. a. über eine Internetsuche (siehe Ziffer 9.3 dieses Berichts) aufmerksam wurden.

Die Datenschutzaufsichtsbehörde wies die jeweiligen Telemedienanbieter zunächst darauf hin, dass schon bei der Anmeldung in einem unentgeltlichen Online-Forum in der Regel die Möglichkeit der pseudonymen Nutzung des

Telemediums nach § 13 Abs. 6 TMG eröffnet werden muss. Die Abfrage personenbezogener Daten zur Registrierung sollte im Sinne des § 14 Abs. 1 TMG ohnehin auf das für die Forenteilnahme erforderliche Minimum beschränkt werden. Zudem sollte den Usern die Möglichkeit gegeben werden, selbst festzulegen, welche Profildaten einsehbar sein sollen und welche Daten zu ihren Beiträgen veröffentlicht werden. Eine Veröffentlichung der E-Mail-Adresse ohne Zustimmung des Adressinhabers ist jedenfalls weder durch § 14 Abs. 1 TMG noch durch § 28 BDSG zu rechtfertigen. Die Anbieter reagierten auf diese Argumentation in der Regel mit der Löschung der Daten der Petenten.

In einem Fall entschied sich ein Forenanbieter, dennoch einen inhaltlich belanglosen Forenbeitrag des Beschwerdeführers weiterhin in einem Foren-Thread (= Diskussionsstrang, Kette von Beiträgen zu einem Thema) zu veröffentlichen. Dabei wurde aber nur noch der Vorname des Petenten genannt. Die Datenschutzaufsichtsbehörde akzeptierte diese Vorgehensweise. Wer in einem Online-Forum einen Beitrag schreibt, weiß auch, dass Online-Foren der Veröffentlichung im WWW dienen. Wenn sich jemand gleichwohl bewusst dafür entscheidet, unter Nennung seines Namens Beiträge in Online-Foren zu schreiben, hat er keinen grundsätzlichen Anspruch auf spätere Löschung aller Beiträge aus diesen Foren (zur Aufgabe der Privatsphäre in Internet-Foren siehe Urteil des LG Berlin vom 25. Oktober 2007, Az.: 27 O 602/07). Ebenso wenig bestand in diesem Fall ein Anspruch darauf, die Beiträge anderer Teilnehmer zu löschen, in denen der Petent von diesen mit seinem Vornamen angesprochen wurde. Zudem kann der Vorname als gutes Pseudonym im Sinne des § 13 Abs. 6 TMG gewertet werden, was zusätzlich für eine Zulässigkeit der von diesem Forenanbieter gewählten Lösung sprach.

Ein anderer Beschwerdeführer bat die Datenschutzaufsichtsbehörde um Unterstützung im Zusammenhang mit einem unentgeltlichen Hobbyforums, in dem sich Mitglieder über gemeinsame Interessen austauschen. Nach einem öffentlich und sehr emotional geführten Streit im Forum hatte der Forenbetreiber einen Brief veröffentlicht, den der Beschwerdeführer an diesen Forenbetreiber persönlich per Post gesandt hatte. Da dem Brief neben dem Namen auch seine Postanschrift und seine persönliche Unterschrift zu entnehmen war, forderte der Nutzer den Anbieter zum Entfernen seines Briefs aus dem Online-Angebot auf. Dieser weigerte sich allerdings gegenüber dem Forenteilnehmer zunächst mit der Begründung, dass der Brief die zuvor öffentlich geführte Diskussion beträfe, wenn nicht sogar fortsetzte und alle Mitglieder, die von dem Konflikt betroffen seien, ein Recht hätten, den Brief zu lesen. Die Datenschutzaufsichtsbehörde wies den Betreiber des Forums darauf hin, dass die aktuelle Online-Auseinandersetzung um inhaltliche Streitigkeiten und Fragen des guten Online-Benehmens auch weitergeführt werden kann, wenn die Postanschrift und der Unterschriftszug des Beschwerdeführers nicht in dem Forum veröffentlicht werden. Die Veröffentlichung dieser Daten auf einer Foren-Seite diente weder einem Vertragsverhältnis mit dem Betroffenen nach § 28 Abs. 1 Nr. 1 BDSG noch waren diese Daten allgemein zugänglich nach § 28 Abs. 1 Nr. 3 BDSG. Die Interessenabwägung des § 28 Abs. 1 Nr. 2 BDSG musste bezüglich dieser Datenarten ebenfalls zu Gunsten des Beschwerdeführers erfolgen. Der Forenanbieter schwärzte daraufhin die beanstandeten Datenarten in dem Brief. Die Veröffentlichung in dieser datenreduzierten Variante wurde von der Datenschutzaufsichtsbehörde nicht mehr beanstandet, da nun nur noch das wiedergegeben wurde, was zuvor bereits öffentlich im Forum argumentiert und angedroht worden war. Es gehört nicht zu den Aufgaben der Datenschutzaufsichtsbehörde, Online-Konflikte zu schlichten oder durchzusetzen, dass durch eine fehlende Online-Diskussionskultur entstandene Streitigkeiten um Befindlichkeiten der Teilnehmer beigelegt werden.

Ein anderer Beschwerdefall betraf die in einige Internetgästebücher anonym eingestreute Suchanfrage nach dem Wohnort einer Person unter Nennung des Namens, des Geburtsdatums und der gleichzeitigen Behauptung, derjenige sei ein Mörder. Der in Hessen ansässige Anbieter einer ganzen Reihe solcher kostenloser Online-Gästebücher, der diese im Rahmen des sog. Application Service Providing (ASP) als Online-Dienstleistung für die Inhaber von WWW-Seiten anbietet, wurde als Host-Provider im Sinne des § 10 Abs. 1 TMG von diesem Umstand in Kenntnis gesetzt und entfernte die anonymen Beiträge daraufhin umgehend.

Eine weitere Eingabe richtete sich gegen den Verleger einer Immobilienzeitschrift, der neben den üblichen Grundstücks-, Haus- und Wohnungsangeboten auch die Daten zu eingeleiteten Zwangsversteigerungsverfahren von Immobilien in einer kostenlos verteilten Offline-Zeitschrift und in seinem Internetauftritt im WWW veröffentlicht. Die Betroffene gab an, dass die in der aktuellen Zeitschrift veröffentlichten Informationen zur Zwangsversteigerung des Familiengrundstücks falsch seien, da das Verfahren bereits vor der Veröffentlichung vom zuständigen Gericht eingestellt worden sei, und legte entsprechende Belege vor.
Die Überprüfung des Sachverhalts bei dem Unternehmen ergab, dass der Verlag die Daten von einem Verlag in Nordrhein-Westfalen erhält, der die Daten seinerseits laufend aus den öffentlichen Bekanntmachungen deutscher Amtsgerichte bezieht und diese sowohl selbst veröffentlicht, als auch an andere Verlage weitergibt. Da zu befürchten war, dass auf diesem Weg noch weitere Verlage die falschen bzw. veralteten Zwangsversteigerungsinformationen zur Veröffentlichung erhalten hatten, wurde die Eingabe diesbezüglich nach § 38 Abs. 1 Satz 4 BDSG an die in Nordrhein-Westfalen nach § 38 BDSG als Aufsichtsbehörde zuständige Landesbeauftragte für Datenschutz weitergeleitet.

Bei einer anschließenden Überprüfung der Internetpräsenz des Verlags stellte sich heraus, dass der Anbieter auf seinen WWW-Seiten weiterhin eine PDF-Variante der kompletten Print-Version seiner Immobilienzeitung zum öffentlichen Abruf bereithielt. Da auch diese Online-Version die falschen Daten zum Zwangsversteigerungsverfahren der Petentin enthielt, wurde der Anbieter nachdrücklich aufgefordert, die falschen Daten aus dem Online-Angebot zu löschen. Bei einer intensiveren Nachschau stellte sich zudem heraus, dass der Verlag in seinem öffentlich zugänglichen Online-Archiv alle Exemplare der letzten Jahre seiner Immobilienzeitung als PDF-Datei zum Herunterladen anbot. Auch in einigen dieser Archiv-Ausgaben waren inzwischen deutlich veraltete personenbeziehbare Angaben zu Zwangsversteigerungsverfahren enthalten. Dem Unternehmen wurde verdeutlicht, dass eine Veröffentlichung dieser Daten nach § 28 Abs. 1 Nr. 3 BDSG lediglich so lange zulässig sein kann, wie die Daten auch von den zuständigen Gerichten zum Abruf bereitgehalten werden. Einer darüber hinausgehenden Veröffentlichung dieser veralteten Daten stehen offensichtlich überwiegende schutzwürdige Interessen der Betroffenen im Sinne dieser Vorschrift entgegen.

Der Verlag entschloss sich daraufhin, die Rubrik "Zwangsversteigerungen" vollständig aus seiner Online-Ausgabe zu entfernen, um Problemen wie im vorliegenden Fall aus dem Weg zu gehen und um künftig keine aufwändige tägliche Pflege der Online-Datenbestände betreiben zu müssen. Die Datenschutzaufsichtsbehörde hat die vorherige Veröffentlichung der veralteten Daten aus Zwangsversteigerungsverfahren ausdrücklich beanstandet. Die gefundene Lösung, die Daten nur im Print-Medium und nicht mehr Online anzubieten, wurde begrüßt.

Der Fall bestätigte die großen Zweifel der Aufsichtsbehörde, dass die privaten Anbieter solcher Daten, die aus öffentlich zugänglichen amtlichen Quellen stammen, bezüglich der Pflege der Daten, der rechtzeitigen Aktualisierung und der Nicht-Auffindbarkeit durch Internetsuchmaschinen den selben Standard zum Schutz der Persönlichkeitsrechte Betroffener gewährleisten können, wie die amtlichen Anbieter.

9.2 Kostenfallen im Internet

Immer mehr Bürgerinnen und Bürger aller Altersgruppen mit unterschiedlichsten technischen Vorkenntnissen nutzen wie selbstverständlich die neuen Möglichkeiten des Internet zu vielfältigsten Zwecken. Die immer bessere Versorgung mit schnellen DSL-Zugängen und die Nutzung günstiger Flatrate-Angebote hat dazu geführt, dass in vielen Haushalten der Internet-PC als Mittel für Freizeitgestaltung und Hobbypflege, Informationssuche- und Beschaffung, zu spielerischen und beruflichen Zwecken, zum Online-Einkauf, zur Selbstdarstellung, zur Meinungsbildung und für die individuelle Kommunikation unverzichtbar geworden ist.
Leider geht angesichts der faszinierenden Möglichkeiten, die die virtuelle Online-Welt eröffnet, bei vielen Surfern die Sensibilität dafür verloren, dass im Netz auch viele reale Gefahren auf sie, ihre Daten und ihren Geldbeutel lauern. So bietet das Internet auch unseriösen Firmen viele neue Chancen, unvorsichtigen Surfern mit geschickt gestalteten Online-Angeboten das Geld

aus der Tasche zu ziehen. Dass das "GeschäftsmodeIl" der sogenannten "Internet-Kostenfalle" im Berichtsjahr geradezu einen Boom erlebte, musste die Datenschutzaufsichtsbehörde anhand einer außergewöhnlich hohen Zahl von Anfragen und Beschwerden von Internetsurfern gegen verschiedene in Südhessen ansässige Internetanbieter feststellen.

Auf allen WWW-Seiten dieser Anbieter werden den Nutzern scheinbar unentgeltliche Dienstleistungen zu unterschiedlichsten Themen offeriert. Es handelt sich z. B. um Lebenserwartungstests, Hausaufgabenhilfen, Gedichttexte, Ahnen- und Namensforschung, Führerscheinfragen, Sex- und IQ-Tests, Gratis-SMS, Kochrezepte, Routenplaner, Sudoku-Rätsel, Bastelanleitungen, Pflanzeninfos, Tauschbörsen-News, Witze, Vornamenslisten, Berufstipps und etliche weitere Bereiche. Ähnliche Angebote anderer Anbieter sind im WWW an vielen Stellen gratis abrufbar. Die Liste der aktiven WWW-Seiten der bekannten hessischen Anbieter von Internet-Kostenfallen umfasste zum Zeitpunkt der Erstellung dieses Berichts fast 100 Domains.

Interessierte arglose Surfer werden von den jeweiligen Startseiten, auf denen vermeintlich eine Gratisdienstleistung angeboten wird, zu Datenerhebungsmasken geleitet, um sich dort unter Angabe von Name, Anschrift, E-Mail-Adresse und Geburtsdatum zu registrieren. Die Kenntnisnahme der Allgemeinen Geschäftsbedingungen (AGB) und des im Text verlinkten und auch über den Seitenfuß leicht erreichbaren Datenschutzhinweises nach § 13 Abs. 1 TMG ist noch durch das Setzen eines Häkchens in ein Optionsfeld aktiv zu bestätigen, bevor die Registrierung mittels eines Absende-Feldes zu beenden ist. Der weit unter dem Absende-Feld oder an einer anderen unauffälligen Stelle befindliche oft schwer lesbare Text mit einer klein gedruckten, nicht hervorgehobenen Preisangabe wird leider gerade von denjenigen Betroffenen leicht übersehen, bei denen schon die für ein kostenloses Online-Angebot recht umfangreiche Datenerhebung keine Zweifel an der Seriosität der Anbieter geweckt hatte. Die Kosten belaufen sich je nach Anbieter auf ca. 60 bis 90 €, was auch regelmäßig den hinteren Seiten der AGB bzw. der Nutzungsbedingungen entnommen werden kann.

Alle Betroffenen, die sich im Jahr 2007 wegen einer solchen "Internet-Kostenfalle" an die Datenschutzaufsichtsbehörde beim Regierungspräsidium Darmstadt wandten, hatten zuvor von den Anbietern bzw. deren beauftragten Rechtsanwälten oder Inkassounternehmen Rechnungen für die Bezahlung angeblich im Internet abgeschlossener Verträge über diese Angebote erhalten. Viele Surferinnen und Surfer waren aber der Ansicht, sich für eine kostenlose Gratis-Dienstleistung registriert zu haben. Andere Petenten gaben an, die fraglichen Seiten gar nicht besucht und dort keine Daten angegeben zu haben. Einige Erziehungsberechtigte betroffener jugendlicher Surfer wiesen darauf hin, dass ihre Söhne oder Töchter noch minderjährig seien und ohne ihre Zustimmung gar keine Verträge abschließen dürfen. Alle Beschwerdeführer bestritten also letztlich, dass überhaupt ein rechtskräftiger Vertrag abgeschlossen wurde, der rechtmäßige Forderungen zur Folge haben könnte. Die Anbieter hingegen ignorierten in fast allen vorliegenden Fällen die E-Mails und Schreiben mit den Einwänden der Betroffenen beharrlich. Statt - mit einigem Aufwand - individuell auf die Einwände zu reagieren, wurden ständig - in der Regel automatisiert und günstig per E-Mail - weitere Mahnungen versandt, in denen eine stetig zunehmende Drohkulisse aufgebaut wurde, um die Verbraucher zu verunsichern und möglichst zur Begleichung des angeblich zustehenden Rechnungsbetrags - zuzüglich Gebühr und Zinsen - zu bewegen. Die reichlich dreisten Drohungen reichten vom möglichen Eintrag in den Datenbestand einer bundesweit tätigen Auskunftei, über die Ankündigung der Einleitung des gerichtlichen Mahnverfahrens, bis hin zur Androhung eines Strafverfahrens wegen Betrugs oder - im Falle minderjähriger Opfer - sogar wegen der vermeintlichen Verletzung der elterlichen Aufsichtspflicht.

Die durch dieses unseriöse Verhalten verärgerten, aber auch vielfach verunsicherten Petenten verlangten daher von der Datenschutzaufsichtsbehörde, die Löschung ihrer Daten bei den Internetanbietern durchzusetzen - in der Regel mit dem Ziel, den Anbietern den weiteren Versand von Rechnungen bzw. Mahnungen unmöglich zu machen. Einige Beschwerdeführer klagten auch darüber, dass die Anbieter die Anfragen der Betroffenen nach § 13 Abs. 7 TMG nicht beantworteten, mit denen Auskunft über zur Person des jeweiligen Petenten gespeicherten Daten, deren Herkunft und mögliche Datenempfänger nach Maßgabe von § 34 BDSG von den Anbietern verlangt wurde.

Bis auf eine Ausnahme firmierten alle der Datenschutzaufsichtsbehörde bekannten Kostenfallen-Anbieter mit hessischer Zweigstelle als englische "Limited" an der gleichen englischen Anschrift und sind korrekt beim englischen House of Companies (ähnlich dem deutschen Handelsregister) angemeldet. Die Anschriften der deutschen Zweigstellen sind in der vorschriftsmäßigen Anbieterkennzeichnung der WWW-Angebote nach § 5 TMG ebenso angegeben wie die Namen der Geschäftsführer. Einige der Firmen existierten nur kurz, viele wechselten im Berichtszeitraum die deutsche Zweigstellenanschrift, den Namen und den Geschäftsführer, was sie aber nicht daran hinderte, immer wieder zu versuchen, mit ständigen Mahnschreiben und weiteren Drohungen die angeblich bestehende Forderung weiterhin einzutreiben. Es kann davon ausgegangen werden, dass ein Teil der angeschriebenen Opfer aus Angst bezahlt und das "Geschäft" der Kostenfallen-Anbieter daher bis heute ergiebig genug ist, um immer wieder neue Internet-Kostenfallen ins WWW zu stellen.

Die Aufsichtsbehörde nahm im Laufe des Jahres mit allen hessischen Zweigstellen der Anbieter solcher WWW-Kostenfallen Kontakt auf und mahnte zunächst die Erteilung der Auskünfte nach § 13 Abs. 7 TMG an die betroffenen Surfer an. Die erforderlichen Auskünfte wurden daraufhin in allen Fällen umgehend vollständig an die Betroffenen erteilt. Die vorherige Nichterteilung der Auskünfte wurde auf Nachfrage mit unzuverlässiger Postzustellung oder individuellen Mitarbeiterfehlern begründet.

Weiterhin forderte die Aufsichtsbehörde die Anbieter auf, mitzuteilen, auf welcher Rechtsgrundlage die Daten der Petenten von dem Unternehmen verarbeitet wurden. Die Aufsichtsbehörde verband dies mit der Empfehlung, die Daten der Petenten zu löschen, da die Betroffenen das Bestehen eines Vertrags bestritten, der nach § 14 Abs. 1 TMG als Rechtsgrundlage für die weitere Verarbeitung der Daten der Betroffenen dienen könnte. Die diesbezüglichen Bemühungen der Datenaufsichtsbehörde blieben allerdings erfolglos. Die Anbieter weigerten sich - in fast gleich lautenden Schreiben - in allen Fällen, die Daten zu löschen und verwiesen auf den grundsätzlich zivilrechtlichen Charakter der Frage, ob ein rechtswirksamer Vertrag abgeschlossen wurde oder nicht. Die Daten seien für die Realisierung der bestehenden Forderung per gerichtlichem Mahnverfahren oder gar für eine Strafanzeige wegen Betrugs nach § 269 StGB weiterhin erforderlich. Die weitere Speicherung der erhobenen Daten erfolge aus Sicht der Anbieter auf der Grundlage des § 14 Abs. 1 TMG, da die Realisierung einer gegen einen Kunden bestehenden Forderung unter die dort geforderte "inhaltlichen Ausgestaltung des bestehenden Vertragsverhältnisses" fällt.

Auch gegenüber der Datenschutzaufsichtsbehörde hielten die Anbieter ihre Drohkulisse wortgewaltig aufrecht. Sobald ein Kunde nachhaltig die Zahlung verweigere oder die im WWW angegebenen Daten falsch seien, gehe das Unternehmen von einem Betrugstatbestand aus. Die weitere Verarbeitung der entsprechenden Daten sei dann zur Wahrung der berechtigten Interessen des Unternehmens in einem Betrugsfall erforderlich und damit auch gegen den Willen des Betroffenen zulässig. Es sei auch nicht ersichtlich, dass bei Betrugsversuchen überwiegende schutzwürdige Interessen der Betroffenen am Ausschluss der Verarbeitung vorliegen würden. Es wurde zudem angekündigt, dass in den Beschwerdefällen, in denen die Petenten bestritten, ihre Daten auf den WWW-Seiten der Anbieter angegeben zu haben, Strafanzeige gestellt würde.

Die Beurteilung der Fragen, ob Preisangaben in den AGB überraschende Klauseln nach § 305c Abs. 1 BGB darstellen, ob es sich bei den WWW-Seiten um eine irreführende Blickfangwerbung handelt oder ob die Preisangaben als leicht erkennbar, leicht lesbar oder sonst gut wahrnehmbar nach § 1 Abs. 6 Preisangabenverordnung (PAngV) zu bewerten sind oder ob Jugendliche ohne Einwilligung der Erziehungsberechtigten Verträge abschließen können und damit letztlich der Frage, ob in den vorliegenden Fällen ein wirksamer Vertragsabschluss vorliegt, liegt nun tatsächlich nicht in der Zuständigkeit der Datenschutzaufsichtsbehörde nach § 38 Abs. 1 BDSG. Obwohl der Datenschutzaufsichtsbehörde und den noch weitaus intensiver mit Internet-Kostenfallen befassten Verbraucherschutzverbänden bislang kein einziger Fall bekannt geworden ist, in denen bei einem aus welchem Grund auch immer zivilrechtlich bestrittenen Vertragsabschluss tatsächlich ein gerichtlicher Mahnbescheid beantragt oder eine Strafanzeige wegen Betrugs gestellt worden wäre, musste die vorgetragene Begründung für die weitere

Speicherung der Daten von der Datenschutzaufsichtsbehörde akzeptiert werden. Eine Löschung der Daten konnte somit in keinem Fall durchgesetzt werden, da vor einer möglichen Datenlöschung immer eine gerichtliche Klärung der geschilderten zivilrechtlichen Fragestellungen erforderlich ist. Weil die Anbieter aber sehr wohl wissen, dass ihre Chancen in einer gerichtlichen Auseinandersetzung sehr gering wären, belassen sie es in der Praxis bisher bei Drohungen und meiden gerichtliche Mahnverfahren, mit denen sie aber weiter drohen, bzw. deren Einleitung sie sich vorbehalten.

Lediglich in einem Fall, in dem der Betroffene weiterhin Mahnungen erhielt, obwohl er den geforderten Betrag bereits gezahlt hatte, wurden die Daten des Petenten nach einem entsprechenden Hinweis der Aufsichtsbehörde bei dem Anbieter aus dem aktiven Datenbestand entfernt.

Eine Nachfrage bezüglich angedrohter Einträge bei einr großen Auskunftei ergab immerhin, dass es sich auch hierbei nur um eine leere Drohung handelte. Keiner der Kostenfallen-Anbieter oder der mit dem Inkasso beauftragten Rechtsanwälte war zu diesem Zeitpunkt Vertragspartner der Auskunftei. Zudem kann die standardmäßige Androhung einer Meldung an die Auskunftei den Empfänger zur Geltendmachung eines zivilrechtlichen Unterlassungsanspruchs aus § 1004 Abs. 1 analog, § 823 BGB berechtigen, wenn nicht unbestrittene oder rechtskräftig festgestellte Forderungen des Anbieters vorliegen (AG Plön, Urteil vom 10. Dezember 2007). Schon aus diesem Grund wäre in keinem der der Aufsichtsbehörde vorliegenden Fälle eine Meldung zulässig gewesen. Diese wurde aber ohnehin immer nur angekündigt, um die Betroffenen einzuschüchtern und zur Zahlung zu bewegen. Da eine Meldung an die Auskunftei in Wahrheit nie erfolgte, konnte die Aufsichtsbehörde die verunsicherten Petenten diesbezüglich zumindest beruhigen. Gegen die bloße Drohung mit einer Meldung kann die Datenschutzaufsichtsbehörde mit den Mitteln des BDSG allerdings nichts unternehmen, da die Ankündigung selbst einer unzulässigen Datenübermittlung faktisch noch keine Datenübermittlung ist und reine Absichtserklärungen nicht vom BDSG erfasst werden. Soweit mit anderen Auskunfteien gedroht wurde, stellte sich heraus, dass es sich ebenfalls um leere Drohungen handelte (vgl. auch die Ausführungen zur Drohung mit der Datenübermittlung an eine angebliche Auskunftei unter Ziffer 7.5 dieses Berichts).

Da das Datenschutzrecht keine Handhabe gegen die dubiose Geschäftemacherei mit Internet-Kostenfallen bietet, wurden die Beschwerdeführer auf die Möglichkeit verwiesen, Strafanzeige gegen die Anbieter zu erstatten und sich wegen der zivilrechtlichen Fragen an die Verbraucherzentralen zu wenden. Im Laufe des Jahres wurden allerdings über 10.000 Verfahren gegen Kostenfallen-Anbieter von den Staatsanwaltschaften Frankfurt und Darmstadt eingestellt. Ein Betrugstatbestand nach § 263 StGB war den Anbietern nach Pressemeldungen der Staatsanwaltschaften ebenso wenig nachzuweisen, wie Wucher, Nötigung, Erpressung oder Irreführung. Auch wenn die Strafanzeigen also folgenlos für die Anbieter blieben, wiesen die Staatsanwaltschaften die Betroffenen ausdrücklich darauf hin, dass die Geltendmachung zivilrechtlicher Ansprüche von den strafrechtlichen Verfahrenseinstellungen unberührt bleibt. Auch die Verbraucherzentralen betonen, dass das Nichtvorliegen eines Straftatbestandes nichts mit der Frage zu tun hat, ob die Verträge rechtswirksam sind und die Internetnutzer die ungewollte Dienstleistung bezahlten müssen oder nicht.

Bei der aktuellen Rechtslage können daher nur noch die Verbraucherzentralen und die Zivilgerichte weiterhelfen. Bei den Verbraucherzentralen gingen im Jahr 2007 bundesweit über 250.000 Beschwerden gegen solche unseriösen Internetanbieter ein. Die Verbraucherzentralen halten mittlerweile ein umfangreiches Informationsangebot zum Umgang mit Kostenfallen im Internet bereit und bieten dabei auch geeignete Musterschreiben für Verbraucher, die in die Kostenfalle getappt sind, zum Download auf ihren Internetseiten an.

Auch wenn der Bundesverband der Verbraucherzentralen e.V. sowie die Zentrale zur Bekämpfung des unlauteren Wettbewerbs e. V. im Berichtsjahr mehrere Urteile gegen Anbieter von Kostenfallen im Internet erwirken konnten (AG München, 16.01.2007, 161 C 23695/06, LG Darmstadt, 08.05.2007, 12 O 532/06, LG Stuttgart, 15.05.2007, 17 O 490/06, LG Frankfurt, 05.09.2007, 3-08 O 35/07, LG Frankfurt, 21.09.2007, 2Ä/03 O 856/06, LG Hanau 07.12.2007, 9 O 870/07), sieht man auf der Seite der Verbraucherschützer bislang trotz eines gegen den größten Kostenfallen-Anbieter eingeleiteten Gewinnabschöpfungsverfahrens grundsätzlich keinen

echten Fortschritt. Der Bundesverband der Verbraucherzentralen e.V. bewertet die bisherigen Urteile gegen Internet-Kostenfallen eher als Pyrrhussiege, da geschädigte Verbraucher sich bei der aktuellen Rechtslage trotz der positiven Urteile gegen unberechtigte Forderungen weiterhin individuell zur Wehr setzen müssen. Wegen der außerordentlich hohen Zahl von Betroffenen und angesichts von Schäden in mehrstelliger Millionenhöhe bleibt zu hoffen, dass die Forderungen des Bundesministers für Ernährung, Landwirtschaft und Verbraucherschutz und der rheinland-pfälzischen Verbraucherschutzministerin nach einer klaren gesetzlichen Regelung zum Schutz vor untergeschobenen Internet-Verträgen sowie engere Vorgaben für die Preisangabe beim Abschluss von Online-Verträgen so bald wie möglich umgesetzt werden.

Den Nutzern des World Wide Web wird geraten, vorsichtiger und sparsamer mit den eigenen Daten im Internet umzugehen und Datenschutzhinweise und Nutzungsbedingungen stets sorgfältig zu lesen. Sensibilität für die Wichtigkeit personenbezogener Daten sowie Aufmerksamkeit und gesunder Menschenverstand sind im Internet mindestens genauso wichtig wie eine Firewall und ein Virenscanner. Misstrauen ist grundsätzlich immer dann anzuraten, wenn die umfangreiche Angabe persönlicher Daten auf Internetseiten zwingend gefordert wird, ohne dass es dafür gute nachvollziehbare Gründe gibt. Solche WWW-Seiten sollten umgehend verlassen werden. Oft findet sich unter den vielen Internetseiten immer noch ein anderes, besseres und günstigeres Angebot.

9.3 Personensuchmaschine im Internet

Ein in Hessen ansässiges Unternehmen brachte Ende Oktober 2007 eine speziell auf die Suche von Personen angelegte Suchmaschine im Internet an den Start. Diese Suchmaschine bietet in einem zweiten Schritt die Möglichkeit, aus den Suchergebnissen ein Profil zu erstellen und auf diese Weise "Reputationsmanagement" zu betreiben. Das Echo der Internetnutzer auf das neue Angebot fiel in den sich mit aktuellen Entwicklungen des Internets befassenden Foren verhalten bis ablehnend aus. Gerade die ausdrückliche Bezeichnung als "Personensuchmaschine" rief den Unmut der Nutzer hervor, obwohl bereits bis zu 30 v.H. der Suchanfragen bei den etablierten Suchmaschinen auf Personen gerichtet sind, und diese sich somit auch als Personensuchmaschinen benutzen lassen. Aufgrund des großen öffentlichen Interesses lud das Regierungspräsidium Darmstadt den Diensteanbieter zu einem Gespräch ein, um diesem Gelegenheit zu geben, das Geschäftskonzept vorzustellen und eine vorläufige datenschutzrechtliche Bewertung des Angebots vornehmen zu können.

Unabhängig von der Möglichkeit einer Profilbildung ist die Suchmaschine für jedermann zugänglich. Sie arbeitet als Metasuchmaschine, sodass bei einer Anfrage nicht das gesamte WWW durchsucht wird, sondern Ergebnislisten zu dem gesuchten Namen aus anderen Suchmaschinen abgefragt bzw. mittels eines Scripts die Suchfunktion allgemein zugänglicher Quellen im Internet genutzt werden, die einen hohen Bezug zu Personen aufweisen, z.B. soziale Netzwerke wie "facebook.com" oder "xing.com", aber auch spezielle Branchendienste wie "anwalt24.de" oder "marketing-boerse.de". Das Ergebnis der Suche ist dadurch wesentlich übersichtlicher gestaltet, am Interesse des Suchenden ausgerichtet und folglich auch dichter, als dies bei herkömmlichen Suchmaschinen der Fall ist.

Mittels der erzielten Suchtreffer ist es in einem zweiten Schritt möglich, ein Personenprofil von sich selber anzulegen. Dazu ordnet man dem eigenen Namen diejenigen Links aus der Trefferliste zu, mit denen man in Verbindung gebracht werden möchte. Dies bezeichnet der Anbieter als "Reputationsmanagement". Ähnlich wie bei anderen sozialen Netzwerken können die Profilinhaber gegenseitig ihre Profile als glaubwürdig bewerten sowie miteinander Bekanntschaft schließen.

Unter rechtlichen Gesichtspunkten ist bei der im Zuge der Verwendung von Suchmaschine und Reputationsmanagement erfolgenden Datenverarbeitung zunächst zu trennen zwischen den personenbezogenen Daten, die im Verhältnis zwischen dem Anbieter des Internetangebots und dem jeweiligen Nutzer verarbeitet werden und den Daten, die den Inhalt der jeweils gefundenen Webseite ausmachen und die für jedermann einsehbar sind, im vorliegenden Fall also die erzeugte Trefferliste zu einem bestimmten Namen.

Während für erstere - die Bestands- und Nutzungsdaten - das TMG gilt, werden letztere - die Inhaltsdaten - von den Regelungen des BDSG erfasst.

In dem Gespräch zwischen dem Suchmaschinenbetreiber und der Aufsichtsbehörde wurde zunächst der Umgang des Anbieters mit den nach den Vorschriften des TMG zu beurteilenden Bestands- und Nutzungsdaten thematisiert. Ursprünglich speicherte der Suchmaschinenbetreiber ohne ersichtliche Rechtsgrundlage bei Suchanfragen die IP-Adresse des jeweiligen Nutzers 72 Stunden lang. IP-Adressen von Nutzern, die ein Profil besitzen, wurden jedoch ohne zeitliche Beschränkung gespeichert. Nach Beanstandung durch die Aufsichtsbehörde hat der Suchmaschinenbetreiber die Speicherung von IP-Adressen gänzlich eingestellt.

Wenn man sich dafür entscheidet, ein Profil anzulegen und die Funktion des Reputationsmanagements zu nutzen, wird dieses erst durch Dritte einsehbar, wenn man es selbst mit einer Bestätigungs-E-Mail aktiviert hat. Nicht aktivierte Profile sind nicht öffentlich zugänglich, werden aber durch den Anbieter gespeichert. Nach § 14 Abs. 1 TMG ist das jedoch nur zulässig, soweit es für die Begründung oder die inhaltliche Ausgestaltung eines Vertragsverhältnisses erforderlich ist. Im Fall eines nicht bestätigten Profils erklärt der jeweilige Nutzer mit diesem Verhalten jedoch gerade, dass er entgegen seiner ursprünglichen Absicht nun doch kein Profil unterhalten möchte. Mangels Vertragsverhältnisses ist dann zweifelhaft, inwieweit eine weitere Speicherung noch gerechtfertigt ist. Bei Redaktionsschluss für diesen Bericht war die Diskussion zu diesem Teilproblem noch nicht beendet.

Bei der Aufsichtsbehörde ging kurz nach Start des Internetdienstes eine Beschwerde ein, die sich gegen die Existenz der Suchmaschine an sich richtete. Der Beschwerdeführer führte an, dass die ausschließlich auf Personen fokussierte Suche ein automatisches, unerwünschtes Profil von ihm erstellen würde. Die Aufsichtsbehörde hat diesen Fall zum Anlass genommen, sich mit der rechtlichen Einordnung der Tätigkeit von Suchmaschinen intensiver auseinanderzusetzen.

Bei den Suchergebnissen handelt es sich, wie bereits erwähnt, um Inhaltsdaten, deren Verarbeitung sich nach den Regelungen des BDSG richtet. Bei der Anwendung des BDSG auf Fallgestaltungen im Internet erweist sich in zunehmendem Maße und an mehreren zentralen Punkten, dass das BDSG den auch in datenschutzrechtlicher Hinsicht bestehenden Herausforderungen des Internetzeitalters nicht vollumfänglich gewachsen ist. So ist zunächst schon sehr fraglich und derzeit in den Meinungsbildungsgremien der Datenschutzaufsichtsbehörden in der Diskussion, ob Suchmaschinenbetreiber überhaupt als verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG angesehen werden können. Obwohl zweifellos feststeht, dass Suchmaschinen mittels der Abfrage von vorhandenen Inhalten im Internet Datenverarbeitung betreiben, geht die Anwendung des § 3 Abs. 7 BDSG jedoch an der primären Funktion der Suchmaschine als "Schlüssel zum Cyberspace" (so die Entschließung der 28. Internationalen Konferenz der Datenschutzbeauftragten, abrufbar unter www.bfdi.bund.de) vorbei. Die Suchmaschinen fungieren im WWW lediglich als Vermittler zu den Inhalten der Webseitenbetreiber. Die primäre Verantwortlichkeit für den Inhalt einer WWW-Seite ist jedoch beim jeweiligen Webseitenbetreiber anzusiedeln. Diesem ist es schließlich zuzurechnen, dass sich ein Inhalt überhaupt im Internet befindet. Angesichts dieses Gefüges von gänzlich unterschiedlich zu gewichtenden Verantwortlichkeitsanteilen wäre es unverhältnismäßig, den bloßen Vermittler zwischen Nachfrage und Angebot als datenschutzrechtlich Verantwortlichen anzusehen (so auch Weichert " Datenschutz bei Suchmaschinen" abrufbar unter www.datenschutzzentrum.de). Dieser Blick auf die tatsächliche Ursächlichkeit für das Vorhandensein von Inhalten im Netz führt das BDSG an seine Grenzen, wenn es um die Beurteilung der Verantwortlichkeit des bloßen Vermittlers zu diesen Inhalten geht, soweit dieser keinen öffentlich abrufbaren "Cache" (eigener temporärer Zwischenspeicher gefundener WWW-Seiten) oder andere zusätzliche eigene Funktionen oder Dienste anbietet. Die vorhandene Rechtsprechung zur zivilrechtlichen Haftung von Suchmaschinenbetreibern will diesen folgerichtig auch nur dann eine Verantwortlichkeit für Inhalte zuweisen, wenn durch die Anzeige des Suchergebnisses tatsächlich eine Verletzung des allgemeinen Persönlichkeitsrechts eingetreten ist und der Suchmaschinenbetreiber auf den entsprechenden Inhalt hingewiesen worden ist (so LG Berlin, AZ.: 27 O 45/05). Diese Sichtweise vertreten auch die Befürworter einer analogen Anwendung des §

10 TMG, der lediglich die sehr begrenzte Verantwortung eines Anbieters regelt, der fremde Inhalte speichert (sog. Host-Provider).

Die obersten Datenschutzaufsichtsbehörden der Länder werden sich im Laufe des Jahres 2008 mit der Frage der Verantwortlichkeit von Suchmaschinenbetreibern für Inhalte im Netz auseinandersetzen. Die Erarbeitung einer von allen Datenschutzaufsichtsbehörden der Länder vertretenen Lösung erachtet das Regierungspräsidium Darmstadt als notwendig.

Wenn man entgegen der tatsächlichen Verantwortlichkeitssituation annimmt, dass auch Suchmaschinenbetreiber als in datenschutzrechtlicher Hinsicht Verantwortliche anzusehen seien, die Gegner von Löschungs- und Auskunftsansprüchen nach BDSG sein könnten, stellt sich die Frage, ob das BDSG überhaupt Erlaubnistatbestände bereithält, auf die sich der Suchmaschinebetreiber berufen kann. Mit den Kernnormen für die erlaubte Datenverarbeitung im nicht-öffentlichen Bereich (§ 28 BDSG Datenverarbeitung zu eigenen Zwecken sowie § 29 BDSG Datenverarbeitung zum Zweck der Übermittlung) kann der weltweiten Strahlkraft und dem presseartig anmutenden Veröffentlichungscharakter, der dem Internet innewohnt, schließlich kaum Rechnung getragen werden:

§ 29 BDSG wurde geschaffen, um die Datenverarbeitung von Auskunfteien, Unternehmen der Markt- und Meinungsforschung und Adresshändlern zu regulieren. Auch wenn einzelne Aspekte dieser Tätigkeit mit der Tätigkeit von Suchmaschinen und deren Möglichkeiten übereinstimmen mögen, passt diese Norm doch von ihrer Ausrichtung her nicht auf Internetsuchmaschinen. Diese sind schließlich nur auf die Suche von Informationen (bei der Personensuchmaschine nach Vor- und Nachname) ausgelegt, die bereits öffentlich im WWW zugänglich sind. Insofern agiert die Suchmaschine hier nicht wie eine klassische Auskunftei als Anbieter der Ware "Daten". Würde man § 29 BDSG trotz dieser Bedenken zur Anwendung bringen, wären die hohen, an sich für Auskunfteien geschaffenen Anforderungen des § 29 BDSG nur mit größerem juristischen Begründungsaufwand zu erfüllen.

Das Anzeigen eines Suchergebnisses wäre als Übermittlung im Sinne des § 3 Abs. 4 Nr. 3 BDSG zu betrachten, die in § 29 Abs. 2 Nr. 1 a BDSG geregelt ist. Danach wäre eine Übermittlung an einen Anfrager nur möglich, wenn dieser ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht hat. Die Natur des Internet macht eine solche Glaubhaftmachung nur schwer möglich, da darunter regelmäßig die konkrete Darlegung des berechtigten Interesses - ggf. unter Vorlage von Dokumenten - durch einen identifizierten Anfrager zu verstehen ist. Die direkte Anwendung der Norm würde folglich dazu führen, dass mangels des Nachweises eines berechtigten Interesses am Suchergebnis die Tätigkeit der Suchmaschine nach § 29 BDSG als nicht zulässig anzusehen wäre.

Aus diesem Ergebnis kann jedoch kaum geschlossen werden, dass der Gesetzgeber die Tätigkeit von Suchmaschinen unterbinden wollte. Vielmehr zeigt sich an dieser Stelle nun deutlich, dass das BDSG ursprünglich nicht dafür geschaffen worden ist, auch die im und durch das Internet stattfindende Datenverarbeitung zu regeln. Solange der Gesetzgeber an dieser Stelle keine eindeutigen Regelungen trifft, könnte es eine denkbare Lösung darstellen, angesichts der Unmöglichkeit einer Glaubhaftmachung im Internet, die Anforderungen zu senken, die der Gesetzgeber an diese stellt und den § 29 BDSG zumindest im Hinblick auf Suchmaschinen rechtsfortbildend auszulegen.

Das Erfordernis der Glaubhaftmachung dient dem Schutz des Einzelnen vor der ungehemmten, anlassfreien Recherche Dritter. Von diesen wird daher verlangt, ein berechtigtes Interesse an bestimmten Informationen, die gerade nicht für jedermann zugänglich sind, auch tatsächlich nachweisen. Eine Suchmaschine ist von der Intensität des datenschutzrechtlichen Eingriffs nicht mit einer Auskunftei zu vergleichen. Suchmaschinen eröffnen lediglich einen Zugang zu allgemein zugänglichen Daten, die ohnehin von jedermann abgerufen werden können. Demzufolge wäre der Schutzmechanismus, den das strenge Erfordernis der Glaubhaftmachung des § 29 Abs. 2 Nr. 1 a BDSG darstellt, bei einer Suchmaschine nicht erforderlich. Vielmehr könnte man die Eingabe des jeweiligen Suchbegriffs als Dokumentation eines berechtigten Interesses ausreichen lassen. Jedoch würde diese Auslegung aus datenschutzrechtlicher Sicht zu einer Schieflage führen. Einerseits wird durch eine solche Auslegung die Schutzfunktion des § 29 BDSG unterlaufen

und man käme zum selben Ergebnis, wenn man § 29 BDSG unangewendet ließe. Andererseits führt die direkte Anwendung des § 29 BDSG auf Suchmaschinen zu einem unangemessen harten Ergebnis. Aus diesen Ausführungen lässt sich folglich in erster Linie der Schluss ziehen, dass § 29 BDSG für eine Anwendung auf Suchmaschinen im Internet nicht geeignet und seine Anwendung insofern in Verbindung mit der Tätigkeit einer Suchmaschine problematisch erscheint.

Wenn man § 28 BDSG statt § 29 BDSG anwenden würde, ergäbe sich die nachfolgende Bewertung. Als Erlaubnistatbestand käme § 28 Abs. 1 Nr. 3 BDSG in Frage, der als ein Ausdruck der Informationsfreiheit aus Art. 5 Abs. 1 S. 1 GG die Übermittlung personenbezogener Daten erlaubt, wenn es sich dabei um allgemein zugängliche Daten handelt. Darunter sind solche Daten zu verstehen, die sich sowohl ihrer Zielsetzung als auch ihrer Publikationsform nach dazu eignen, einem individuell nicht bestimmbaren Personenkreis Informationen zu vermitteln. Daten, die bereits auf Internetseiten veröffentlicht worden sind, sind folglich als allgemein zugänglich anzusehen.

Problematisch erscheint, dass eine Suchmaschine bei der Anzeige ihrer Ergebnisse keine Rücksicht darauf nehmen kann, dass nicht jedes im Internet befindliche Datum auch mit Willen und Billigung des Betroffenen veröffentlicht worden ist. Es ist zu unterscheiden zwischen Daten, die jemand selbst über sich ins Netz gestellt hat, solchen, deren Veröffentlichung man billigend in Kauf nimmt, und schließlich den Daten, die von Dritten über die eigene Person ohne deren Wissen und Wollen ins Netz gestellt worden sind.

§ 28 Abs. 1 Nr. 3 BDSG trägt diesem schon aus dem Vor-Internetzeitalter bekannten Problem Rechnung, indem allgemein zugängliche Daten nur dann verarbeitet werden dürfen, wenn das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung das berechtigte Interesse der datenverarbeitenden Stelle nicht offensichtlich überwiegt. Diese Interessenabwägung hat allerdings - für eine Suchmaschine unmöglich - im Vorfeld des Verarbeitungsvorgangs statt zu finden. Jedoch geht der Gesetzgeber bei allgemein zugänglichen Angaben ohnehin von der Vermutung aus, dass ihre Verwendung den Belangen des Betroffenen grundsätzlich nicht widerspricht. Davon ist in der Praxis nur bei einem extremen Auseinanderfallen von Verarbeitungs- und Ausschlussinteresse auszugehen.

Ein solches hatte der Beschwerdeführer im vorliegenden Fall gerade nicht dargelegt. Die angezeigten Treffer hatten keinen ehrverletzenden oder rufschädigenden Inhalt und zeichneten sich im übrigen dadurch aus, dass sie überwiegend auf die Aktivitäten und eigene Initiative des Beschwerdeführers zurückzuführen waren, der selbst seit Jahren eine hochfrequentierte Webseite betreibt und über diese Internetpräsenz hinaus sehr viele Inhalte auf anderen Seiten im Internet unter seinem Namen veröffentlicht hat. Einige wenige andere Treffer betrafen Seiten mit Informationen, die sein Arbeitgeber zulässigerweise veröffentlicht hatte.

Angesichts der unsicheren Rechtslage ist die Aufsichtsbehörde bei der Frage der rechtlichen Einordnung von Suchmaschinen noch nicht zu einer gefestigten Position gelangt. Sie ist bestrebt, im Gespräch mit anderen Aufsichtsbehörden eine gemeinsame Haltung zu entwickeln und auch spezielle Zusatzfunktionen einzelner Anbieter vertieft zu prüfen und rechtlich zu bewerten. Dabei wird auch die auf europäischer und internationaler Ebene stattfindende Datenschutzdiskussion über Suchmaschinen zu berücksichtigen sein. Noch in diesem Jahr wird dazu eine Entschließung der Art. 29 - Gruppe erwartet, wobei sich schon jetzt Einigkeit darüber abzeichnet, dass das bislang geltende Recht die durch Suchmaschinen aufgeworfenen Fallgestaltungen und Fragestellungen kaum erfassen kann.

9.4 Auskunftserteilung über Kundenkonto bei Online-Flugbuchungen

Eine Beschwerdeführerin, welche berufsmäßig häufig ins In- und Ausland verreist, nahm Ihre Flugbuchungen regelmäßig "online" auf der Internetseite eines Reiseunternehmens vor. Im Sinne des § 13 Abs. 7 TMG bzw. § 34 Abs. 1 BSDG verlangte sie von dem Unternehmen Auskunft darüber, welche Daten es zu ihrer Person gespeichert hatte, woher diese stammten, über welchen Zeitraum und aus welchen Gründen die Speicherung erfolgte und an welche Unternehmen und zu welchem Zweck die Daten weitergegeben wurden. Das Unternehmen erteilte auf ihre Nachfrage die Auskunft, es habe

keine Daten zu ihrer Person gespeichert. Da die Beschwerdeführerin aber selbst auf ihr Online-Kundenkonto zugreifen und dort die Daten ihrer letzten Reisebuchungen abrufen konnte, wandte sie sich mit der Bitte um Unterstützung bei ihrem Auskunftsersuchen an die Aufsichtsbehörde. Durch die offensichtlich falsche Antwort des Unternehmens verärgert, forderte die Beschwerdeführerin nun zusätzlich die vollständige Löschung der Daten nach erfolgter Auskunftserteilung.

Auf Nachfrage der Datenschutzaufsichtsbehörde bei dem betrieblichen Datenschutzbeauftragten des Reiseunternehmens mit der Aufforderung, diesen Widerspruch zu klären, stellte sich heraus, dass das Buchungsportal auf der Internetseite des Reiseunternehmens von einer hierauf spezialisierten Fremdfirma betrieben wird. Die Datenverarbeitung im Online-Buchungsportal war daher getrennt von der Verarbeitung in den eigenen Systemen des Reiseunternehmens zu sehen. Auf dem Server des Buchungsportals der Fremdfirma werden nur die Daten gespeichert, die Kundinnen und Kunden des Reiseunternehmens dort bei ihrer Buchung selbst eingegeben haben, sowie die notwendigen Daten von weiteren im Rahmen der Reisebuchung in Anspruch genommenen Leistungserbringern, z. B. Hotels, Veranstalter usw.. Die Benutzerprofile in diesem Buchungsportal können vom jeweiligen Benutzer selbst gelöscht oder geändert werden. Bei Nichtlöschung durch den Benutzer erfolgt die Aufbewahrung im Buchungsportal für sechs Monate, danach erfolgt eine automatische Archivierung.

In den eigenen Systemen des Reiseunternehmens erfolgt getrennt davon eine Speicherung der Daten, wobei die Daten, die den gesetzlichen Aufbewahrungspflichten nach dem Handelsgesetzbuch (HGB) oder der Abgabeordnung (AO) unterliegen, nach einer gewissen Zeit zur Aufbewahrung in ein Archivierungssystem überführt werden. Die Daten werden dort für den gesetzlich vorgeschriebenen Zeitraum vorgehalten, sind aber nach § 35 Abs. 3 Nr. 1 BDSG für jede andere Nutzung gesperrt.

Nach Auskunft des Reiseunternehmens werden die gespeicherten Daten der Kunden ausschließlich zum Zweck der Reiseabwicklung verwendet. Eine Übermittlung findet nur an die mit der Reiseabwicklung beauftragten Firmen statt. Aufgrund der Beschwerde wurde eine Löschung der Benutzerprofile der Beschwerdeführerin durch das Reiseunternehmen vorgenommen, wobei allerdings darauf hingewiesen wurde, dass bei Anmeldung mit einer neuen Benutzerkennung selbstverständlich wieder eine Datenspeicherung im Online-System erfolgt.

Nach einigen Monaten wandte sich die Petentin erneut an die Aufsichtsbehörde und schilderte Probleme bei dem Versuch, die anlässlich einiger Reisen neu angelegten Benutzerprofile in dem Buchungsportal zu löschen. Ein Zugriff auf die Benutzerprofile sei teilweise nicht möglich, da ihr hierfür kein Kennwort vorliegen würde. Habe sie Kenntnis von den Zugangdaten und damit den Zugriff auf eines der Benutzerprofile erlangt, sei dann - anders als zuvor zugesagt - dennoch keine Löschung der Profile möglich.

Die diesbezüglichen Nachforschungen der Aufsichtsbehörde und des erneut eingeschalteten betrieblichen Datenschutzbeauftragten ergaben, dass die Petentin die E-Mails des Reiseunternehmens mit den für den Zugriff auf das jeweilige Benutzerkonto notwendigen Passworten nicht immer zur Kenntnis genommen, sondern teilweise als unverlangte E-Mail (Spam) aussortiert und ungelesen gelöscht hatte. Weiterhin stellte sich heraus, dass die Petentin versucht hatte, bei Profilen, zu denen ihr das Kennwort vorlag, die Daten im Buchungsportal sofort nach der Buchung und Bezahlung zu löschen. Das Reiseunternehmen stellte hierzu gegenüber der Datenschutzaufsichtsbehörde glaubhaft dar, dass eine Aufbewahrung der Daten zumindest bis zum Ende der Reise und der Abwicklung aller Buchungen im Zusammenhang mit den beauftragten Leistungserbringern erforderlich ist und daher eine frühere Löschung nicht möglich sei. Vorzeitige Löschversuche der Benutzerin mussten daher erfolglos bleiben. Die Beschwerdeführerin wurde darüber informiert, dass es nicht im Verschulden des Reiseunternehmens liegt, wenn die E-Mails, welche das jeweilige Passwort enthalten, von ihr als Spam aussortiert wurden und die Aufsichtsbehörde die Rechtsauffassung des Unternehmens teilt, dass einer sofortigen Datenlöschung im vorliegenden Fall die weiterhin bestehende Notwendigkeit der Kenntnis der Daten für die Erfüllung des Zwecks der Speicherung entgegensteht. Eine Datenlöschung nach § 35 Abs. 2 Nr. 3 BDSG kann also nicht sofort nach Buchung der Reise erfolgen.

Auch das Anlegen eines Benutzerkontos als solches bemängelte die Petentin. Sie wurde darauf hingewiesen, dass dies letztlich nicht zu einer zusätzlichen Datenspeicherung führt, da alle von ihr bei der Buchung eingegebenen Daten auch gespeichert würden, wenn das Online-Buchungsportal nicht über Benutzerkonten verfügen würde. Allerdings bestünde dann für die Kunden keine Möglichkeit mehr, selbst eine Überprüfung der eigenen Daten und der einzelnen Buchungen durchzuführen.

Die zunächst unrichtige Auskunftserteilung des Unternehmens entgegen § 34 Abs. 1 BDSG wurde von der Aufsichtsbehörde beanstandet, da sich das Unternehmen auch die Datenverarbeitung des Buchungsportalanbieters zurechnen lassen muss und schon aus Transparenzgründen eine entsprechend umfassende Auskunftserteilung hätte erfolgen müssen.

Außerdem wurde das Unternehmen um eine frühzeitige Archivierung von elektronischen Belegen, möglichst innerhalb eines Jahres, gebeten, da der Aufsichtsbehörde während der Beschwerdebearbeitung von der Petentin aktuelle Ausdrucke über Reisen vorgelegt wurden, die zu diesem Zeitpunkt bereits drei Jahre abgeschlossen waren. Das Unternehmen ordnete daraufhin eine Archivierung der aufbewahrungspflichtigen Daten sechs Monate nach Ende der jeweiligen Reise an, sperrte die Daten der Petentin in den eigenen Systemen und löschte deren dort gespeichert E-Mail-Adressen, wie von der Beschwerdeführerin gewünscht.

10. Aspekte internationaler Datenverarbeitungen

10.1 Safe Harbor - Reichweite der Zertifizierung

Der betriebliche Datenschutzbeauftragte eines Unternehmens wandte sich an die Aufsichtsbehörde, sein Unternehmen wolle in Geschäftsbeziehungen mit einem in den USA ansässigen Unternehmen A treten und zu diesem Zweck personenbezogene Daten an das Unternehmen A übermitteln. Katalogausnahmen im Sinne des § 4 c Abs. 2 BDSG seien nicht gegeben und das Unternehmen A habe sich nach seinen Erkenntnissen auch nicht dem Safe Harbor Abkommen unterworfen. Die Vertreter des Unternehmens A hätten jedoch darauf hingewiesen, dass das Unternehmen A eine hundertprozentige Tochtergesellschaft des Unternehmens B sei. Das Unternehmen B - die Konzernmutter- seinerseits sei Safe Harbor-zertifiziert.
Daher stelle sich nun die Frage, ob personenbezogene Daten an das Unternehmen A exportiert werden dürften.

Die Aufsichtsbehörde beantwortete diese Anfrage mit dem Hinweis, dass maßgeblich ist, was konkret in der Safe Harbor-Liste (im Internet abrufbar unter: "http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list") bei dem Unternehmen B eingetragen ist. Die Safe Harbor-Eintragungen enthalten nämlich genaue Aussagen, inwieweit Tochtergesellschaften umfasst sind.

Wenn die US-Tochtergesellschaften des Unternehmens B umfasst wären, würde die Eintragung in der Safe Harbor-Liste für das Unternehmen B lauten: "B-Corporation/Company and its controlled U.S. subsidiaries".

Möglich ist auch, dass nicht alle beherrschten Tochtergesellschaften, sondern nur bestimmte von der Safe Harbor-Zertifizierung umfasst sind. Dann würde die Eintragung lauten: "B-Corporation/Company and its controlled U.S. subsidiaries, except as noted".
In der zugehörigen Safe Harbor Information ist dann genau aufgeführt, welche US-Konzerngesellschaften nicht erfasst sind: "This certification does not apply to the following subsidiaries: ……".

Selbstverständlich können nur solche Tochtergesellschaften erfasst sein, die ihren Sitz in den USA haben, denn die Safe Harbor-Zertifizierung bedeutet, dass sich das Unternehmen der Datenschutzkontrolle ("Enforcement") durch eine US-Behörde, nämlich grundsätzlich der Federal Trade Commission (US-Handelsministerium) oder dem Department of Transport (US-Verkehrsministerium), unterwirft. Deren Kontrollzuständigkeit ist insoweit auf die USA begrenzt.

Im konkreten Fall wäre also zu prüfen, ob sich die Safe Harbor-Zertifizierung auch auf das Unternehmen A erstreckt.

Für die Frage, ob Daten an A übermittelt werden dürfen, käme es zusätzlich darauf an, ob auch die konkreten Daten von der Safe Harbor-Zertifizierung erfasst sind. Auch insoweit ist die Reichweite der Safe Harbor-Zertifizierung aus der Safe Habor-Liste und aus der zugehörigen Safe Harbor Information zu jedem Unternehmen zu entnehmen, z. B. ob und inwieweit Personaldaten, ob nur Offline- oder auch Online-Daten erfasst sind.
Ferner sind auch bei einem Drittstaatentransfer stets die Voraussetzungen der "1. Stufe", insbesondere § 28 BDSG, zu prüfen (siehe Ziffer 7.4 des 15. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Drs. 15/4659 sowie Ziffer 9.2 des 20. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Drs. 16/7646).

10.2 Safe Harbor - Weitergabe der Daten durch das Safe-Harbor-zertifizierte Unternehmen

Übermittelt ein in Deutschland ansässiges Unternehmen personenbezogene Daten an die Safe-Harbor-zertifizierte Konzernmutter in den USA und übermittelt diese die Daten weiter an ein drittes Unternehmen in den USA, stellt sich die Frage, unter welchen Voraussetzungen dies zulässig ist. Ferner ergibt sich die Frage, ob und inwieweit das datenexportierende deutsche Unternehmen prüfen muss, dass diese Voraussetzungen vorliegen.

Bezüglich der ersten Frage ist auf die Safe-Harbor-Entscheidung der EU-Kommission bzw. das Safe-Harbor-Abkommen (Im Internet abrufbar unter: "http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_de.htm") zu verweisen, denn hierin sind die Voraussetzungen für eine Weiterübermittlung geregelt. In dem "Grundsatz der Weitergabe" im Anhang 1 zur Safe-Harbor-Entscheidung heißt es:
"Eine Organisation darf Daten nur dann an Dritte weitergeben, wenn sie die Grundsätze der Informationspflicht und Weitergabe anwendet. Möchte eine Organisation Daten an einen Dritten weitergeben, der in ihrem Auftrag tätig wird, so kann sie dies tun, sofern der Dritte entweder dem ‚Sicheren Hafen' angehört oder der EG-Datenschutzrichtlinie unterliegt oder von einer anderen Feststellung angemessenen Schutzniveaus erfasst wird oder sich schriftlich in einer Vereinbarung mit der Organisation dazu verpflichtet, mindestens das Maß an Schutz personenbezogener Daten zu gewährleisten, das in den entsprechenden Grundsätzen des ‚Sicheren Hafens' gefordert wird."
Ein spezieller Datenschutz-Vertrag zwischen einem Safe-Harbor-zertifizierten Empfänger und der dritten Stelle ("Onward Transfer Agreement") allein kann danach nur im Fall der Auftragsdatenverarbeitung, wenn also die dritte Stelle lediglich als Dienstleister für die Datenverarbeitung fungiert, eine Weiterleitung an eine andere Stelle im Drittstaat rechtfertigen.

Bei der Weiterübermittlung durch ein US-Unternehmen an einen selbständigen Dritten gilt der "Grundsatz der Wahlmöglichkeit", wonach die betroffenen Personen die Möglichkeit haben müssen, der Übermittlung zu widersprechen; bei sensitiven Daten ist ohnehin eine Einwilligung erforderlich. Ein "Onward Transfer Agreement" reicht für diesen Fall nicht, denn der Grundsatz der "Weitergabe" lässt den Grundsatz der "Wahlmöglichkeit" im Anhang zur Safe-Harbor-Entscheidung unberührt, wie sich auch aus der Formulierung des Grundsatzes der "Weitergabe" ergibt. Im oben zitierten Satz 1 heißt es, dass die Grundsätze der Informationspflicht und Weitergabe angewendet werden müssen. Im oben zitierten Satz 2 ist ausdrücklich nur die Übermittlung an den "...Dritten,.. der in ihrem Auftrag tätig wird." geregelt. Auch der Umkehrschluss aus der diesbezüglichen Fußnote, wonach der Grundsatz der Wahlmöglichkeit nicht gilt, wenn der Dritte im Auftrag oder auf Anweisung der Organisation tätig wird, bestätigt dies.

Einer anderen an die Aufsichtsbehörde gerichteten Beratungsanfrage lag der Fall zugrunde, dass die in den USA ansässige Safe-Harbour-zertifizierte Konzernmutter einen ebenfalls in den USA ansässigen Datenverarbeitungsdienstleister, der nicht Safe-Harbor-zertifiziert war (vgl. hierzu oben Ziffer 9.1), mit bestimmten Datenverarbeitungen beauftragt und zu diesem Zweck personenbezogene Mitarbeiterdaten des deutschen Tochterunternehmens an diesen weitergeleitet hatte. Da in diesem Fall die dritte Stelle nur als "Auftragsverarbeiter" fungiert, könnte hier also ein "Onward Transfer Agreement" die Weiterübermittlung an diesen rechtfertigen.

Für das deutsche Tochterunternehmen war nun fraglich, ob es prüfen müsse, ob die US-Konzernmutter, die als eigenständige verantwortliche Stelle ("Controller") fungierte, eine ausreichende Datenschutzvereinbarung mit dem Dienstleister getroffen hat.

Die Aufsichtsbehörde teilte hierzu nach Abstimmung in der Arbeitsgruppe Internationaler Datenverkehr mit, dass die Übermittlung in die USA keine totale Zäsur darstellt, die den Datenexporteur von jeder weiteren Verantwortung freistellt. Vielmehr hat er zumindest dann eine Prüfpflicht, wenn sich Anhaltspunkte für die Verletzung des Datenschutzrechts ergeben, weil sich z.B. die Rechtswidrigkeit der Weiterverarbeitung aufdrängt. Entsprechendes muss auch bei der Verwendung der Standardverträge vom Juni 2001 und Dezember 2004 gelten. Zu der Besonderheit bei der Einschaltung eines Unterauftragnehmers in einem Drittstaat durch einen ebenfalls in einem Drittstaat ansässigen "Auftragsverarbeiter", der die Daten aufgrund des Standardvertrags vom Dezember 2001 erhalten hat, siehe Fallgruppe A der Handreichung der Aufsichtsbehörden, abrufbar unter "www.rp-darmstadt.hessen.de", Pfad: Sicherheit&Ordnung/Datenschutz/-Auslandsdatenverkehr).
Im Übrigen besteht aber keine allgemeine Pflicht zur Prüfung, ob der Datenimporteur einen Vertrag bzgl. der Weiterübermittlung ("Onward Transfer-Aggreement") geschlossen hat. Es besteht auch keine grundsätzliche Pflicht zur Kontrolle, ob durch einen solchen Vertrag ein ausreichendes Datenschutzniveau bei der dritten Stelle im Drittstaat gewährleistet wird, auch keine Pflicht zur diesbezüglichen Plausibilitätskontrolle.

11. Arbeitnehmer Datenschutz

11.1 Einschaltung einer Beratungsfirma bei einem Personalauswahlverfahren

Wenn man sich auf eine Stellenanzeige bewirbt, rechnet man entweder mit einer Einladung zu einem Vorstellungsgespräch oder mit einer Absage – und zwar von dem Unternehmen, bei dem man sich beworben hat. Sehr verwundert war daher eine Bewerberin, als sie eine Absage nicht von der Firma erhielt, an die ihr Bewerbungsschreiben gerichtet war, sondern von einer Unternehmensberatung, mit der sie noch nie in Kontakt gestanden hatte. In ihrer an die Aufsichtsbehörde gerichteten Beschwerde gab die Betroffene an, auch sonst keinerlei Hinweise auf die Einbindung Dritter in das Bewerbungsverfahren erhalten zu haben.

Das Unternehmen führte in seiner Stellungnahme aus, erstmals eine Unternehmensberatung in ein Bewerber-Auswahlverfahren eingeschaltet zu haben. Aufgabe dieses Service-Unternehmens war es, eine Vorauswahl für die Bewerbergespräche zu treffen sowie die ausgewählten Bewerber einzuladen, die Gespräche selbst zu begleiten und die Absagen an die nicht ausgewählten Bewerber zu versenden.

Die Beauftragung einer Personalberatung zur Durchführung von Bewerbungsverfahren ist datenschutzrechtlich nicht zu beanstanden. Allerdings besteht in einem solchen Fall für die verantwortliche Stelle die Verpflichtung, die Bewerber über die Kategorien der Empfänger ihrer Daten zu unterrichten. Diese Information kann nur entfallen, wenn die Bewerber nach den Umständen des Einzelfalles und der Lebenserfahrung mit der Weitergabe ihrer Daten an den Empfänger hätten rechnen müssen. Diese Voraussetzungen liegen aber bei der Einschaltung eines externen Personalberaters nicht vor, denn es handelt sich hierbei keineswegs um eine allgemein übliche Praxis. Auch in der Stellenanzeige war die Beteiligung einer Beratungsfirma nicht erwähnt. Die Bewerber hätten also über die Hinzuziehung des externen Personalberaters informiert werden müssen, wobei die Nennung des Namens des Service-Unternehmens nicht erforderlich gewesen wäre.

Die Tatsache, dass das Unternehmen seiner Unterrichtungspflicht nach § 4 Abs. 3 Nr. 3 BDSG nicht nachgekommen war, wurde von der Aufsichtsbehörde beanstandet. Seitens der Unternehmensleitung wurde versichert, zukünftig bereits in die Stellenanzeige einen entsprechenden Hinweis aufzunehmen, sodass eine weitere Information an die Bewerber dann nicht mehr erforderlich ist.

11.2 Mithören und Aufzeichnen von Telefongesprächen

Immer wieder erhält die Aufsichtsbehörde Anfragen oder Beschwerden, die sich auf das - meist in Call-Centern praktizierte - Mithören und Aufzeichnen von Telefongesprächen beziehen.

Als Maßnahme der Qualitätssicherung wurden in einem Call-Center zu Trainings- und Schulungszwecken Gespräche im sogenannten One-Way-Verfahren aufgezeichnet. Hierbei wird nur das aufgezeichnet, was der Call-Center-Agent sagt, nicht aber das, was der Gesprächspartner sagt. Die Mitarbeiter hatten bei Abschluss des Arbeitsvertrags durch Unterzeichnung einer Vereinbarung über "Silent Monitoring" in die Aufzeichnung der Telefonate eingewilligt. Eine Rückfrage bei dem Unternehmen ergab, dass zwar nur ca. 5 v.H. der aufgezeichneten Gespräche abgehört und ausgewertet wurden, aufgezeichnet wurden aber sämtliche von den Agenten geführten Gespräche. Dieses Verfahren wurde von der Aufsichtsbehörde beanstandet.

Eine Befugnis zum Aufzeichnen von Telefongesprächen in Call-Centern besteht nur dann, wenn die jeweiligen Gesprächspartner - beim One-Way-Verfahren nur die Call-Center-Agenten - hierin eingewilligt haben oder eine gesetzliche Erlaubnis besteht. Nach § 4a Abs. 1 BDSG ist eine Einwilligung aber nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Die Rechtswirksamkeit von Einwilligungserklärungen im Arbeitsverhältnis ist allerdings immer kritisch zu bewerten, weil es wegen des Abhängigkeitsverhältnisses der Arbeitnehmer oft an der Freiwilligkeit der Einwilligung fehlt. Häufig müssen sich Mitarbeiter eines Call-Centers schon bei Eingehung des Arbeitsverhältnisses zwangsläufig - wie auch in diesem Fall durch Unterzeichnung der Vereinbarung zum "Silent Monitoring" - mit der betriebsbedingten Aufzeichnung von Gesprächen einverstanden erklären. Dem Bewerber bzw. Mitarbeiter bleibt hier nur die Wahl, entweder zuzustimmen oder auf die Eingehung des Arbeitsverhältnisses zu verzichten.

Diese Zwangssituation muss zur Wahrung des Persönlichkeitsrechts des Arbeitnehmers dadurch ausgeglichen werden, dass die Einwilligung nicht mehr gestattet, als betrieblich - z.B. zum Zweck der Qualitätssicherung und Schulung - notwendig ist. D. h. der Arbeitgeber darf zwar die "Qualität" der Arbeit der Call-Center-Agenten kontrollieren, um ggf. das Arbeitsverhalten verbessern zu können. Er darf aber nicht die Beschäftigten einem permanenten Überwachungsdruck aussetzen, da dieser einen schweren Eingriff in die Persönlichkeitsrechte der Betroffenen darstellen würde.

Ein solcher unzulässiger Überwachungsdruck war in vorliegendem Fall dadurch gegeben, dass beim One-Way-Verfahren sämtliche Gespräche der Agenten aufgezeichnet wurden, wodurch die Mitarbeiter sich - auch bei einer Auswertung von nur 5 v.H. - ständig kontrolliert fühlen mussten und dem Arbeitgeber darüber hinaus auch die Möglichkeit einer lückenlosen Leistungs- und Verhaltenskontrolle der Mitarbeiter eröffnet wurde.

Der Aufforderung der Aufsichtsbehörde, seine Aufzeichnungspraxis datenschutzkonform zu gestalten, ist das Unternehmen nachgekommen. Gesprächsaufzeichnungen werden jetzt nur noch in dem erforderlichen, d.h. dem zulässigen stichprobenartigen Umfang durchgeführt. Die Silent Monitoring Vereinbarung wurde entsprechend überarbeitet.

In einem anderen Fall gab es zwar keine Anhaltspunkte für eine unzulässige Kontrolle der Mitarbeiter, aber ein Anrufer der Service-Hotline eines Unternehmens fühlte sich in seinen Persönlichkeitsrechten durch die Aufzeichnung des Gesprächs verletzt. Hier wurde dem Anrufer folgender Ansagetext verlesen:

"Sie werden gleich weiter verbunden, dabei kann ihr Anruf zur Qualitätsverbesserung aufgezeichnet werden."
Nach Auskunft des Unternehmens musste der Kunde bei seinem Anruf nicht in jedem Fall mit einem Gesprächsmitschnitt rechnen, da nur zur internen Qualitätssicherung nach Zufallsauswahl aufgezeichnet wurde. Dementsprechend war auch die Ansage am Anfang des Gesprächs formuliert.

Das ohne Einwilligung der Gesprächspartner erfolgende Aufzeichnen von Gesprächen ist rechtswidrig und grundsätzlich nach § 201 StGB strafbar. Dem Gesprächspartner ist daher **vor** Einschaltung des Bands die Möglichkeit zu geben, der Aufzeichnung zuzustimmen oder sie abzulehnen.

Dem Gesprächspartner wurde hier aber weder Gelegenheit zur vorherigen Einwilligung oder Ablehnung eingeräumt, noch enthielt die Ansage einen Hinweis, dass der Kunde mit seinem Schweigen und der Fortführung des Gesprächs in die mögliche Aufzeichnung einwilligt. Auch eine Einwilligung durch konkludentes Handeln konnte daher nicht unterstellt werden. Aber auch durch einen entsprechenden Hinweis in der Bandansage hätten sich Zweifel, ob eine rechtswirksame Einwilligung durch konkludentes Handeln vorliegt, nicht ohne weiteres ausräumen lassen. Die Anrufer beabsichtigten mit Ihrem Anruf, ihren Dienstleistungswunsch vorzutragen. Die Gründe dafür, dass der Kunde das Gespräch trotz Hinweises auf eine Aufzeichnung fortführt, können vielfältig sein und müssen nicht bedeuten, dass er damit einverstanden ist. Das Verfahren muss so gestaltet sein, dass der Anrufer eindeutig die Wahl und entsprechende Möglichkeit hat, die Aufzeichnung zu verhindern.

Die Aufsichtsbehörde forderte daher das Unternehmen auf, das Aufzeichnungsverfahren den gesetzlichen Erfordernissen anzupassen und dem Gesprächspartner die Gelegenheit zur vorherigen Einwilligung oder Ablehnung einzuräumen. Das Unternehmen hat daraufhin den Ansagetext wie folgt geändert:

"Zur Qualitätssicherung kann ihr Anruf mitgeschnitten werden. Wenn Sie damit einverstanden sind, drücken Sie bitte die Rautetaste."

Wiesbaden, 15. September 2008

Der Hessische Ministerpräsident:
Koch

Der Hessische Minister des Innern und für Sport:
Bouffier