16. Wahlperiode

Drucksache **16/5892**

HESSISCHER LANDTAG

16. 08. 2006

Vorlage
der Landesregierung

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

Vorgelegt mit der Stellungnahme zum Vierunddreißigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten - Drucks. 16/5359 - nach § 30 Abs. 2 des Hessischen Datenschutzgesetzes in der Fassung vom 7. Januar 1999.

Eingegangen am 16. August 2006 · Ausgegeben am 24. August 2006
Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

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 gemäß § 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.
Die Zuständigkeitskonzentration beim Regierungspräsidium Darmstadt für ganz Hessen ist zum 1. März 2005 erfolgt.

Im Berichtsjahr wurden von der Aufsichtsbehörde **in 561 Fällen** Überprüfungen von nicht öffentlichen Stellen vorgenommen, die Datenverarbeitung gemäß § 28 BDSG für die Erfüllung eigener Geschäftszwecke betreiben oder personenbezogene Daten gemäß §§ 29, 30 BDSG zur personenbezogenen oder anonymisierten Übermittlung speichern und nutzen.

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

Die **561 Überprüfungen** auf Grund von Eingaben, Beschwerden und Pressemeldungen durch die Aufsichtsbehörde betrafen:

- in 91 Fällen die Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA),
- in 91 Fällen Teledienstеanbieter (Anbieter von Internetzugängen, -diensten und -inhalten, unverlangte E-Mail-Werbung),
- in 63 Fällen Banken, Kreditinstitute und EDV-Dienstleister im Zahlungsverkehr,
- in 54 Fällen Handels- und Wirtschaftsauskunfteien,
- in 41 Fällen Stellen und Unternehmen der Direktmarketing- und Werbewirtschaft,
- in 37 Fällen Versicherungsgesellschaften,
- in 33 Fällen den Datenschutz in Arbeitsverhältnissen und bei Arbeitsvermittlern,
- in 22 Fällen das Gesundheitswesen (Ärzte, Krankenhäuser, Senioren- und Pflegeheime),
- in 21 Fällen Vereine (Sport, Soziales, Kultur) sowie deren Landes- u. Bundesverbände,
- in 16 Fällen die Videoüberwachung von Grundstücken, Häusern und Wohnungen,
- in 16 Fällen Unternehmen der Freizeit-, Touristik- und Reisebranche,
- in 12 Fällen Unternehmen des Groß- und Einzelhandels,
- in 12 Fällen Inkassounternehmen,
- in 9 Fällen Unternehmen der Versandhandelsbranche,
- in 9 Fällen Vermieter sowie Wohnungs- u. Immobilienverwaltungsfirmen,
- in 7 Fällen Kreditkartenunternehmen,
- in 5 Fällen Adresshandelsunternehmen,
- in 4 Fällen Markt- u. Meinungsforschungsunternehmen,
- in 3 Fällen Auslandsdatenverarbeitung,
- in 2 Fällen Verlage und Presse,
- in 11 Fällen sonstige Stellen (z.B. Politische Partei, Privatdetektei, Insolvenzverwalter).

Bei ca. 21 % der Beschwerden konnte zeitnah festgestellt werden, dass diese begründet waren. In insgesamt **118 Fällen** wurden bei den Nachforschungen der Aufsichtsbehörde unzulässige Verarbeitungen personenbezogener Daten und andere Verstöße gegen Vorschriften des Datenschutzrechts und des Rechts der Tele- und Mediendienste festgestellt, die zu Beanstandungen bei den betroffenen Stellen führten.

Die bei den Überprüfungen beanstandeten **118 Verstöße** gegen Datenschutzbestimmungen wurden festgestellt:

- in 26 Fällen bei Anbietern von Tele- und Mediendiensten im Internet (Access- und Content-Provider und Versender von Werbe-E-Mails),
- in 19 Fällen bei der Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA), davon war in 12 Fällen ein Verstoß durch den Vertragspartner der SCHUFA ursächlich,
- in 15 Fällen bei Kreditinstituten und Banken,
- in 10 Fällen bei Unternehmen der Direktmarketing- und Werbebranche,
- in 6 Fällen bei Unternehmen der Freizeit-, Touristik- und Reisebranche,
- in 5 Fällen bei Versicherungsgesellschaften,
- in 5 Fällen bei der Verarbeitung von Arbeitnehmer- und Bewerberdaten,
- in 5 Fällen bei Inkassounternehmen,
- in 5 Fällen bei Kreditkartenunternehmen,
- in 4 Fällen im Groß- und Einzelhandel,
- in 3 Fällen bei Handels- und Wirtschaftsauskunfteien,
- in 3 Fällen im Gesundheitssektor (Arzt, Krankenhaus),
- in 3 Fällen in der Versandhandelsbranche,
- in 3 Fällen im Wohnungswesen (Vermieter),

sowie in jeweils einem Fall bei einer politischen Partei, bei der Videoüberwachung, einem Verein und im Verlags- und Medienbereich, sowie bei zwei sonstigen Stellen.

Ein Teil der eingeleiteten Überprüfungen konnte 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 **125 Fälle** abgeschlossen. Die Beurteilung dieser in der Regel nur mit hohem Ermittlungsaufwand aufklärbaren Eingaben durch das Regierungspräsidium ergab, dass davon **68 Eingaben** begründet waren. Damit musste die Aufsichtsbehörde bei **55 %** dieser Fälle einen Datenschutzverstoß feststellen.

Die beanstandeten **68 Verstöße** gegen Datenschutzbestimmungen wurden festgestellt:

- in 17 Fällen bei Unternehmen der Werbewirtschaft und werbenden Einzelhändlern,
- in 14 Fällen bei Anbietern von Telediensten (Internetprovider),
- in 7 Fällen bei Inkassounternehmen,
- in 7 Fällen bei der SCHUFA,
- in 5 Fällen bei Arbeitgebern und Arbeitsvermittlern,
- in 4 Fällen bei Vermietern, Wohnungs- und Immobilienfirmen,
- in 3 Fällen bei Banken,
- in 3 Fällen bei Versicherungsunternehmen,
- in 2 Fällen im Gesundheitswesen,
- in 2 Fällen bei der Video-Beobachtung öffentlich zugänglicher Räume,

sowie in jeweils einem Fall bei einem Versandhändler, einem Kreditkartenunternehmen, einer Anwaltskanzlei und einer sonstigen Stelle.

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

Im Berichtsjahr wurden häufig Überprüfungen vor Ort durchgeführt, die sich aus einer Eingabe eines Betroffenen über die Datenverarbeitung eines Unternehmens ergaben. Waren die Auskünfte eines Unternehmens zur Aufklärung des Sachverhalts unzulänglich oder war der Auskunft des Unternehmens zu entnehmen, dass die Vorschriften des BDSG bisher nicht ausreichend beachtet wurden, führte dies zu einer Überprüfung vor Ort. Darüber hinaus wurden auch anlassunabhängige Überprüfungen vorgenommen.

Insgesamt wurden im Berichtsjahr 35 Kontrollen durchgeführt.

Diese betrafen folgende Branchen/Bereiche:

- Videoüberwachungssysteme	15
- Ärztliche Praxen/Kliniken/Laboratorien	5
- Vereine/Verband	5
- Markt- und Meinungsforschung	4

- Handels- und Gewerbeunternehmen 3
- Konzerndatenverarbeitungsdienstleister/Rechenzentren 3

Bei allen Überprüfungen mussten Mängel festgestellt werden, wobei folgende Mängel am häufigsten festgestellt wurden:

1. Voraussetzungen des § 6b BDSG (Videoüberwachung) nicht erfüllt.
2. Fehlendes oder nicht ausreichendes Verfahrensverzeichnis, erforderliche Vorabkontrolle nicht durchgeführt, keine Möglichkeit zur Löschung von Daten in der Software.
3. Mängel in den Bereichen der Datensicherheit, z.B. fehlende oder nicht ausreichende Passworte, zu weit gehende Zugriffsrechte für einzelne Mitarbeiter, fortbestehende Zugriffsrechte ausgeschiedener Mitarbeiter, Daten auf Laptops werden unverschlüsselt gespeichert.
4. Eine Sicherung des aktuellen Datenbestandes findet überhaupt nicht statt, die externen Datenträger mit den gesicherten Daten werden auf dem Server ungeordnet gelagert.

Darüber hinaus bestanden oftmals weitere Mängel, wie sie auch in den vorangehenden Tätigkeitsberichten schon aufgezeigt wurden.

Ein Prüfungsschwerpunkt ist besonders hervorzuheben. Die Überprüfung der im Rahmen der Fußball WM 2006 erfolgten Datenverarbeitungen. Diese wird unter Nr. 16 gesondert dargestellt.

2. Bearbeitung von Anfragen zu datenschutzrechtlichen Problemstellungen und Beratungstätigkeit

2.1 Anfragebearbeitung und datenschutzrechtliche Beratung

Die Aufsichtsbehörde hatte im Berichtsjahr erneut eine hohe Anzahl von Anfragen und Beratungsersuchen zu bearbeiten. In **289 Fällen** (im Vorjahr: 199 Fälle) erfolgte die Beratung und Information von Unternehmen, Vereinen und Verbänden, Bürgerinnen und Bürgern sowie Arbeitnehmern, Arbeitnehmerinnen 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:

35 Anfragen zum Arbeitnehmerdatenschutz:
Handel mit den Daten einer Betriebskrankenkasse, Übermittlung der Daten von Auszubildenden an eine Krankenkasse, Umfang der Datenerhebung durch den Betriebsarzt, Durchführung von Drogentests (siehe unten Nr. 12.2), Ablage der Protokolle von Zielvereinbarungsgesprächen in den Personalakten und anschließende Übersendung der Akten an die Konzernzentrale in der Schweiz, Privatnutzung von Firmenhandys, Aufzeichnung der Inhalte von Telefongesprächen, private Nutzung von betrieblichen E-Mail- und Internet-Anschlüssen, Ausgestaltung von Betriebsvereinbarungen, Übermittlung von Lebensläufen aus Bewerbungsverfahren an weitere Arbeitgeber, Speicherdauer von Daten aus Online-Bewerbungen, Nutzung von Arbeitnehmeradressen zur Zusendung einer Arbeitgeberzeitschrift, Veröffentlichung von Mitarbeiterdaten (z. B. Krankheit, Geburtstag, Telefonkosten) am schwarzen Brett und im Intranet von Unternehmen, Mikroverfilmung von Personalakten, Öffnen von persönlich adressierten Briefen, Verpflichtung von Arbeitnehmern auf das Datengeheimnis gemäß § 5 BDSG.

33 Anfragen zur SCHUFA:
Grundsätzliches zur Arbeitsweise der SCHUFA und ihrer Vertragspartner (siehe unten Nr. 6.2), SCHUFA-Selbstauskunft und deren Kosten, Fragen zur Beantragung der Eigenauskunft über das WWW, Problematik des SCHUFA-Scorings (siehe unten Nr. 6.1), Fragen Betroffener zur Bedeutung und Reichweite der SCHUFA-Klausel, Unzulässigkeit der Nutzung des SCHUFA-Systems durch Nicht-Vertragspartner unter Zuhilfenahme von SCHUFA-Vertragspartnern als Vermittler, Löschfristen für SCHUFA-Einträge, Werbung mit einem nicht vorhandenen SCHUFA-Anschluss, Bezug von Auszügen aus dem Schuldnerverzeichnis durch die SCHUFA, Vor-

lage einer SCHUFA-Selbstauskunft zur Visum-Erteilung, Anforderung einer SCHUFA-Selbstauskunft vor Gewährung eines städtischen Darlehens.

29 Anfragen aus dem Gesundheitssektor:
Aufbewahrung, Digitalisierung und Archivierung von Patientenakten, datenschutzrechtliche Zuständigkeiten bei juristisch selbständigen Niederlassungen eines Klinikkonzerns, Auswertung anonymisierter Patientendaten für die medizinische Marktforschung, Übermittlung von Patientendaten an Laborunternehmen, Weitergabe von Patientendaten an Dienstleister in unsicheren Drittländern, Übermittlung von Bonitätsdaten der Patienten zwischen Ärzten, Umfang von Patienteninformationen, Einsichts- und Auskunftsrechte, Formulierung von Patienteneinwilligungen, Anforderungen an Einwilligungserklärungen der Erziehungsberechtigten bei der DNA-Diagnostik betreffend Babys, Beratung zur datenschutzgerechten, sicheren Übermittlung von sensiblen Gesundheitsdaten, Anfragen zum Datenschutz im Zusammenhang mit dem Transplantationsgesetz, Beratung zur Einrichtung eines Gesundheitsnetzes zur Verbesserung der Kommunikation zwischen Ärzten über das Internet, Beschlagnahme von Patientenunterlagen bei Ärzten, Einhaltung des Patientengeheimnisses am Empfangsschalter einer Arztpraxis, Datenschutz in Apotheken beim Schalterverkauf.

28 Anfragen von und zum betrieblichen Datenschutzbeauftragten:
Voraussetzungen der korrekten Bestellung von betrieblichen Datenschutzbeauftragten, Inkompatibilität bei der Bestellung von Führungspersonal zum Datenschutzbeauftragten, Probleme bei der Bestellung externer Datenschutzbeauftragter, Rechtsstellung eines stellvertretenden Datenschutzbeauftragten, Aufgaben des betrieblichen Datenschutzbeauftragten, Bitten um Unterstützung durch die Aufsichtsbehörde bei Schulungs- und Weiterbildungsveranstaltungen, Umfang des eigenen Schulungsanspruchs, Nachfragen nach Qualifikation und Zertifizierung von betrieblichen Datenschutzbeauftragten, Schulung der Mitarbeiter, Erstellung eines Verfahrensverzeichnisses gemäß § 4g Abs. 2 BDSG, Datenschutzbeauftragte in Arztpraxen und Privatkliniken, Rechtsstellung des betrieblichen Datenschutzbeauftragten bei Umwandlung eines Unternehmens.

28 Anfragen zum Datenschutz im Internet:
Beratung zu empfangenen Phishing-E-Mails, Anfragen zum Umgang mit unverlangten Werbe-E-Mails und zu E-Mails mit getarnten Schadprogrammen im E-Mail-Anhang (Viren, Trojaner, Würmer), Veröffentlichung von Stammbaumdaten im Internet, Nachvollziehbarkeit von Internet-Bestellungen zur Ermittlung von Straftätern, Einrichtung einer zulässigen und sicheren Online-Plattform zur Kreditvermittlung im WWW, Speicherung dynamisch vergebener IP-Nummern durch Zugangsprovider, Auskunftspflicht eines Zugangsproviders über die vergebene dynamische IP-Nummer nach § 4 Abs. 7 TDDSG bzw. § 34 Abs. 1 BDSG gegenüber dem Betroffenen, Auskunftserteilung eines Zugangsproviders an Finanz- und Strafverfolgungsbehörden, Verpflichtung von Mitarbeitern einer EDV-Abteilung auf das Fernmeldegeheimnis nach § 85 TKG, allgemeine Fragen zur Sicherheit im Internet und zur Sicherheit von E-Mail-Kommunikation, Filtern und Löschen unverlangter Werbe-E-Mails (Spam) durch Arbeitgeber, Folgen der Nutzung von temporären E-Mail-Adressen bei Neuvergabe, Veröffentlichung einer "schwarzen Liste" mit Schuldnern im WWW, zulässiger Umfang einer Datenerhebung im WWW, Formulierung von Datenschutzhinweisen in WWW-Angeboten gemäß § 4 Abs. 1 TDDSG, Beratung zu den Grenzen des zulässigen Permission-Marketing im WWW, "Double-Opt-In"-Verfahren für Online erhobene E-Mail-Adressen nach § 4 Abs. 2 TDDSG, Online-Datenschutz beim E-Learning.

21 Anfragen zur Datenverarbeitung durch Vereine und Dachverbände:
Anfragen zur Zulässigkeit der Datenverarbeitung des Deutschen Fußball-Bundes anlässlich der Fußball-WM 2006 (Ticketing, Akkreditierung, RFID-Chip etc., vgl. auch unten Nr. 16), Ausgabe einer "Vereinskarte" mit Bonuspunkten, Umgang mit Personaldaten in der Vereinsgeschäftsstelle, Veröffentlichung von Mitgliederdaten und -bildern im Internet, Übermittlung von Mitgliederdaten an einen Dachverband, Weitergabe von Mitgliederdaten innerhalb des Vereins zur Versendung der Einladung zu einer außerordentlichen Mitgliederversammlung, Automatisierung eines Verfahrens zur Vergabe von Urkunden und Abzeichen, interner Umgang mit E-Mail-Adressen von Vereinsmitgliedern.

20 Anfragen zur Datenverarbeitung im Ausland:
Fragen zur Datenübermittlung in sog. "Drittstaaten", d. h. in Staaten außerhalb der Europäischen Union und des Abkommens über den Europäischen Wirtschaftsraum, insbesondere im Zusammenhang mit dem Transfer von Arbeitnehmerdaten an außereuropäische Konzern-Muttergesellschaften, Beratung, ob die installierten Verfahren zur Sicherstellung eines angemessenen Datenschutzes bei der Übermittlung von personenbezogenen Daten an Drittländer ausreichend sind, Fragen zur Anwendung der Ausnahmevorschrift des § 4c Abs. 1 Nr. 1 BDSG, Datenübermittlung auf Grund des "Sarbanes Oxley Act", Auslagerung von Datenverarbeitungen an Datenverarbeitungsdienstleister in Drittstaaten, Ausgestaltung eines Mustervertrags über die Erbringung von IT-Dienstleistungen bei konzerninternen Aus- oder Verlagerungen von Leistungen, Fragen zur Safe-Harbor-Entscheidung (siehe unten Nr. 11.1), Fragen nach dem Erfordernis der Genehmigung durch die Datenschutzaufsichtsbehörde (vgl. auch unten Nr. 3), Fragen zu den EU-Standardvertragsklauseln (siehe unten Nr. 11.2 und 11.3).

15 Anfragen zum Datenschutz bei Banken:
konzerninterner Datenverkehr, Beratung einer Einrichtung zur Notfall-Kartensperrung, Aufdruck von Name und Kartennummer auf einer Kreditkartenabrechnung, Formulierung von Einwilligungserklärungen und Klauseln, Nutzung von Umsatzdaten zu Marketingzwecken, Sicherheitsfragen bei der Verarbeitung von Bankdaten, Beratung zum Umgang mit EC-Karte und PIN, Übermittlung von Kundendaten an eine Bausparkasse.

10 Anfragen zum Groß- und Einzelhandel:
Anfrage zur datenschutzgerechten Netzwerkadministration, Überprüfung von Bankdaten beim Online-Handel, Datenweitergabe an ein Inkassounternehmen, Nennung der Anschrift für das elektronische Lastschriftverfahren, datenschutzrechtliche Aspekte der Veröffentlichung gewerblicher Referenzkunden im WWW, personenbezogene Auswertung von Kartenzahlungen an Tankstellen, zulässige Übermittlung von Kundendaten an den gewerblichen Adresshandel, telefonische Preisgabe personenbezogener Daten an Arbeitskollegen einer Kundin (siehe unten Nr. 15.7).

8 Anfragen zur Videoüberwachung:
Fragen zur Beobachtung von öffentlichen Plätzen und Veröffentlichung im WWW (Webcams) (vgl. auch unten Nr. 14.2), Videoaufzeichnungen durch den Arbeitgeber am Arbeitsplatz (siehe unten Nr. 12.1), Videoüberwachung in Mietshäusern und Wohnungsanlagen mit vielen Betroffenen sowie in einem Behindertenwohnheim (siehe unten Nr. 14.1), Beobachtung von Straßen, Gehwegen, Grundstückszufahrten, Wohnanlagen, Hausfluren und Treppenhäusern, Video-Aufzeichnungen in Nachbarschaftsstreitigkeiten, Ausgestaltung des nach § 6b Abs. 2 BSDG erforderlichen Hinweises auf die Videobeobachtung.

8 Anfragen zu Handels- und Wirtschaftsauskunfteien:
Beratung von Handels- und Wirtschaftsauskunfteien zu datenschutzrechtlich zulässigen Verarbeitungen und Übermittlungen, Adressermittlung bei Einwohnermeldeämtern, Beratung von Betroffenen zur Arbeitsweise von Auskunfteien, Aufklärung von Bürgern über die Wahrnehmung von Datenschutzrechten (Auskunft, Löschung, Sperrung) gegenüber Auskunfteien (vgl. auch unten Nr. 7), Scoring-Verfahren bei Auskunfteien (siehe unten Nr. 6.1), Einrichtung zentraler branchenspezifischer Hinweissysteme (schwarze Listen und Warndateien, auch im Internet).

7 Anfragen zur Werbewirtschaft und zum Adresshandel:
Erhebung von Besucherdaten bei Messen zur späteren werblichen Nutzung, Einrichtung eines Kundenbindungssystems bei einem Zeitungsverlag, Beratung zum Recht auf Auskunftserteilung nach § 34 Abs. 1 BDSG, Informationen zum Werbewiderspruch gemäß § 28 Abs. 4 BDSG sowie zur Löschung bzw. Sperrung von Daten nach § 35 BDSG, Zulässigkeit des Adresshandels nach §§ 28, 29 BDSG, Unzulässigkeit des Telefonmarketings ohne Einwilligung (siehe unten Nr. 15.2 – 15.4), digitale Aufzeichnung von Gesprächen beim Telefonmarketing (voice-recording).

6 Anfragen zur Meldepflicht nach §§ 4d, 4e BDSG:
Gesetzliche Voraussetzungen für die Meldung bei der Datenschutzaufsichtsbehörde, Meldepflicht eines Adressermittlungsunternehmens, Meldepflicht ausländischer Unternehmen.

5 Anfragen zur Markt- und Meinungsforschung:
Zulässigkeit telefonischer Umfragen ohne Werbe- oder Verkaufscharakter, Bewertung von Konzepten zur Durchführung von Marktforschungsstudien, Zulässigkeit der Speicherung von Telefonnummern in einer Sperrdatei nach Widerspruch des Betroffenen nach § 28 Abs. 4 BDSG.

5 Anfragen zum Datenschutz durch Technik und zur Datensicherheit:
Datensicherheitsmaßnahmen zur Abwehr von Hackerangriffen, Nachfrage zur Möglichkeit der forensischen Analyse von sicherheitsrelevanten Vorfällen auf einzelnen Windows-PCs, Löschung von Daten auf einem defekten USB-Stick vor der Einsendung zur Reparatur.

4 Anfragen zur datenschutzgerechten Datenträgervernichtung:
Anfragen zu Rechtsgrundlagen für die datenschutzgerechte Datenträgervernichtung, Beratung zur Einhaltung der Sicherheitsstufen der DIN 32757-1, Abschluss von Dienstleistungsverträgen nach § 11 BDSG zur sicheren Entsorgung von Datenträgern.

3 Anfragen zur Versicherungsbranche:
Nachfrage nach der Zulässigkeit von Bonitätsabfragen zur Antragsprüfung, Scorewerte zur Steuerung von Marketingmaßnahmen, Unzulässigkeit der Einsichtnahme in Mitarbeiterdaten anderer Unternehmen.

3 Anfragen zum Versandhandel:
Unzulässige Versendung von Mahnungen per E-Mail ohne vorherige Information und Einwilligung, Prüfung und Beratung bei der Ausgestaltung und Formulierung der Hinweise und Unterrichtungen nach § 4 Abs. 3 BDSG und § 28 Abs. 4 BDSG im Versandhauskatalog,

2 Anfragen aus dem Bereich Miete und Wohnen:
Unzulässigkeit der Herausgabe von Daten ehemaliger Mieter an Anfrager, Installation und Betrieb einer hausbezogenen Datenbank für Betriebskosten mit anonymisierten Mieterdaten durch einen Mieterschutzverein.

Da in der modernen Informationsgesellschaft kaum noch ein Sektor existiert, in dem keine personenbezogenen Daten automatisiert verarbeitet werden, waren die weiteren Anfragen und Beratungsersuchen breit über viele Lebens- und Wirtschaftsbereiche gestreut. Sie betrafen unter anderem die Erhebung und Verarbeitung personenbezogener Daten der Besucher von Spielbanken, die Auftragsdatenverarbeitung nach § 11 BDSG, die Reise- und Touristikbranche, den Umgang mit Visitenkartendaten von Seminarbesuchern, den Umgang mit Schülerdaten in Privatschulen, die Unabhängigkeit der Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich, die zulässige Weitergabe von Daten durch Rechtsanwälte an Gerichte, die Aufzeichnung von Telefonaten in Call-Centern, die Herausgabe personenbezogener Daten an Strafverfolgungsbehörden, das Recht auf Auskunftserteilung nach § 34 Abs. 1 BSDG bzw. § 4 Abs. 7 TDDSG und die jeweiligen rechtlichen Rahmenbedingungen der Auskunft, die Erstellung eines betrieblichen Datenschutzkodex sowie die Offenlegung von Vermögensverhältnissen in Unterhaltsauseinandersetzungen.

2.2 Vorträge, Informationsmaterial und Orientierungshilfen

Das Regierungspräsidium Darmstadt hat auch im Rahmen von Informationsveranstaltungen diverser Veranstalter Fragen zum Datenschutz beantwortet und Vorträge gehalten. Auf besonderes Interesse stießen die Thematik des konzerninternen Datentransfers (siehe hierzu unter Nr. 10 des 18. Berichtes der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, LT-Drucksache 16/4752). Eine Vertreterin der Aufsichtsbehörde referierte hierzu auf Einladung der Gesellschaft für Datenschutz und Datensicherung e.V. zunächst in deren Erfahrungsaustauschkreis für Hessen und dann im Rahmen der jährlich stattfindenden Datenschutz-Fachtagung in Köln.

Auf Wunsch eines Netzwerks betrieblicher Datenschutzbeauftragter aus ganz Europa informierte eine Vertreterin des Regierungspräsidiums Darmstadt über die Aufgaben und Befugnisse der deutschen Aufsichtsbehörden sowie ebenfalls über die Zulässigkeit des konzerninternen Datentransfers. Da viele internationale Konzerne eine Niederlassung im Rhein-Main-Gebiet haben, sind solche Informationsveranstaltungen für beide Seiten hilfreich.

Bereits im vergangenen Jahr hat sich die Aufsichtsbehörde eingehend mit der RFID-Technik beschäftigt, die bei der Fußball-Weltmeisterschaft 2006 zum Einsatz kommen soll (siehe hierzu ausführlich unter Nr. 11.1.3 des 18. Berichtes der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, LT-Drucksache 16/4752, zur WM 2006 vgl. auch unten Nr. 16). Über diese neue Technik sind häufig keine oder nur unzureichende Kenntnisse vorhanden oder es bestehen falsche Vorstellungen.
Die Aufsichtsbehörde nutzte daher gerne die Gelegenheit, im Rahmen des von der Hessischen Landesregierung veranstalteten eGovernment-Forums sowie auf Einladung des Landeskriminalamtes Wiesbaden hierüber zu informieren.

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

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

3. Genehmigungsverfahren nach § 4c Abs. 2 BDSG

Im Berichtsjahr gingen drei Anträge auf Genehmigung des Datentransfers in die USA und andere außereuropäische Staaten ein.

In einem Fall wurde zunächst ein bereits im Jahr 2004 gestellter Antrag betreffend den Transfer von Mitarbeiterdaten an einen US-Dienstleister zurückgezogen und nach Überarbeitung durch einen neuen Antrag ersetzt. Dem waren intensive Beratungen durch die Aufsichtsbehörde und eingehende Erörterungen innerhalb des Konzerns vorausgegangen. Einige Detailpunkte veranlassten die Aufsichtsbehörde noch zu Rückfragen; es ist jedoch davon auszugehen, dass die Genehmigung nun in 2006 erteilt werden kann, sobald die erbetene Stellungnahme vorliegt.

In einem weiteren Fall beantragte die Bevollmächtigte der deutschen Tochtergesellschaften eines US-Konzerns die Genehmigung, Mitarbeiterdaten an die Muttergesellschaft in den USA zu übermitteln und legte hierfür einen Vertrag vor, der wörtlich dem EU-Standardvertrag vom Juni 2001 entsprach, aber eine marginale Ergänzung enthielt. Nach Abstimmung mit den Aufsichtsbehörden in Baden-Württemberg und Bayern, wo sich die anderen Tochtergesellschaften befinden, teilte das Regierungspräsidium Darmstadt der Bevollmächtigten mit, dass hierfür keine Genehmigung erforderlich sei. (Zur Frage der Genehmigungsfreiheit bei Verwendung der EU-Standardvertragsklauseln siehe unter Nr. 7.2 des 15. Berichtes der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, LT-Drucksache 15/4659.) Die Angelegenheit hatte angesichts der Komplexität der Datenverarbeitungen und vor allem der Konzernstrukturen, die beim Ausfüllen der Anhänge zum Standardvertrag zutreffend abzubilden sind, gleichwohl umfangreiche Beratungen und Abstimmungen erfordert. Ferner waren hierbei Fragen zur Datenweiterübermittlung in den USA zu klären.

Im dritten Fall beantragte eine Bank die Genehmigung für den Transfer von Kundendaten an einen konzernangehörigen Dienstleister in Indien. Betroffen waren nur Firmenkunden, bei denen es sich fast ausschließlich um juristische Personen handelte. Personenbezogene Daten waren also nur zu einem geringen Teil umfasst. Die Bank legte eine Datenschutzvereinbarung ("Data Protection Memorandum") mit dem Dienstleister in Indien vor. Dieser Vereinbarung war als Anlage der EU-Standardvertrag vom Dezember 2001 in wörtlicher Fassung beigefügt. Es stellte sich daher die Frage, ob überhaupt

eine Genehmigungspflicht besteht. Allerdings hieß es in der vorangehenden Datenschutzvereinbarung: "Die Standardvertragsklauseln werden *mit folgenden Änderungen* in diese Vereinbarung einbezogen."
Es folgten beispielsweise Begriffsbestimmungen, die sich auf die konkrete Situation im Konzern bezogen. Überwiegend schien es sich - wie vom Unternehmen auch bestätigt wurde - nur um Vorgaben zur praktischen Umsetzung der EU-Standardvertragsklauseln im Konzern zu handeln.

Das Regierungspräsidium Darmstadt verdeutlichte dem Unternehmen, dass dann aber klargestellt werden müsste, dass die EU-Standardvertragsklauseln inhaltlich unberührt bleiben sollen. Die Genehmigungspflicht kann nur entfallen, wenn bei einem Rechtsstreit letztlich die Interpretation der EU-Standardvertragsklauseln durch die Gerichte maßgeblich ist. Insoweit muss von vornherein klargestellt sein, was letztendlich gewollt ist.

Auf Grund dieser Hinweise hat das Unternehmen die Datenverarbeitung überarbeitet und darin vorsorglich klar gestellt, dass im Falle von Unstimmigkeiten/Widersprüchen zwischen den konkreten Umsetzungsvorgaben im Memorandum selbst und den als Anhang beigefügten EU-Standardvertragsklauseln auf jeden Fall die Regelungen des EU-Standardvertrages Vorrang haben.

Auf diese Weise wurde also eine Lösung gefunden, die auch anderen Unternehmen empfohlen werden kann. Sie trägt dem Interesse der Unternehmen Rechnung, die doch recht abstrakten Regelungen der EU-Standardvertragsklauseln durch konkrete, auf die Situation im Konzern zugeschnittene Regelungen "mit Leben zu erfüllen" und nutzt zugleich die Vorteile der EU-Standardvertragsklauseln (unbürokratisch, da genehmigungsfrei).

4. Register der meldepflichtigen Verfahren nach § 4d BDSG

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

Am Ende des Berichtsjahres waren 88 Verfahren von 83 verantwortlichen Stellen im Melderegister eingetragen. Wie sich aus diesen Zahlen ergibt, haben nur drei verantwortliche Stellen mehr als ein Verfahren gemeldet.

Davon werden in 40 gemeldeten Verfahren geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung gespeichert (Adresshändler, Handels- und Wirtschaftsauskunfteien, meldepflichtig nach § 4d Abs. 4 Nr. 1 BDSG). 48 der eingetragenen Verfahren dienen dem Zwecke der anonymisierten Übermittlung (Markt- und Meinungsforschung, meldepflichtig nach § 4d Abs. 4 Nr. 2 BDSG).

5. Ordnungswidrigkeitenverfahren

Im Berichtsjahr wurden vom Regierungspräsidium Darmstadt acht Verfahren nach dem Ordnungswidrigkeitengesetz (OWiG) eingeleitet, wie sich aus nachfolgender Übersicht ergibt:

nach § 43	Grund der Einleitung	Rechtskraft	Bußgeld
Abs. 1 Nr. 10 BDSG	Nichterteilung von Auskünften	Nein	500 €
Abs. 2 Nr. 1 BDSG	unbefugte Verarbeitung	Ja	750 €
Abs. 2 Nr. 1 BDSG	unbefugte Verarbeitung	Ja	750 €
Abs. 2 Nr. 1 BDSG	unbefugte Verarbeitung	Ja	750 €
Abs. 2 Nr. 1 BDSG	unbefugte Verarbeitung	Ja	1.500 €
Abs. 2 Nr. 1 u. 3 BDSG	unbefugte Verarbeitung	eingestellt	
Abs. 2 Nr. 3 BDSG	unbefugtes Abrufen	Ja	300 €
Abs. 2 Nr. 3 BDSG	unbefugtes Abrufen	Ja	300 €

Erfreulicherweise zeigten sich die in aufsichtsrechtliche Verfahren einbezogenen Personen gegenüber der Behörde in der Mehrzahl kooperativ, so dass es - mit einer Ausnahme - im Jahr 2005 nicht erforderlich wurde, Auskunftsansprüche über Bußgeldverfahren durchzusetzen. In diesem einen Fall war ein Klinikleiter bzw. dessen Rechtsanwalt trotz mehrfacher Aufforderung nicht zu einer Stellungnahme zu bewegen, was letztlich zu einem Verfahren nach §§ 43 Abs. 1 Nr. 10, 38 Abs. 3 Satz 1 BDSG führte.

Dagegen mussten in vier Ordnungswidrigkeitenverfahren Missstände bei der Verarbeitung von Patientendaten in Arztpraxen geahndet werden, auf die Bürgerinnen und Bürger aufmerksam gemacht hatten.

In einem Fall teilte ein anonymer Anrufer mit, dass in einem gelben Sack vor einer Arztpraxis neben Einwegspritzen und Praxisabfällen auch Schriftstücke mit personenbezogenen Daten erkennbar seien. Bei einer unangemeldeten Prüfung vor Ort fanden Behördenvertreter in den Abfallcontainern der Praxis zahlreiche Rezepte, Befunde, Protokolle und weitere Unterlagen über Patienten, die entweder gar nicht oder nur grob auseinander gerissen waren. Die dafür verantwortlichen Personen erklärten dazu, dass Schriftgut mit personenbezogenen Daten grundsätzlich gesammelt und im Shredder unkenntlich gemacht werde und es sich bei dem beanstandeten Sachverhalt um ein Einzelvorkommnis handele.

Bei einem ähnlich gelagerten Sachverhalt hatte die Polizei eine blaue Papiertonne einer Arztpraxis beschlagnahmt, nachdem eine Bürgerin darin eine große Menge ärztlicher Unterlagen vorgefunden hatte. Bei den Papieren handelte es sich um etwa 650 große, mit Namen und Geburtsdatum versehene Briefumschläge, die EEG-Untersuchungsergebnisse in teilweise kommentierter Form enthielten. Auch in diesem Fall machte der Praxisinhaber geltend, dass zu entsorgende Patientenunterlagen normalerweise geshreddert würden und hier ein Versehen des Praxispersonals vorliege.

Da es in beiden Fällen Außenstehenden möglich wurde, durch einen Blick in den für jedermann frei zugänglichen Altpapierbehälter Kenntnis von teilweise sensiblen Patientendaten zu erlangen, war jeweils der Tatbestand des § 43 Abs. 2 Nr. 1 BDSG verwirklicht. Für das unberechtigte Übermitteln personenbezogener Daten an eine unbekannte Anzahl dritter Personen wurden daher Bußgelder in Höhe von 1.500,00 € verhängt.

Anlass für ein weiteres Verfahren gab eine Fachärztin, die sich mit persönlich adressiertem Schreiben bei ihren Patienten als neue Praxisinhaberin vorstellte. Dabei teilte sie mit, dass sie die Patientenkartei von der Vorinhaberin übernommen habe und nun auf alle aktuellen Befunde zugreifen könne. Eine Patientin wendete sich darauf hin an die Aufsichtsbehörde, weil sie in eine Überlassung ihrer Behandlungsdaten nicht eingewilligt habe und sich dadurch in ihren Persönlichkeitsrechten verletzt fühle. Ermittlungen zum Sachverhalt ergaben, dass die Vorinhaberin der Praxis in einem Übernahmevertrag eine klare Regelung zur Übergabe der manuell geführten Patientenkartei getroffen hatte. Demnach wurden die Unterlagen nur zur Aufbewahrung überlassen und eine Nutzung der Karteikarten sei nur nach schriftlicher Zustimmung des Patienten zulässig. Vor Ort wurde überdies festgestellt, dass die Patientenkartei in den Räumlichkeiten einer Rechtsanwaltskanzlei "zwischengelagert" wurde und damit auch für dort beschäftigte Personen die Möglichkeit der Einsichtnahme bestand. Dies wurde von der Aufsichtsbehörde – in Verbindung mit der Nutzung und Speicherung der Daten zur Versendung der Infobriefe - als unbefugtes Verarbeiten personenbezogener Daten bewertet und mit einer Geldbuße in Höhe von 750,00 € geahndet.

Zwei Ordnungswidrigkeitenverfahren mit einer Bußgeldsumme in Höhe von 600,00 € wurden gegen einen Mitarbeiter eines Kreditinstitutes durchgeführt, der SCHUFA-Anfragen für private Zwecke getätigt hatte. Einer davon betroffenen Person war dies anhand einer SCHUFA-Selbstauskunft aufgefallen, auf der sich ein Vermerk über die Anfrage der Bank befand. Es stellte sich heraus, dass der Beschuldigte in zwei Fällen Erkundungen zu den Mietern im elterlichen Wohnhaus eingeholt hatte. Die Vorgehensweise war als unbefugtes Abrufen nicht allgemein zugänglicher Daten nach § 43 Abs. 2 Nr. 3 BDSG zu ahnden.

Ein weiteres Verfahren betraf die Mitarbeiterin einer Versicherung, die im Zusammenhang mit ihrem Scheidungsverfahren einige Versicherungsdaten des Ehemannes abgefragt und an das Familiengericht weitergeleitet hatte. Im Anhörungsverfahren konnte die Beschuldigte glaubhaft darlegen, dass die versicherten Sachen gemeinsam beschafft worden waren und Kenntnis darüber auch ohne die abgefragten Daten bestanden hätte. Der Vorfall wurde zwar gleichwohl aus datenschutzrechtlicher Sicht beanstandet, das Bußgeldverfahren aber im Rahmen der pflichtgemäßen Ermessensausübung nach § 47 Abs. 1 OWiG eingestellt.

Ausgesuchte Probleme und Einzelfälle

6. Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA)

6.1 Scoring-Verfahren

Im Jahr 2005 gingen zahlreiche telefonische und schriftliche Anfragen und Beschwerden zur Berechnung des SCHUFA-Scorewerts ein.

Exemplarisch für die Vielzahl der Beschwerden werden zwei Fälle heraus gegriffen:

Ein Betroffener beschwerte sich darüber, dass sein Scorewert mit 40 von 1000 Scorepunkten extrem schlecht war. Er gab an, dass ihm im Laufe des Jahres 2005 drei Barkreditanfragen von jeweils unterschiedlichen Banken abgelehnt worden seien, obgleich er in ungekündigter Stellung und mit einem sehr hohen, frei verfügbaren Einkommen ausgestattet sei und keinerlei Negativeinträge habe. Da er als Akademiker mit beratender Tätigkeit in der Vergangenheit seinen Wohnort häufiger habe wechseln müssen, seien bei der SCHUFA 8 Adressen gespeichert.

Die SCHUFA hatte seine Anfrage, aus welchen Gründen er so schlecht eingestuft worden sei, mit einem merkblattartigen Schreiben beantwortet, das lediglich allgemeine Ausführungen zum Scoreverfahren enthielt. Sie verwies darauf, dass die Ablehnungen wegen der Vertragsfreiheit der Kreditgeber und der Prüfung der Kreditsachbearbeiter nicht auf den SCHUFA-Scorewert zurück zu führen seien und der Betroffene im übrigen doch noch einen Kredit bei einer anderen Bank bekommen habe.
Es wurden keine auf den konkreten Fall bezogenen Auskünfte erteilt, aus welchen Gründen der konkrete Scorewert so schlecht ausgefallen war, vielmehr berief sich die SCHUFA hinsichtlich der Wertigkeiten in den Score-Berechnungen auf das Geschäftsgeheimnis.

In einem anderen Fall übersandte ein Betroffener der Aufsichtsbehörde seine Korrespondenz mit der SCHUFA, die sich um die wiederholte Berechnung seiner Scorewerte und deren drastischer Veränderung innerhalb von zwei Jahren drehte. Wenngleich die Entwicklung zum Positiven erfolgt war, verlangte er eine Erklärung.

Der Betroffene hatte sich im September 2004 seine Scorewerte für alle Sparten berechnen lassen. Dabei wurden hohe Risikoquoten ausgewiesen, d.h. der Beschwerdeführer wurde in schlechte Ratingstufen einordnet. Kurz zuvor hatte der Betroffene auch eine Selbstauskunft eingeholt, in der verschiedene Kreditverträge, Kreditanfragen und eine Anfrage wegen Dienstleistung enthalten waren. Dem Betroffenen war durch die Diskussion in der Öffentlichkeit bekannt, dass mehrere Kreditanfragen bei der Berechnung des Scorewerts problematisch sein könnten.
Seine Beschwerde bei der SCHUFA führte zu einer allgemeinen Erläuterung des Scoring-Verfahrens sowie dem Hinweis, dass der Scorewert allein keine hinreichende Grundlage für eine Kreditentscheidung sei. Nicht beantwortet wurde jedoch die Frage, aus welchen Gründen die Werte im konkreten Fall des Betroffenen so schlecht ausgefallen waren.

Die nächsten Scorewerte, die sich der Betroffene im November 2004 errechnen ließ, wiesen eine starke Verbesserung bis zu drei Ratingstufen auf, obgleich die parallel eingeholte Selbstauskunft keine Verringerung der Kreditbelastungen zeigte, sondern vielmehr zwei neue Kreditanfragen und eine weitere Anfrage "Dienstleistung" hinzu gekommen waren.

Eine dritte Scoreberechnung im September 2005 ergab schließlich eine noch deutlichere Verbesserung der Ratingstufen, eine davon sogar Ratingstufe A, eine andere Stufe B, obgleich in der Selbstauskunft vier neue Kreditanfragen, eine Leasinganfrage und zwei neue Kreditkarten eingetragen waren.

Die Leasinganfrage stellte sich später als fehlerhaft heraus, weil sie einem Leasinggeschäft galt, das mit einer Aktiengesellschaft geschlossen werden sollte, bei dem der Betroffene Geschäftsführer (Vorstandsvorsitzender) war. Nachdem die fehlerhafte Leasinganfrage gelöscht worden war, übersandte die SCHUFA dem Betroffenen im Februar 2006 eine neue Berechnung des Scorewerts, die noch viel besser ausfiel, so dass alle Ratingstufen hervorra-

gend waren. Die drastisch positiven Veränderungen der Scorewerte des Betroffenen waren nicht ohne weiteres zu erklären.

Der Beschwerdeführer vermutete, dass dies mit dem Wegfall der oben genannten zwei Anfragen zu einer Dienstleistung zusammen hängen müsse, die nach Ablauf der Jahresfrist inzwischen automatisch gelöscht waren und somit bei den späteren Scoreberechnungen nicht mehr einflossen. Diese Anfragen waren von einem Anbieter von Gentests gestellt worden, dessen wesentliches Geschäftsfeld die Durchführung von Abstammungsgutachten ist.
Der Betroffene vermutete, dass Kunden dieses Unternehmens hauptsächlich Väter seien, die einen Vaterschaftstest durchführen ließen, um sich aus finanziellen Gründen ihren Unterhaltspflichten zu entziehen, und dass er in diese Kategorie eingeordnet worden sei.
Da diese Klientel zu einem hohen Anteil finanziell schwach sei, jedoch im Verhältnis zur Gesamtbevölkerung eine relativ kleine Vergleichsgruppe darstelle, seien die daraus gewonnenen statistischen Aussagen nicht aussagekräftig.

Für die Aufsichtsbehörde ist neu, dass offensichtlich auch Dienstleister dieser Art Vertragspartner der SCHUFA sind. Sollte sich die Vermutung des Betroffenen bestätigen, würde dies wohl bedeuten, dass beim SCHUFA-Scoring der Geschäftsgegenstand bzw. der einmeldende Vertragspartner einfließen und gewichtet werden. Die Aufsichtsbehörde befindet sich diesbezüglich in der Prüfung.

Sowohl den geschilderten Fällen als auch nahezu allen anderen Eingaben ist gemeinsam, dass die Betroffenen mehr Transparenz bzgl. des Scoring-Verfahrens fordern. Sie wollen vor allem wissen, warum ihre Scorewerte schlecht sind oder waren.

Für den SCHUFA-Score ist zwar bekannt, dass im Grundsatz alle im Auskunftsdatenbestand gespeicherten Daten für die Scoreberechnung verwendet werden (können), so dass sich die Datenbasis prinzipiell aus der Eigenauskunft ersehen lässt, die jeder Betroffene einholen kann (siehe hierzu unter Nr. 6.1 des 17. Berichtes der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, LT-Drucksache 16/3650).

Allerdings gibt dies noch keine klare Vorstellung, inwieweit und wie die Daten tatsächlich für die Scoreberechnung nach den verschiedenen Scorekarten verwendet werden und welche Daten letztlich maßgeblich waren für einen schlechten Scorewert. Die Betroffenen können derzeit, wie die Beispielsfälle zeigen, nur spekulieren.

Die Aufsichtsbehörde forderte die SCHUFA immer wieder auf, das Verfahren transparenter zu machen, so dass die Betroffenen die Möglichkeit haben, die durch den Scorewert ausgedrückte Risikoprognose durch Darlegung ihrer individuellen Situation, ggfs. verbunden mit weiteren Nachweisen für ihre Bonität, zu entkräften.
Die SCHUFA lehnte dies mit der Begründung ab, dass die Bewertung (Auswahl und Gewichtung) der von den Betroffenen vorhandenen Daten im Rahmen des Scoring-Verfahrens ihr Geschäftsgeheimnis sei.

Die Beschwerdeführer beklagten auch, dass sie von den potentiellen Kreditgebern bzw. Vertragspartnern nicht offen darüber informiert würden, dass ihre Entscheidung auch auf einem enthaltenen Scorewert beruhte. Ferner trugen die Beschwerdeführer z.T. vor, sie seien eher durch Zufall und zumeist durch die Medien auf mögliche Zusammenhänge der Scorewertberechnung aufmerksam geworden und hätten einen zuvor ablehnenden Kreditgeber nur durch ihre Eigeninitiative doch noch von ihrer guten Bonität überzeugen können.

Die Aufsichtsbehörde hält ergänzende gesetzliche Verpflichtungen der Scoreentwickler und -nutzer zur Schaffung größerer Transparenz für erforderlich, damit die Interessen der Scorenutzer und die Interessen der Betroffenen in ein ausgewogenes Verhältnis zueinander gelangen.

Es wäre denkbar, die Pflichten aus § 6a Abs. 2 Nr. 2 BDSG, geeignete Maßnahmen zur Wahrung der berechtigten Interessen der Betroffenen zu

ergreifen, sowie die ggfs. zu präzisierende Auskunftspflicht aus § 6a Abs. 3 BDSG auf Entscheidungen auszudehnen, bei deren Zustandekommen ein Scorewert in nicht unerheblichem Maße berücksichtigt wurde. Bisher gilt die Vorschrift nur für Entscheidungen, die *ausschließlich* auf einen Scorewert gestützt werden.

Die Aufsichtsbehörde begrüßt es daher, dass sich die Bundesregierung in ihrem angekündigten Bericht über die Auskunfteien u.a. mit Fragen des Scorings befassen will. Bemerkenswert und erfreulich ist, dass im Rahmen einer Plenardebatte im Deutschen Bundestag alle Redner Handlungsbedarf gesehen und sich für eine gemeinsame Initiative ausgesprochen haben (Plenardebatte am 9. März 2006, Bundestagsdrucksache 16/022, S. 1733-1740).

Neben der Frage der Transparenz ist für das Scoring-Verfahren auch maßgeblich, welche Faktoren überhaupt einfließen dürfen.

Problematisch ist insoweit beispielsweise die Verwendung des Merkmals "AK" (=Anfrage Kredit). Dieses Merkmal wird bei einer SCHUFA-Anfrage eines Kreditinstitutes gespeichert und für 10 Tage beauskunftet, um zu verhindern, dass ein Kunde mehrere Kredite gleichzeitig erhält, die kumulativ seine Zahlungsfähigkeit übersteigen. Anschließend bleibt es für ein Jahr zu Dokumentations- und Kontrollzwecken (Überprüfung der Rechtmäßigkeit der Anfrage) gespeichert und wird dem Betroffenen in der Selbstauskunft mitgeteilt. Während des gesamten Zeitraumes wird das Merkmal jedoch für die Scoreberechnung verwendet (je nach Scorekarte).

In der Arbeitsgruppe Auskunfteien des Düsseldorfer Kreises bestand Einvernehmen zwischen den Aufsichtsbehörden, dass dies jedenfalls ab dem 11. Tag im Hinblick auf den Rechtsgedanken des § 31 BDSG nicht gerechtfertigt sei. Die SCHUFA widersprach dem jedoch und versucht möglicherweise, der Kritik auch durch eine Änderung der SCHUFA-Klauseln zu begegnen.

Die Verwendung der Anzahl der Kreditanfragen für das Scoring kann u.U. dazu führen, dass sich ein verbraucherpolitisch erwünschtes Verhalten (Einholung mehrerer konkreter Vergleichsangebote) negativ auf den Score auswirkt und ist auch insoweit kritisch zu sehen.

Auch mit Blick auf die Frage der zulässigen Faktoren ist es daher sehr zu begrüßen, dass sich die Bundesregierung und der Bundestag mit der Scoringproblematik befassen.

6.2 Erweiterung des Kreises der Vertragspartner

Die SCHUFA ist bestrebt, den Kreis ihrer Vertragspartner immer weiter auszudehnen. Bereits unter Nr. 6.4 des Siebzehnten Berichtes der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden (Drs. 16/3650) wurde über die kritische Bewertung der Datenschutzaufsichtsbehörden in der Arbeitsgruppe "Auskunfteien/SCHUFA" berichtet.

Die SCHUFA hat jedoch große gewerbliche Vermieter bereits als B-Vertragspartner angeschlossen, ohne irgendwelche Beschränkungen, wie sie vom Hessischen Ministerium des Innen und für Sport als Co-Vorsitzendem der Arbeitsgruppe gegenüber der SCHUFA gefordert wurden, vorzunehmen.

Auch Versicherungsunternehmen bietet die SCHUFA - trotz der Kritik der Aufsichtsbehörde - in weitaus größerem Umfang als bisher an, SCHUFA-Vertragspartner zu werden. Bislang haben die Aufsichtsbehörden den Anschluss von Versicherungsunternehmen nur akzeptiert, soweit ein echtes kreditorisches Risiko der Versicherung besteht (grundpfandrechtlich gesicherte Kreditanträge bei Versicherungsgesellschaften, Deckungszusage bei Kfz-Haftpflichtversicherungen).

Die SCHUFA versucht einen weitergehenden Datenaustausch mit der Versicherungswirtschaft ua. mit dem Argument zu rechtfertigen, dass es einen Zusammenhang zwischen der Bonität eines Kunden und dem Versicherungsrisiko gäbe. Den Versicherungen soll die Möglichkeit gegeben werden, die Höhe einer Versicherungsprämie nach der Bonität zu berechnen oder einen

Versicherungsvertrag ganz abzulehnen, sofern kein Kontrahierungszwang besteht.

Nach Auffassung der Aufsichtsbehörden handelt es sich hierbei nicht um ein kreditorisches Risiko im eigentlichen Sinne, es geht vielmehr um die Absicherung des wirtschaftlichen Risikos, dass ein Versicherungskunde den Versicherungsschutz tatsächlich in Anspruch nimmt. Der behauptete statistische Zusammenhang ist jedoch für die Aufsichtsbehörden nicht nachvollziehbar. Die SCHUFA verweist zum Beleg auf ein von ihr in Auftrag gegebenes Gutachten, dass den Aufsichtsbehörden jedoch nicht vorliegt.

Darüber hinaus haben die Aufsichtsbehörden aber vor allem bekräftigt, dass die Übermittlung von Bonitätsdaten, die nur mittelbar und allenfalls nach statistischen Erkenntnissen relevant sind, die schutzwürdigen Interessen der Betroffenen verletzt. Auch die von der SCHUFA und der Versicherungswirtschaft vorgetragenen weiteren Argumente konnten die Aufsichtsbehörden nicht überzeugen. Insgesamt ist dabei zu berücksichtigen, dass die Versicherungswirtschaft bereits jetzt über einen umfangreichen Datenbestand und gute Möglichkeiten zur Risikoabwägung infolge der branchenspezifischen Warn- und Hinweissysteme verfügt. Dies wurde dem Gesamtverband der Deutschen Versicherungswirtschaft daher auch in der Arbeitsgruppe "Versicherungswirtschaft" des Düsseldorfer Kreises entgegengehalten (siehe auch 20. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten, Nr. 20.4).

Die dargestellte Problematik die Wohnungs- und Versicherungswirtschaft betreffend beschränkt es sich nicht auf die SCHUFA. Auch andere Auskunfteien übermitteln Daten an diese Branchen, zum Teil schon länger als die SCHUFA. Angesichts des sehr großen Datenbestands der SCHUFA und des insbesondere bei der Kreditvergabe im privaten Bereich sehr großen Kreises von Vertragspartnern, die die SCHUFA-Auskunft erhalten, ist die Problematik bei dieser besonders bedeutsam.

Die SCHUFA lässt nach Auffassung der Aufsichtsbehörden die Tendenz erkennen, Bonitätsauskünfte bei wirtschaftlichen Risiken jedweder Art und aus jeglichen Branchen, über Verbraucher, Selbständige, sowie Kleingewerbetreibende erteilen zu wollen. Eine entsprechende Änderung des in der SCHUFA-Klausel enthaltenen Hinweises auf die Kategorien von Empfängern hat die SCHUFA bereits geplant. Eine derartige Ausweitung des Beauskunftungssystems könnte dazu führen, dass jegliches Handeln im Wirtschaftsleben in immer mehr Lebensbereichen nur noch nach einer erfolgreichen Bonitätsabfrage möglich würde.

Nach Auffassung der Aufsichtsbehörde wäre dies nicht gerechtfertigt. Auch von daher ist es zu begrüßen, dass sich die Bundesregierung und der Bundestag mit der Auskunftssysthematik befassen, wobei dies insbesondere in Bezug auf die generalklauselartigen Abwägungstatbeständen des BDSG und den begrenzten Befugnissen der Aufsichtsbehörden gilt.

6.3 Probleme mit SCHUFA-Vertragspartnern

Ein Dauerthema bei der Aufsicht über die Datenverarbeitung der SCHUFA sind fehlerhafte Eintragungen, die im Rahmen des Massengeschäfts durch Vertragspartner der Auskunftei verursacht werden. Diese reichen vom unberechtigten Einmelden, über das Unterlassen von Einmeldungen bis hin zu fehlerhaften Einmeldungen mit teilweise erheblichen finanziellen Folgen für die Betroffenen.

Die Aufsichtsbehörde legt großen Wert darauf, dass die konkreten Ursachen bei den Vertragspartnern im Detail aufgeklärt werden und die betroffenen Vertragspartner wirksame Maßnahmen ergreifen, damit sich Fehler nicht beständig wiederholen.

Die SCHUFA selbst hat der Aufsichtsbehörde bei Besuchen dargelegt, dass sie diese Problematik fortlaufend im Rahmen ihres Qualitätsmanagements angeht.

6.4 Vertraulichkeit in den SCHUFA-Geschäftsstellen

Einige Bürger beklagten sich bei der Aufsichtsbehörde, dass in den SCHUFA-Geschäftsstellen keine Vertraulichkeit gewährleistet sei. Als sie in

einer Geschäftsstelle von ihrem Recht Gebrauch machten, eine kostenlose mündliche Selbstauskunft einzuholen (§ 34 Abs. 6 Satz 1 BDSG), hätten andere Auskunftssuchende das Gespräch mit der SCHUFA-Mitarbeiterin mithören können.

Bei der Besichtigung der Geschäftsstelle Frankfurt konnte die Aufsichtsbehörde feststellen, dass der Wartebereich erfreulicherweise vom Auskunftsbereich (Schalterbereich) durch eine Glaswand und -tür getrennt und akustisch abgeschirmt ist. Im Schalterbereich befinden sich aber mehrere Auskunftsplätze, so dass bei der Einholung einer Selbstauskunft die Gespräche zumindest an dem benachbarten Auskunftsplatz mitgehört werden können.

Im Wartebereich war ein Hinweisschild angebracht, auf dem u.a. folgendes stand: "Die Auskunftsplätze sind offen und Gespräche können von Anwesenden mitgehört werden. Sofern Sie dieses vermeiden möchten, richten Sie Ihr Auskunftsersuchen bitte schriftlich an die SCHUFA."

Auch andere Aufsichtsbehörden im Bundesgebiet haben sich auf Grund von Beschwerden mit der Thematik befasst und z.T. Prüfungen vorgenommen, bei der die gleichen Feststellungen getroffen wurden.

Daher wurde die Angelegenheit im Düsseldorfer Kreis behandelt, wo zwischen den Datenschutzaufsichtsbehörden im Bundesgebiet Einigkeit darüber bestand, dass die SCHUFA die Möglichkeit schaffen muss, Betroffenen eine kostenlose mündliche Selbstauskunft zu erteilen, ohne dass Dritte zuhören können.

Auskunftssuchende dürfen nicht durch mangelnde Vertraulichkeit abgeschreckt und auf die entgeltpflichtige schriftliche Auskunftserteilung verwiesen werden, denn dadurch würde die Verpflichtung des § 34 Abs. 6 Satz 1 BDSG unterlaufen werden.

Die SCHUFA hatte dem zunächst widersprochen. Nach intensiven Diskussionen berichtete sie jedoch, sie habe den Geschäftsstellen Arbeitsanweisungen gegeben, welche die Vertraulichkeit bei Einholung einer Selbstauskunft gewährleisteten. Die entsprechende Änderung der Hinweisschilder in den Geschäftsstellen sei in Auftrag gegeben.

Künftig werde wie folgt vorgegangen:

- Der Betroffene wird zunächst gefragt, ob er die Aushändigung der kostenpflichtigen schriftlichen Selbstauskunft oder nur die kostenlose Einsichtsnahme wünscht.
- Wenn der Betroffene die kostenlose Einsichtnahme wünscht, wird ihm der Ausdruck der Selbstauskunft zum Lesen vorgelegt. Bei Beendigung der Einsichtnahme hat er den Ausdruck an die SCHUFA zurück zu geben. Alternativ besteht die Möglichkeit, dass der Betroffene Gelegenheit erhält, die Daten selbst auf dem Bildschirm zu lesen.
- Zum besseren Verständnis der Auskunft erhält der Betroffene ggf. Informationsmaterial der SCHUFA, das er auch nach Beendigung der Einsichtnahme behalten kann.
- Wenn der Betroffene ein Gespräch wünscht, z. B. weil er Fragen hat oder Erläuterungen benötigt, erhält er die Möglichkeit, das Gespräch trotz eingeschränkter Vertraulichkeit im Aufsichtsraum sofort zu führen, er erhält jedoch zuvor den Hinweis, seine Einwendungen schriftlich vortragen zu können oder das Gespräch erst fortzusetzen, wenn sich keine anderen Auskunftssuchenden mehr im Raum befinden. Bis zur Beendigung des Gesprächs werden dann keine anderen Auskunftssuchenden eingelassen.

Die Aufsichtsbehörden akzeptierten schließlich dieses von der SCHUFA dargestellte Verfahren, da der Betroffene durch Aushändigung eines Ausdrucks der Selbstauskunft zumindest die nach § 34 Abs. 6 Satz 1 BDSG vorgesehene Möglichkeit zur kostenlosen Einsicht in seine Daten erhält, ohne bei diesem eigentlichen Auskunftsvorgang gesondert Vertraulichkeit verlangen zu müssen.

7. Auskunfteien

Auskünfte über Herkunft und Empfänger von Daten an Betroffene

Die in § 33 Abs. 1 BDSG vorgeschriebene Benachrichtigung der Betroffenen durch Auskunfteien führte auch im vergangenen Jahr zu einer erheblichen Zunahme von Anfragen Betroffener, die von ihrem Auskunftsrecht nach § 34 BDSG Gebrauch machten und hierbei von den Auskunfteien, welche die personenbezogenen Daten für geschäftsmäßige Zwecke an Dritte übermittelt hatten, Auskunft über die konkreten Empfänger der Daten sowie die Datenherkunft verlangten. In vielen Fällen behaupteten und beanstandeten die Betroffenen eine unzureichende Beauskunftung.

Das nach § 34 Abs. 1 Satz 1 BDSG bestehende Auskunftsrecht des Betroffenen bezieht sich im Hinblick auf die Herkunft der personenbezogenen Daten zunächst nur auf gespeicherte Daten. Die Pflicht zur Beauskunftung umfasst neben den zu der Person gespeicherten Daten und dem Zweck der Speicherung auch das Recht auf Information über die Empfänger oder Kategorien der Empfänger seiner Daten, sowie den Zweck der Speicherung. Bei Auskunfteien, welche personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung speichern, ist eine Speicherung der Herkunft nicht Voraussetzung für eine Beauskunftung der Anfragenden über die Datenherkunft (§ 34 Abs. 1 Satz 4 BDSG, hieraus ist also ggfs. eine entsprechende Dokumentationspflicht für die Auskunfteien ableitbar). Demnach kann der Betroffene nach § 34 Abs. 1 Satz 3 und 4 BDSG Auskunft über Herkunft und Empfänger verlangen, sofern nicht das Interesse der Auskunftei und der verantwortlichen Stelle an der Wahrung des Geschäftsgeheimnisses überwiegen sollte.

Nach einhelliger Meinung der Datenschutzaufsichtsbehörden im Bundesgebiet sind auf entsprechende Auskunftsersuchen daher die Datenherkunft und Datenempfänger im Regelfall zu beauskunften. Nur das Bestehen besonderer Umstände rechtfertigt eine Auskunftsverweigerung.

Bezüglich der Erteilung einer Auskunft zu den Datenempfängern besteht bereits seit längerem Einvernehmen zwischen den Aufsichtsbehörden, dass generell in folgenden, bestimmten Fallgruppen diese Auskunft zu erteilen ist:

- Sofern der Betroffene begründete Zweifel an der Richtigkeit der Daten vorträgt.
- Bei Vortrag des Betroffenen, wonach er Schadenersatz- oder Richtigstellungsansprüche geltend machen möchte, da einzelne Daten unzutreffend seien.
- Bei Angabe des Betroffenen, wonach der Auskunftsempfänger den Auskunftsdatensatz in unberechtigter Weise an Dritte weitergegeben bzw. den Datensatz in der Weise missbräuchlich verwendet habe.
- Sofern der Betroffene vorträgt, dass der Auskunftsempfänger unter keinen Umständen ein berechtigtes Interesse an der Auskunft gehabt haben könne.
- Darüber hinaus generell bei folgenden Branchen:
  - Kreditversicherungen / Versicherungen,
  - Versandhandel,
  - Telekommunikation,
  - Banken,
  - Leasing-/Factoringgesellschaften,
  - Konzerngesellschaften

In den übrigen Fällen muss eine Prüfung im Einzelfall stattfinden. Dies wurde dem Verband der Handelsauskunfteien bereits im Jahre 2004 entsprechend schriftlich mitgeteilt.

Auch bzgl. der Datenherkunft kann nichts anderes gelten, wie durch Urteil des AG Altona (Az.:317 C 328/04) bestätigt wurde.

Sollte bei der Abwägung der Interessen des Betroffenen gegen die Interessen der Auskunftei auf Wahrung des Geschäftsgeheimnisses, das letztere Interesse überwiegen, sind die Ablehnungsgründe und das vorgebrachte Geschäftsgeheimnis im Einzelfall der Aufsichtsbehörde unter Vorlage entsprechender Belege darzulegen.

Im konkreten Fall informierte die Aufsichtsbehörde die Auskunftei über die Rechtsauffassung. Seitens der Auskunftei wurde zugesagt, künftig eine entsprechende und umfassende Beauskunftung der Betroffenen vorzunehmen.

8. Inkassounternehmen

8.1 Datenverarbeitungshinweis und Fragebogen als Anlagen zum Inkasso-Mahnschreiben

Unter Nr. 8 des Siebzehnten Berichtes der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden (Drs. 16/3650) wurde von zahlreichen Beschwerden gegen den Datenverarbeitungshinweis und den Fragebogen eines Inkassounternehmens berichtet, die zusammen mit einem Mahnschreiben an die Schuldner versandt wurden.
Die Aufsichtsbehörde hatte den Datenverarbeitungshinweis als irreführend kritisiert, weil nicht klar war, unter welchen Voraussetzungen die erfragten Daten an welche Empfänger übermittelt werden.
Nach intensiver Auseinandersetzung über die einzelnen Formulierungen hat das Inkassounternehmen nun die Forderungen der Aufsichtsbehörde umgesetzt und den Datenverarbeitungshinweis so verfasst, dass für die Betroffenen erkennbar wird, dass ihre Daten nur unternehmensintern verwendet bzw. an die benannten Auskunfteien übermittelt werden, wenn eine Forderung ohne substantiierte Einwände nicht beglichen wird.

Der Fragebogen des Inkassounternehmens soll die Abwicklung von Inkassoaufträgen beschleunigen, indem der Schuldner selbst detaillierte Angaben zu seinen eigenen finanziellen Verhältnissen und z.T. auch denen des Ehepartners macht sowie Vorschläge und Erklärungen zur Begleichung der Schulden abgibt (Ratenzahlung, Anerkenntniserklärung, Einzugsermächtigung, Abtretungserklärung).
Nach umfangreichen Auseinandersetzungen gestaltete das Inkassounternehmen seinen Fragebogen an die Adressaten des Mahnschreibens entsprechend den Forderungen der Aufsichtsbehörde so um, dass die Freiwilligkeit der Angaben erkennbar wurde und Daten Dritter nur wirksam mit deren Einwilligung erhoben werden können.
Im Detail wurde der Fragebogen so verändert, dass je nach dem konkreten Sachverhalt nur die Angaben abgefragt werden, die auch im Schuldnerinteresse der Fortführung bzw. Beendigung des Inkassoverfahrens dienen. Wurde die Forderung bereits bezahlt oder besteht sie nach Ansicht des Adressaten gegen ihn nicht, kann er dies nunmehr einfach ankreuzen, ohne weitere Angaben machen zu müssen.
Das Inkassounternehmen bittet dann lediglich um einen Zahlungsnachweis bzw. eine Begründung, warum die Forderung nicht bestehen soll.

8.2 Vollautomatisierte Mahnanrufe

Die Aufsichtsbehörde erlangte von einem Amtsgericht Kenntnis davon, dass ein Inkassounternehmen zur Beitreibung von Forderungen Anrufautomaten einsetzte.
Inkassounternehmen bedürfen einer Zulassung durch das Amtsgericht, in dessen Bezirk sie ihren Sitz haben. Im konkreten Fall befasste sich das Amtsgericht auf Grund der Beschwerde eines betroffenen Bürgers mit der Frage, ob die vollautomatisierten Mahnanrufe rechtmäßig sind und bat die Aufsichtsbehörde um Stellungnahme.

Der Sachverhalt stellte sich wie folgt dar:

Bei Entgegennahme des Anrufs unter der (vermeintlichen) Telefonnummer des Schuldners teilte eine Computerstimme dem Gesprächspartner mit, dass das Inkassounternehmen sich nunmehr melde, weil auf eine zuvor zugesandte Inkassomahnung noch nicht bezahlt worden sei. Mit dem Anruf werde letztmalig die Gelegenheit gegeben, den Betrag der offenen Forderung innerhalb der nächsten 7 Tage zu überweisen.

Das Inkassounternehmen berief sich darauf, dass der vom Anrufautomaten übermittelte Text weder nötigend noch beleidigend sei und nicht darauf abziele, den Schuldner in der Öffentlichkeit verächtlich zu machen. Dass "versehentlich" Dritte den Anruf entgegen nehmen könnten, führe ebenfalls nicht zu einem Eingriff in das allgemeine Persönlichkeitsrecht des Schuld-

ners, denn es müsse bei einer Zahlungsaufforderung nicht stets und unbedingt ausgeschlossen werden, dass Dritte davon Kenntnis erlangten. Soweit "versehentlich" Familienmitglieder, Hausangestellte, Arbeitskollegen oder sonstige Personen den Anruf entgegen nähmen und dadurch von der Existenz der Forderung erfahren könnten, sei dies vergleichbar mit dem Klingeln des Gerichtvollziehers an der Tür. Auch dabei könne nicht ausgeschlossen werden, dass Dritte von einer Forderung erfahren und dennoch sei dies kein Eingriff in das Persönlichkeitsrecht des Schuldners. Des Weiteren sei auch der Versand von Mahn-SMS an die Mobiltelefonnummer des Schuldners in der Branche üblich. Der Schuldner müsse im Zweifelsfall selbst dafür sorgen, dass Dritte keine Anrufe entgegennähmen, die nicht für sie bestimmt sind.
Selbst wenn man jedoch einen Eingriff in das Persönlichkeitsrecht unterstellen würde, müsse dieser hinter die kollidierenden Grundrechte des Rechts auf freie Berufsausübung, als Interesse des Inkassounternehmens an automatisierten, rationalisierten Arbeitsgängen, und das Recht auf Eigentum, als Recht des Gläubigers zur Durchsetzung seiner vermögensrechtlichen Forderungen, zurücktreten.

Die Aufsichtsbehörde hielt diesen Standpunkt für nicht vertretbar, weil er die Anforderungen des BDSG vollständig außer Acht ließ. Mangels Einwilligung des Schuldners in die Übermittlung der Mahndaten an Dritte kam als möglicher Erlaubnistatbestand nur § 28 BDSG in Betracht.Zwar erkannte die Aufsichtsbehörde an, dass das Interesse des Inkassounternehmens, offene Forderungen anzumahnen und dabei Kosten sparend zu verfahren, grundsätzlich berechtigt ist.
Insoweit war die Geeignetheit nicht zu bestreiten, denn ein vollautomatisierter Mahnanruf erspart den Einsatz von Personal und dürfte in einer Reihe von Fällen wohl auch zu dem gewünschten Zahlungserfolg führen.
Allerdings wurde die Erforderlichkeit des vollautomatisierten Mahnanrufs angezweifelt, da die Information des Schuldners eben auch, wie bei anderen Inkassounternehmen, mit Personalbeteiligung stattfinden konnte; das Informationsziel also auch anders erreicht werden konnte (vgl. Simitis, Kommentar zum BDSG, 5. Auflage 2003, § 28 Rdnr.143). Der Einsatz von Personal konnte daher nicht von vornherein als unzumutbar angesehen werden.

Unabhängig davon bestand Grund zu der Annahme, dass jedenfalls die schutzwürdigen Interessen der Betroffenen am Ausschluss der Nutzung ihrer Daten zu vollautomatisierten Mahnanrufen überwogen.

Die Art und Weise der Datennutzung setzte die Betroffenen der nicht mehr akzeptablen Folge (vgl. Simitis aaO Rdnr.163) aus, dass über ihre Telefonnummern Dritte von den vollautomatisierten Mahnanrufen Kenntnis nehmen konnten. In der Abwägung des Interesses des Inkassounternehmens an einem günstigen Mahnverfahren mit dem Interesse der Betroffenen an der Nichtweitergabe personenbezogener Informationen an unbeteiligte Dritte war nicht zu akzeptieren, dass es dem Zufall überlassen wurde, ob an einem bestimmten Telefonanschluss der dort erreichbare Betroffene tatsächlich erreicht wurde oder ein Dritter den Anruf zur Kenntnis nahm.

Der Inhalt des Mahnanrufs bewirkte gegenüber dritten Gesprächsempfängern eine Deklaration des Betroffenen als säumigen Schuldner. Selbst wenn eine Forderung unbestritten bestand, wäre diese Deklaration nach Ansicht der Aufsichtsbehörde unangemessen, weil das Mahnanliegen nur die am Inkassoverfahren Beteiligten etwas angeht und dem Betroffenen das Recht nimmt, im Rahmen der Gesetze selbst darüber zu entscheiden, ob und wer diese personenbezogenen Informationen zur Kenntnis bekommt.

Noch viel mehr gilt dies, wenn der Betroffene berechtigte Einwände gegen die Forderung oder Teile derselben hat.

Entgegen der These des Inkassounternehmens ist die Situation eines vollautomatisierten Mahnanrufs schon deshalb nicht mit dem Klingeln des Gerichtsvollziehers an der Tür vergleichbar, weil der Gerichtsvollzieher titulierte, also öffentlich festgestellte Forderungen vollstrecken soll, während den Mahnanrufen im Regelfall nur Forderungen zu Grunde liegen, deren Bestand nicht rechtsverbindlich geklärt ist.

Der Bundesverband Deutscher Inkasso-Unternehmen e.V. hat in einer Stellungnahme zu dem zu Grunde liegenden Beschwerdefall Mahnanrufe per

Anrufautomat bzw. Inkassomahnungen per Postkarte als "unseriös" bezeichnet.
Er hat ebenfalls darauf hingewiesen, dass die anzusprechende Person als Schuldner identifiziert werden muss. Erfreulicherweise bestand also volle Übereinstimmung zwischen dem Verband und der Aufsichtsbehörde. Auch das zuständige Amtsgericht machte sich die Auffassung der Aufsichtsbehörde und des Verbands zu Eigen und hielt diese dem Inkassounternehmen entgegen.

Das betroffene Inkassounternehmen hat die vollautomatisierten Mahnanrufe daraufhin eingestellt.

Anders wäre die Situation wohl zu beurteilen, wenn lediglich der Verbindungsaufbau des Telefongesprächs automatisiert erfolgt, danach ein Mitarbeiter des Inkassounternehmens die Identität des Gesprächspartners abklärt und erst nach Feststellung des richtigen Mahnadressaten das Mahnanliegen kommuniziert wird.

9. Banken

9.1 Personalausweiskopien

Die Geschäftsbeziehung zu einer Bank besteht in der Regel über Jahre hinweg und gestaltet sich vielschichtig. Es werden zur Abwicklung des Zahlungsverkehrs und der Geldanlage diverse Konten eingerichtet und die entsprechenden Verträge geschlossen, Kredit- und auch Wertpapiergeschäfte abgewickelt. Oftmals wird schon bei Geburt des Kindes ein Sparkonto eröffnet, später bei Beginn der Berufsausbildung des Minderjährigen ist für diesen ein Girokonto einzurichten.

Verwundert waren hier einige langjährige Bankkunden als ihre Hausbank erstmals eine Identitätsprüfung vornahm, hierzu die Vorlage des Personalausweises erbat und eine Kopie davon anfertigte. Die Erklärungen der Bankmitarbeiter stellten die Kunden nicht zufrieden, weshalb sie sich bei der Aufsichtsbehörde nach der Rechtmäßigkeit erkundigten.

Diese Problematik beschäftigte die Aufsichtsbehörde bereits kurz nach Inkrafttreten des Gesetzes über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz) vom 25.10.1993 (siehe unter Nr. 13 des Achten Berichtes der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden (Drs. 14/299) und Nr. 5.7 des Dreizehnten Berichtes der Landesregierung (Drs. 15/1539). Im Gegensatz zu den früher zu beurteilenden Eingaben ist die Fertigung einer Kopie des Personalausweises nun eindeutig nach § 4 Abs. 1 BDSG zulässig.

Durch das Gesetz zur Verbesserung der Bekämpfung der Geldwäsche und der Bekämpfung der Finanzierung des Terrorismus (Geldwäschebekämpfungsgesetz) vom 8. August 2002 wurde die Identifizierungspflicht strenger gefasst. Nach § 2 Abs. 1 des Geldwäschegesetzes (GwG) hat ein Kreditinstitut bei Abschluss eines Vertrages zur Begründung einer auf Dauer angelegten Geschäftsbeziehung den Vertragspartner zu identifizieren. Dies ist das "Feststellen des Namens auf Grund eines gültigen Personalausweises oder Reisepasses sowie des Geburtsdatums, des Geburtsortes, der Staatsangehörigkeit und der Anschrift, soweit sie darin enthalten sind, und das Feststellen von Art, Nummer und ausstellender Behörde eines amtlichen Ausweises" (§ 1 Abs. 5 GwG). Diese Feststellungen sind durch Aufzeichnung der dort genannten Angaben oder durch Anfertigung einer Kopie der Seiten des zur Feststellung der Identität vorgelegten Ausweises, die diese Angaben enthalten, aufzuzeichnen (§ 9 Abs. 1 Satz 1 GwG). Diese beiden Alternativen stehen gleichberechtigt nebeneinander, eine Prioritätensetzung ist durch den Gesetzgeber nicht erfolgt. Die nach sachlichen Kriterien getroffene Entscheidung der Bank, geradewegs Ausweiskopien anzufertigen, ist nicht zu beanstanden.

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat in ihrer Verlautbarung vom 8. November 1999 klargestellt, dass die Identifizierungspflicht auch für Kreditkonten und sog. Unterkonten gilt. Die Verwendung der Aufzeichnungen nach § 9 Abs. 1 GwG darf nur zur Verfolgung

einer Straftat nach § 261 StGB und der in dieser Rechtsnorm aufgelisteten Straftaten erfolgen.

Mit einer ausführlichen Erläuterung der gesetzlichen Grundlagen, auf denen die Prüfung der Banken beruht, konnten den Petenten die Hintergründe dargestellt werden. Den Banken wurde empfohlen, den Mitarbeitern im Kundenbereich die Rechtslage ausführlich darzulegen. Durch umfassende Information der Kunden können die aufgetretenen Irritationen verhindert werden.

9.2 Beleglose Überweisung

Ein Fall aus dem Bankenbereich zeigt, dass die Unterrichtung des Betroffenen auch dann sinnvoll sein kann, wenn das BDSG dies nicht verlangt.

Ein Bankkunde beschwerte sich darüber, dass er anlässlich einer Überweisung aufgefordert wurde, auf einem elektronischen Signatur-Pad zu unterschreiben, ohne ihn vorher über die Speicherung der Unterschrift und den Zweck der Speicherung zu informieren.

Die Bank schilderte der Aufsichtsbehörde die Abwicklung eines Zahlungsauftrages wie folgt: Die vom Kunden auf einem Formular in Papierform ausgefüllten Zahlungsdaten werden von einem Mitarbeiter der Bank in das elektronische Zahlungssystem eingegeben. Das handschriftlich ausgefüllte Überweisungsformular wird vernichtet. Nach Überprüfung der Richtigkeit der erfassten Daten durch den Kunden erfolgt die elektronische Einholung der handgeschriebenen Unterschrift über ein Signatur-Pad. Die so geleistete Unterschrift wird untrennbar mit dem Auftragsdokument verbunden, d. h. sie kann nicht mehr für andere Geschäftsvorgänge herangezogen und damit auch nicht missbräuchlich verwendet werden. Aus Sicht der Aufsichtsbehörde ist das angewandte Verfahren zur elektronischen Speicherung der Unterschrift nicht zu beanstanden.

Auf die nach § 4 Abs. 3 Nr. 2 BDSG vorgeschriebene Unterrichtung des Betroffenen kann bei einem Überweisungsauftrag zwar verzichtet werden, weil die erhobenen Daten (hier die Unterschrift) ausschließlich der Vertragsabwicklung dienen und der Betroffene von dem Zweck zwangsläufig Kenntnis hat. Dennoch war dem Kunden in vorliegendem Fall offensichtlich nicht bewusst, was mit seiner Unterschrift geschieht. Deshalb wäre aus Gründen der Transparenz eine vorherige Information wünschenswert gewesen, da die Erfassung der Unterschrift in elektronischer Form noch nicht der allgemeinen Praxis entspricht.

Die Einschaltung der Aufsichtsbehörde wurde von der Bank zum Anlass genommen, die Mitarbeiter auf das relativ neue Abwicklungsverfahren nochmals im Detail hinzuweisen, um den Kunden künftig entsprechende Auskünfte erteilen zu können.

10. Gesundheitswesen

10.1 Mahnungen im Wartezimmer

Ein Bürger beschwerte sich anonym darüber, dass im Wartezimmer eines Tierarztes Rechnungsmahnungen säumiger "Patienten" ausgehängt würden.
Daneben sei ein Hinweis angebracht, dass man die Tiere nicht mehr auf Rechnung behandeln werde, sondern nach der Behandlung unverzüglich eine Entrichtung der Behandlungskosten durch die Tierbesitzer in bar zu erfolgen habe.

Auf die Anhörung des Tierarztes durch die Aufsichtsbehörde reagierte dieser ungehalten. Er war der Auffassung, dass die ärztliche Schweigepflicht und der Patientendatenschutz lediglich in Bezug auf die Tiere Geltung hätten und beides durch die Aushänge der Rechnungsmahnungen der Tierbesitzer nicht tangiert sei.

Im Übrigen seien die Praxisräume nicht für jedermann zugänglich, sondern das Wartezimmer würde lediglich von den Besitzern seiner Patienten besucht.

Der Einwand des Tierarztes, der Patientendatenschutz gelte lediglich im Bezug auf die behandelten Tiere, geht fehl.

Er wurde darüber unterrichtet, dass die ärztliche Schweigepflicht nach § 203 Abs. 1 Nr. 1 Strafgesetzbuch (StGB) auch für Tierärzte gilt, d.h. auch die persönlichen Daten der Tierbesitzer dem Patientengeheimnis unterfallen und nicht ohne Einwilligung des Patienten (hier des Tierbesitzers) offenbart werden dürfen. Tierärzte wurden in die Regelung des § 203 Abs. 1 Nr. 1 StGB unter anderem aufgenommen, weil gewisse Krankheiten vom Tier auf den Menschen und umgekehrt übertragbar sind und der Tierarzt oft neben oder sogar vor dem Humanmediziner von entsprechenden Erkrankungen bei Menschen erfährt. Datenschutz und ärztliche Schweigepflicht sind eng miteinander verknüpft, weil sie gleichermaßen den Schutz informationeller Selbstbestimmung bezwecken.

Deshalb hätten neben der Entbindung des behandelnden Tierarztes von der ärztlichen Schweigepflicht, die jeweiligen Tierbesitzer in die Aushängung der sie betreffenden Mahnungen schriftlich einwilligen müssen, da es sich dabei um eine Übermittlung von Patientendaten an eine unbekannte Anzahl unbefugter dritter Personen handelte. Die wirksame Einwilligung würde voraussetzen, dass der Betroffene vorab über den Zweck der Aushängung und die Folgen der Verweigerung der Zahlung informiert würde und damit entscheiden könnte, ob er unter diesen Bedingungen eine Behandlung seines Tieres durchführen lassen will.

Der Tierarzt wurde darüber aufgeklärt, dass er andere Möglichkeiten, z.B. einen eindeutigen Hinweis auf Barentrichtung der Behandlungskosten durch sein Praxispersonal vor Beginn der Behandlung oder Vorkasse, zu ergreifen und es aus den beschriebenen Gründen zukünftig zu unterlassen habe, die Rechnungsmahnungen in dem für alle Tierbesitzer zugänglichen Wartezimmer auszuhängen.

10.2 Weitergabe von Patientendaten an Verrechnungsstellen

Zahlreiche Ärzte sind dazu übergegangen, ärztliche Leistungen gegenüber ihren Patienten nicht mehr selbst abzurechnen, sondern damit eine private Verrechnungsstelle zu beauftragen.
Grundsätzlich gilt, dass ein Arzt ein ihm anvertrautes Patientengeheimnis offenbart, wenn Patientendaten den Bereich seiner Praxis verlassen. Erfolgt die Einziehung des Honorars nicht durch den behandelnden Arzt, sondern übernimmt dies eine externe Verrechnungsstelle, ist eine weit reichende Offenbarung von Patientendaten gegenüber der Verrechnungsstelle unumgänglich. Nach § 4a Abs. 3 BDSG muss bei der Verarbeitung besonderer Arten von personenbezogener Daten (§ 3 Abs. 9 BDSG), zu den u.a. Daten über die Gesundheit gehören, der Betroffene eine Einwilligungserklärung abgeben, die sich ausdrücklich auf diese Daten bezieht.

Die Weitergabe von Patientendaten an eine private Verrechnungsstelle ist nach § 4 BDSG also stets unbefugt, wenn sie ohne schriftliche Einwilligung des Patienten bzw. ohne sonstigen Rechtfertigungsgrund erfolgt.

Dies gilt ebenso für den Fall, dass der behandelnde Arzt einen Laborarzt beauftragt und dieser wiederum auch über private Verrechnungsstellen abrechnet.

Die im Berichtsjahr der Aufsichtsbehörde zugegangenen Beschwerdefälle haben gezeigt, dass vielen Ärzten diese rechtlichen Anforderungen teilweise unbekannt sind.

Um die Ärzteschaft bezüglich der datenschutzrechtlichen Regelungen insgesamt zu sensibilisieren, nahm das Regierungspräsidium Darmstadt Kontakt mit der Landesärztekammer auf. Diese kündigte an, entsprechende Hinweise in den internen Mitteilungsorganen zu veröffentlichen.

11. Aspekte internationaler Datenverarbeitungen

11.1 Safe Harbor

In den USA sind keine umfassenden bzw. ausreichenden Datenschutzgesetze vorhanden, so dass grundsätzlich kein angemessenes Datenschutzniveau besteht (vgl. oben Ziff. 3).

Durch die Entscheidung der EU-Kommission vom 26. Juli 2000 ist jedoch anerkannt und festgestellt, dass gleichwohl vom Vorhandensein eines angemessenen Datenschutzniveaus auszugehen ist, wenn sich das datenempfangende Unternehmen in den USA verpflichtet hat, die "Grundsätze des sicheren Hafens zum Datenschutz" zu beachten (sog. Safe-Harbor-Entscheidung, im Internet abrufbar unter: http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_de.htm)

Ein im Rhein-Main-Gebiet ansässiges Unternehmen beabsichtigte, ein Safe-Harbor-zertifiziertes Unternehmen in den USA mit Datenverarbeitungsdienstleistungen (Datenverarbeitung im US-Rechenzentrum) zu beauftragen. Das Unternehmen bat die Aufsichtsbehörde um Auskunft, ob weitere datenschutzrechtliche Anforderungen zu beachten sind, insbesondere, ob weitere vertragliche Regelungen zum Datenschutz erforderlich sind (EU-Standardvertrag vom Dezember 2001 und/oder Vertrag nach § 11 BDSG?).

Das Regierungspräsidium Darmstadt gab hierzu folgende Hinweise:

Grundsätzlich muss bei der Prüfung der Zulässigkeit der Datenübermittlung zwischen der ersten Stufe (Zulässigkeit nach den allgemeinen Vorschriften, insbesondere § 28 BDSG) und der zweiten Stufe (besondere Anforderungen bzgl. des Drittstaatentransfers nach §§ 4b, 4c BDSG) unterschieden werden (vgl. hierzu unter Nr. 7.4 des Fünfzehnten Berichtes der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Drs. 15/4659).

Durch die Safe-Harbor-Zertifizierung des Auftragnehmers wird nur den Voraussetzungen des § 4b BDSG Rechnung getragen. Zusätzlich muss geprüft werden, ob die Übermittlung den Anforderungen des § 28 BDSG genügt, insbesondere ob die Voraussetzungen des § 28 Abs. 1, Satz 1 Nr. 2 BDSG erfüllt sind. Wenn der US-Dienstleister beispielsweise günstiger ist oder wenn er die Dienstleistung besser erbringt als ein Dienstleister in Europa, wird man davon ausgehen können, dass ein berechtigtes Interesse für die Übermittlung besteht. Zusätzlich ist zu prüfen, ob die schutzwürdigen Belange der Betroffenen entgegenstehen. Dies erfordert jedenfalls, dass vertragliche Regelungen getroffen werden, damit sichergestellt ist, dass der US-Dienstleister die Daten nur genau zu dem Zweck und in der Weise verarbeitet, wie das Unternehmen in Deutschland es vorgibt. Folglich müssen entsprechende vertragliche Regelungen getroffen und konkrete Weisungen gegeben werden. Letztlich sind daher vertragliche Regelungen erforderlich, die dem Mustervertrag gemäß § 11 BDSG angelehnt sind, obwohl an sich eine Übermittlung vorliegt (§ 3 Abs. 8 BDSG).

Wenn statt der Safe-Harbor-Zertifizierung der EU-Standardvertrag vom Dez. 2001 geschlossen würde, müsste zwar auch § 28 Abs. 1, Satz 1 Nr. 2 BDSG geprüft werden. Aber der Abschluss eines weiteren Vertrages entsprechend dem Mustervertrag nach § 11 BDSG würde sich erübrigen, weil der Standardvertrag vom Dezember 2001 dem "deutschen" Mustervertrag nach § 11 BDSG nachgebildet ist und jedenfalls dessen wesentliche Regelungen (Weisungsgebundenheit des Dienstleisters etc.) bereits enthält. Die Weisungen wären freilich zu konkretisieren (z.B. im Dienstleistungsvertrag).

Der EU-Standardvertrag vom Dezember 2001 muss hingegen nicht abgeschlossen werden, wenn der US-Dienstleister bereits Safe-Harbor-zertifiziert ist, denn diese beiden Möglichkeiten (EU-Standardvertrag, Safe-Harbor-Zertifizierung) stehen alternativ zur Verfügung, um die besonderen Anforderungen für den Drittstaatentransfer nach §§ 4b, 4c BDSG zu erfüllen.

Das anfragende Unternehmen war in diesem Punkt auf Grund einer völlig missverständlichen Formulierung in der Antwort zu FAQ 10 der Safe-Harbor-Grundsätze (ebenfalls unter der o.g. WWW-Adresse abrufbar) verständlicherweise sehr irritiert.

Die Safe-Harbor-Entscheidung der EU-Kommission bezieht sich und basiert auf den vom US-Handelsministerium am 21. Juli 2000 vorgelegten Grundsätzen des sicheren Hafens zum Datenschutz und den diesbezüglichen Erläuterungen in Form von Antworten auf häufig gestellte Fragen (FAQs).

FAQ 10 bezieht sich auf Artikel 17 der Datenschutzrichtlinie und behandelt daher die "Datenverarbeitung im Auftrag".

FAQ 10 lautet:
"Wenn Daten aus der EU in den USA im Auftrag verarbeitet werden sollen, muss dafür ein Vertrag geschlossen werden, unabhängig davon, ob der Auftragsverarbeiter der Vereinbarung zum sicheren Hafen beigetreten ist oder nicht?"

Im ersten Absatz der Antwort wird hierzu folgendes ausgeführt:

"Ja. Werden Daten lediglich zur Verarbeitung im Auftrag übermittelt, muss der in Europa für die Verarbeitung Verantwortliche darüber stets einen Vertrag schließen, gleich ob die Verarbeitung in oder außerhalb der EU stattfindet. Der Vertrag soll die Interessen des für die Verarbeitung Verantwortlichen schützen, also der natürlichen oder juristischen Person, die Mittel und Zweck der Verarbeitung bestimmt und die gegenüber der (den) betroffenen Person(en) voll verantwortlich bleibt. Im Vertrag wird festgehalten, welche Arbeiten genau auszuführen sind und mit welchen Vorkehrungen für die Sicherheit der Daten zu sorgen ist."

Dieser Teil der Antwort besagt also nur, dass selbstverständlich ein Dienstleistungsvertrag zu schließen ist, in dem der Gegenstand der Datenverarbeitungsdienstleistung zu konkretisieren ist. Ferner korrespondiert dieser Teil der Antwort zu FAQ 10 mit den obigen Ausführungen, wonach Regelungen zu treffen sind, die dem Mustervertrag zu § 11 BDSG angelehnt sind.

Im dritten (und letzten) Absatz der Antwort zu FAQ wird ausgeführt, dass der Drittstaatentransfer keiner Genehmigung bedarf, wenn der Auftragsverarbeiter im Drittstaat sich den Safe-Harbor-Regelungen unterworfen hat. Dies ist gerade die Kernaussage der Safe-Harbor-Entscheidung der EU-Kommission.

Äußerst missverständlich ist aber der zweite Absatz der Antwort zu FAQ 10, der wie folgt lautet:
"Eine amerikanische Organisation, die der Vereinbarung zum "sicheren Hafen" beigetreten ist und personenbezogene Daten aus der EU zur Verarbeitung im Auftrag übermittelt bekommt, braucht bei diesen Daten die Grundsätze nicht anzuwenden, denn die Verantwortung dafür gegenüber der betroffenen Person liegt nach den geltenden EU-Rechtsvorschriften (die strenger sein können als die Grundsätze des "sicheren Hafens") weiterhin bei dem für die Verarbeitung Verantwortlichen."

Wären die Safe-Harbor-Grundsätze überhaupt nicht anwendbar, würde durch die Safe-Harbor-Zertifizierung kein angemessenes Datenschutzniveau geschaffen, der zweite Absatz der Antwort zu FAQ 10 stünde somit im Widerspruch zum dritten Absatz der Antwort zu FAQ 10.

Die Aussage, dass auf die im Rahmen einer "Auftragsdatenverarbeitung" erhaltenen Daten die Safe-Harbor-Grundsätze nicht anwendbar seien, ist allerdings insoweit zutreffend, als die Grundsätze nicht völlig auf diesen Fall passen. Die Grundsätze regeln die Frage, unter welchen Voraussetzungen der Datenempfänger im Drittstaat die Daten zu Werbezwecken nutzen darf (opt-out). Dies passt hier selbstverständlich nicht, denn der US-Dienstleister darf hier von vornherein keine eigenen Nutzungsrechte haben. Auch der Safe-Harbor-Grundsatz über die Informationspflichten des Datenempfängers passt nicht, denn Informationspflichten hat nach § 4 Abs. 3 oder § 33 BDSG nur der Auftraggeber (Datenexporteur).
Aber andere Bestandteile der Safe-Harbor-Grundsätze, u.a. der Safe-Harbor-Grundsatz über die Datensicherheit, müssen anwendbar sein, konkretisiert durch genaue vertragliche Vorgaben des Datenexporteurs.

Das Regierungspräsidium Darmstadt vertrat daher die Auffassung, dass der zweite Absatz der Antwort zu FAQ 10 in diesem Sinne einschränkend auszulegen ist. Soweit in dem zwischen dem EU-Datenexporteur und dem US-Datenimporteur zu schließenden Vertrag abweichende bzw. strengere Regelungen im Hinblick auf den besonderen Charakter der "Auftragsverarbeitung" zu treffen sind, gehen diese insoweit den Safe-Harbor-Grundsätzen vor.

Wegen der grundsätzlichen Bedeutung hat das Regierungspräsidium Darmstadt diese Problematik in die Arbeitsgruppe "Internationaler Datenverkehr"

des Düsseldorfer Kreises eingebracht, wo sich die Mitglieder der Interpretation des Regierungspräsidiums Darmstadt anschlossen. Zugleich wurde beschlossen, das Thema in die Art. 29-Gruppe einzubringen.

Im konkreten Fall bat das Unternehmen auch um datenschutzrechtliche Beratung zur Einschaltung eines "Subauftragnehmers" in den USA.

Hierzu gab das Regierungspräsidium Darmstadt folgende Empfehlung:

Wenn der US-Dienstleister einen Subunternehmer in den USA oder einem anderen Drittstaat einschalten will, müsste der deutsche Auftraggeber vertraglich, in dem an den Mustervertrag an § 11 BDSG angelehnten Vertrag, (siehe oben) regeln, dass dies nur mit der Zustimmung des Datenexporteurs zulässig ist. Zusätzlich dürften die Anforderungen von Satz 2 des Safe-Harbor-Grundsatzes zur Datenweitergabe gelten. Vorsorglich sollte der deutsche Auftraggeber in der vertraglichen Regelung ausdrücklich diese Anforderungen regeln, also dass der Subunternehmer entweder selbst Safe-Harbor-zertifiziert sein muss oder sich in einem Land mit angemessenem Datenschutzniveau befindet. Wenn diese Voraussetzungen nicht erfüllt sind, sollte der deutsche Auftraggeber die Zustimmung zur Einschaltung eines Subunternehmers nur erteilen, wenn der Subunternehmer bereit ist, mit dem Auftragnehmer den Standardvertrag vom Dezember 2001 zu schließen.

11.2 Verwendung der EU-Standardvertragsklauseln bei Datentransfer von/an unselbständige/r Niederlassung

Will ein in Deutschland ansässiges Unternehmen personenbezogene Daten an eine in einem Drittstaat befindliche unselbständige Zweigstelle desselben Unternehmens personenbezogene Daten weitergeben, liegt zwar keine "Übermittlung" i.S.d. § 3 Abs. 4 Nr. 3 BDSG vor, gleichwohl finden die besonderen Anforderungen der §§ 4b, 4c BDSG Anwendung (siehe hierzu ausführlich unter Nr. 7.1 des Fünfzehnten Berichtes der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Drs. 15/4659).

Gleiches muss für den spiegelbildlichen Fall gelten, wenn von einer unselbständigen Zweigstelle in Deutschland personenbezogene Daten an das in einem Drittstaat ansässige Unternehmen, dem die Zweigstelle zugehört, weitergegeben werden.

Das Regierungspräsidium Darmstadt hat mehrfach Anfragen von betrieblichen Datenschutzbeauftragten erhalten, wie denn in solchen Fallkonstellationen die Anforderungen der §§ 4b, 4c BDSG konkret erfüllt werden könnten.

Insbesondere wurde die Frage gestellt, ob auch in solchen Fällen die EU-Standardvertragsklauseln verwendet werden können. Der Abschluss eines EU-Standardvertrags mit einer unselbständigen Zweigstelle wurde verständlicherweise als problematisch angesehen, da ein Vertragsschluss dann ein unzulässiges In-sich-Geschäft darstellen würde.

Die Aufsichtsbehörde vertrat die Auffassung, dass die EU-Standardvertragsklauseln inhaltlich durchaus verwendet werden könnten, es muss nur ein anderer Weg gefunden werden, um diese rechtliche Verbindlichkeit, vor allem auch zugunsten der vom Datentransfer betroffenen Personen, zu verschaffen.

Dies hat sich an den Anforderungen zu orientieren, welche die Artikel 29-Gruppe zur Herstellung der internen und externen Verbindlichkeit von Unternehmensregeln zum Drittstaatentransfer aufgestellt hat (Nr. 5 des Arbeitspapiers 108, im Internet abrufbar unter:
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_de.pdf).

Zur Herstellung der externen Verbindlichkeit bietet sich vor allem eine einseitige zugangsbedürftige, aber nicht annahmebedürftige, Garantieerklärung durch den Datenimporteur bzw. das Unternehmen (da ja eine rechtliche Einheit besteht) an, durch welche ein Garantievertrag mit den betroffenen Datensubjekten zustande käme. Dies könnte erfolgen, indem die Standardvertragsklauseln nebst entsprechender Erklärung, sich an diese zu halten, in das Internet oder Intranet gestellt werden (je nach betroffenem Personen-

kreis) oder in sonstiger Weise gegenüber den betroffenen Personen zugänglich gemacht werden.

Diese Rechtsauffassung des Regierungspräsidiums Darmstadt wurde auch von den Mitgliedern der Arbeitsgruppe "Internationaler Datenverkehr" des Düsseldorfer Kreises geteilt.

Die Vorteile der Standardvertragsklauseln können also auch in den beschriebenen Sonderfällen genutzt werden. Es besteht weder eine Genehmigungs- noch eine Vorlagepflicht (siehe Nr. 7.2 des Fünfzehnten Berichtes der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Drs. 15/4659).

11.3 EU-Standardvertragsklauseln vom Dezember 2004

Am 27. Dezember 2004 hat die EU-Kommission die von sieben Unternehmensverbänden vorgeschlagenen alternativen Standardvertragsklauseln für den internationalen Datentransfer zur Gewährleistung ausreichender Datenschutzgarantien anerkannt.

Auf Grund entsprechender Beratungsanfragen betrieblicher Datenschutzbeauftragter beschäftigte sich das Regierungspräsidium Darmstadt hier u.a. mit der Frage, ob diese alternativen Standardvertragsklauseln zur Anwendung kommen können, wenn ein in Deutschland ansässiges Unternehmen sich zur Verarbeitung personenbezogener Daten eines Datenverarbeitungsdienstleisters in einem Drittstaat bedienen will.

Wie unter Nr. 7.2 des Fünfzehnten Berichtes der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden (Drs. 15/4659), ausgeführt wurde, sind für solche Fälle die mit Entscheidung der EU-Kommission vom 27. Dezember 2001 verabschiedeten Standardvertragsklauseln vorgesehen.

Für die Fälle, bei denen der Datenempfänger im Drittstaat nicht nur als weisungsgebundener Datenverarbeitungsdienstleister tätig wird, sondern darüber hinausgehende Aufgaben und Kompetenzen erhält, kommen dagegen die von der EU-Kommission am 15. Juni 2001 verabschiedeten Standardvertragsklauseln in Betracht.

Der Standardvertrag vom Dezember 2004 stellt nur eine Alternative zum Standardvertrag vom Juni 2001 dar, also für den Fall, dass der Datenimporteur als eigenständige verantwortliche Stelle agiert. Dies ergibt sich daraus, dass mit der betreffenden Entscheidung der EU-Kommission auf die Kommissionsentscheidung vom Juni 2001 Bezug genommen wird, die damit abgeändert wird. Auch die Überschrift der Klauseln macht deutlich, dass diese nicht für Übermittlungen an einen bloßen Datenverarbeitungsdienstleister genutzt werden können (siehe auch Kuner/Hladjik, RDV 2005, S. 193 (195)).

12. Arbeitnehmerdatenschutz

12.1 Videoüberwachung in einer Produktionsstätte

Anlässlich einer Beschwerde über die in den Werkshallen angebrachten Videokameras wurde ein Metall verarbeitender Betrieb einer Überprüfung nach § 38 BDSG unterzogen, bei der folgende Feststellungen getroffen wurden:

Das Betriebsgelände und die Werkshallen werden durch insgesamt 4 Videokameras, eine am Eingang zum Verwaltungsgebäude und drei in den zwei Werkshallen, überwacht. Die Aufzeichnung läuft durchgehend eine Woche und wird dann überspielt. Der Monitor steht in der Verwaltung, ist allerdings in der Regel, z.B. auch während der Überprüfung, ausgeschaltet.

Die Anschaffung der Videokameras erfolgte, nachdem mehrere Diebstähle von Silber und Nickel in großen Mengen und von beträchtlichem Wert vorgekommen waren. Die Versicherung hatte angekündigt, die künftige Beitragsfestsetzung und Schadensregulierung von der Erweiterung der Einbruchmeldeanlage mit Videotechnik abhängig zu machen. Allein mit dem bereits vorhandenen Bewegungsmelder und der Direktschaltung des Alarms

zu einem Sicherheitsdienst wollte sich die Versicherung nicht mehr zufrieden geben.

Eine Inaugenscheinnahme der in den Werkshallen installierten Kameras ergab, dass diese auf die dort lagernden Metalle gerichtet sind. Es ist zwar unvermeidbar, dass die Beschäftigten auch von den Kameras erfasst werden, sie befinden sich aber nicht ständig im Blickfeld der Kameras, stehen also nicht unter Dauerbeobachtung. Auch erfolgt die Videobeobachtung nicht verdeckt, sondern deutlich erkennbar.

Nach Abwägung der schutzwürdigen Interessen der betroffenen Mitarbeiter an der Wahrung ihrer Persönlichkeitsrechte und des berechtigten Interesses des Arbeitgebers an der Videoüberwachung ist die Aufsichtsbehörde zu dem Ergebnis gelangt, dass in diesem Fall die Interessen des Arbeitgebers überwiegen.

Als zulässig kann eine Videobeobachtung am Arbeitsplatz nur dann bewertet werden, wenn überwiegende Sicherheitsinteressen diese erforderlich machen. Generell ist - auch wenn § 6b BDSG mangels öffentlicher Zugänglichkeit des Arbeitsplatzes nicht greift - zur Wahrung der Persönlichkeitsrechte der Beschäftigten von dem Grundsatz auszugehen, dass das Interesse des Arbeitgebers, etwa zum Schutz vor Verlust von Firmeneigentum durch Diebstahl, nur dann als berechtigt und schutzwürdig anzuerkennen ist und einen Eingriff in die Persönlichkeitsrechte der Beschäftigten rechtfertigen kann, wenn es vor Beginn der Videoüberwachung durch konkrete Anhaltspunkte und Verdachtsmomente belegt wurde.

Diese Voraussetzungen sind hier erfüllt. Die Betriebsleitung des Unternehmens war nach den wiederholten Diebstählen auf Grund einer Forderung der Versicherung gehalten, geeignete Sicherheitsvorkehrungen zu treffen, um auch bei evtl. weiteren Einbrüchen Versicherungsleistungen in Anspruch nehmen zu können. Videokameras sind als geeignetes Mittel zum Schutz vor Eigentumsdelikten anzusehen, insbesondere unter dem Aspekt der Abschreckung vor möglichen Straftätern und zur Sicherung von Beweismaterial.

Bei der Interessenabwägung war auch die Intensität der Beobachtung relevant, also die Tatsache, dass die Mitarbeiter nicht dauernd, sondern nur gelegentlich erfasst werden, da die Videokameras nicht direkt auf die Arbeitsplätze und die dort tätigen Mitarbeiter gerichtet sind.

Auch die Art der Aufzeichnung (Laufzeit 1 Woche, dann Überspielung) war akzeptabel.

12.2 Drogentest bei Mitarbeitern

Die Geschäftsleitung eines in Hessen ansässiges Daten- und Aktenvernichtungsunternehmens bat um Prüfung, ob die Anordnung von regelmäßigen Drogentests bei Mitarbeitern zulässig sei. Grund für die Anfrage war die Absicht des Unternehmens, sich durch die NAID (National Association of Information Destruction) mit Sitz in USA zertifizieren zu lassen. Zu den Prüfkriterien dieses Verbandes gehören u. a. Drogentests, denen sich zum Zeitpunkt der Einstellung alle Mitarbeiter, die Zugang zu Daten Dritter haben, und während des Arbeitsverhältnisses einmal jährlich nach einem Zufallsverfahren ausgewählte 50 % dieser Beschäftigten, zu unterziehen haben.

Das Bundesarbeitsgericht hatte bereits mit Urteil vom 12.08.1999 (Recht der Datenverarbeitung - RDV - 2000, S. 66) entschieden, dass ein Arbeitnehmer ohne entsprechende gesetzliche oder tarifvertragliche Verpflichtung und ohne konkrete Verdachtsmomente nicht verpflichtet ist, sich routinemäßig auf eine eventuelle Alkohol- oder Drogenabhängigkeit untersuchen zu lassen.
Der Persönlichkeitsschutz ist auch im Arbeitsverhältnis garantiert, weshalb Eingriffe jeweils im Einzelfall einer Interessen- und Güterabwägung bedürfen. Die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung von Mitarbeiterdaten hat sich primär nach dem Zweck des Arbeitsvertrages, also nach § 28 Abs. 1, Satz 1 Nr. 1 BDSG zu richten. Eine Erhebung der durch Drogentests zu gewinnenden Daten stand hier aber in keinem unmittelbaren Bezug zum Zweck des Arbeitsvertrages. Auch die Zulässigkeitsalternative des § 28 Abs. 1, Satz 1 Nr. 2 BDSG kam nicht in Betracht, da die Zertifi-

zierung für das Unternehmen keine zwingende Voraussetzung darstellte und es somit an dem Erfordernis zur Wahrung berechtigter Interessen fehlte. Im Übrigen bietet der Bundesverband Sekundärrohstoffe und Entsorgung e.V. (bvse) Zertifizierungen für Entsorgungsbetriebe an, ohne Drogentests bei Mitarbeitern zu fordern. In diesem Fall standen der Erhebung derartiger Gesundheitsdaten die überwiegenden schutzwürdigen Interessen der Beschäftigten entgegen. Ebenso wurde die Zulässigkeit solcher Drogentests mit Einwilligung der Betroffenen verneint, da von der Freiwilligkeit solcher Erklärungen im Arbeitsverhältnis bei der Erhebung sensibler Daten regelmäßig nicht ausgegangen werden kann.

13. Tele- und Mediendienste

13.1 Verwirrung um eine falsche E-Mail-Weiterleitung

Die meisten Internet-Nutzer verfügen heute über mehr als eine E-Mail-Adresse, um die Kommunikation zu strukturieren oder um E-Mail-Spam besser vorfiltern zu können. Für kostenlose Zusatzadressen gibt es eine ganze Reihe von Anbietern auf dem Markt. Auch fast alle Zugangsprovider bieten als Standardleistung inzwischen mehrere kostenlose Zusatzadressen an. Dass diese entstandene Vielfalt und Dynamik in einigen Fällen auch zu einer gewissen Unübersichtlichkeit führt, die datenschutzrechtlich unerwünschte Folgen haben kann, wurde bereits unter Nr. 11.6 des Sechzehnten Berichtes der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, (Drs. 16/1680), dargestellt.

Im Berichtsjahr bat nun ein betroffener Adressinhaber die Datenschutzaufsichtsbehörde um Unterstützung, da er seit einiger Zeit beständig E-Mails für eine Person mit ähnlichem Realnamen erhalte, die er allerdings nicht kenne. Es handele sich nicht um Spam oder ähnliche unerwünschte Nachrichten, sondern um den ganz normalen E-Mail-Eingang eines anderen Internet-Nutzers. Ihm sei das alles sehr unangenehm, er möchte keine E-Mails erhalten, die nicht für ihn bestimmt sind. Unter den E-Mails befanden sich auch Rechnungen mit personenbezogenen Daten, unter anderem auch vom Zugangs- und E-Mail-Provider der anderen Person. Der Petent bat die Datenschutzaufsichtsbehörde sich der Sache anzunehmen, da er vermutete, dass der Provider die E-Mails seiner Kunden falsch zustellen würde.

Die Nachforschungen der Aufsichtsbehörde ergaben allerdings ein anderes Bild. Auf Nachfrage teilte der betroffene Provider mit, der Kunde habe die in Rede stehende E-Mail-Adresse des Beschwerdeführers vor Jahren selbst als zusätzliche Weiterleitungsadresse angegeben. Die Konfiguration der E-Mail-Weiterleitung sei Kundensache, man habe auf diese Einstellungen keinen Einfluss. Da der Provider nicht bereit war, seinen Kunden auch nur auf die veraltete Konfiguration hinzuweisen, nahm die Datenschutzaufsichtsbehörde Kontakt mit dem Kunden auf und bat ihn dafür zu sorgen, dass keine Kopien seines E-Mail-Eingangs mehr an die aktuellen Inhaber einer seiner alten E-Mail-Adressen versandt werden. Der zunächst verblüffte Providerkunde hatte selbst größtes Interesse daran, dass seine E-Mail-Kommunikation nicht in Kopie anderen Internet-Nutzern zur Kenntnis gelangt. Er hatte die Weiterleitung auf seine alte E-Mail-Adresse schlichtweg vergessen. Nach dem Hinweis der Datenschutzaufsichtsbehörde löschte er die veraltete Einstellung in seiner Konfiguration umgehend.

Die anfänglichen Befürchtungen des Beschwerdeführers, der Provider habe Kunden-E-Mails falsch zugestellt und damit gegen datenschutzrechtliche Regeln und das Fernmeldegeheimnis verstoßen, stellten sich somit als unbegründet heraus. Der Aufsichtsbehörde bleibt nur der Hinweis, vor einem Wechsel der E-Mail-Adresse sorgsam zu überprüfen, wo die alte E-Mail-Adresse eingetragen und angegeben wurde. Auf jeden Fall sollten vor dem Kündigen der E-Mail-Adresse alle Kommunikationspartner benachrichtigt, alle Newsletter abbestellt und alle eingestellten E-Mail-Weiterleitungen gelöscht werden, um sich selbst und anderen Internet-Nutzern unnötigen Aufwand und Ärger zu ersparen.

13.2 Unzulässiges Telefonmarketing eines Internet-Providers

Im Berichtsjahr ging eine Welle von Beschwerden bei der Datenschutzaufsichtsbehörde gegen unverlangte Telefonanrufe ein, die im Auftrag eines

großen südhessischen Internet-Providers erfolgten. Die Beschwerdeführer gaben teils an, der werblichen Nutzung ihrer Telefonnummer nie zugestimmt zu haben, obwohl dies für die werbliche Nutzung einer Telefonnummer erforderlich ist (zur UWG-Novelle und zum datenschutzrechtlich unzulässigen kalten Telefonmarketing siehe unten Ziff. 15.2). Andere schilderten, dass man ihnen Zugangssoftware und Kennwort zugesandt habe, obwohl sie in dem Telefonat deutlich gemacht hätten, dass sie nicht an einem Vertrag interessiert seien. Diese Betroffenen verlangten von dem Provider die umgehende Löschung ihrer Daten, da kein Vertragsverhältnis existiere.

Die Ermittlungen der Datenschutzaufsichtsbehörde und des betrieblichen Datenschutzbeauftragten des Providers ergaben, dass die Marketingabteilung des Unternehmens einen Vertriebspartner damit beauftragt hatte, weitere Sub-Auftragnehmer mit der Gewinnung der Daten potentieller Kunden zu beauftragen und entsprechende Telefonmarketing-Aktionen von einem Call-Center als zusätzlichem externen Dienstleister durchführen zu lassen. Dabei war vertraglich festgelegt, dass die datenschutzrechtlichen und wettbewerbsrechtlichen Bestimmungen einzuhalten sind und eine Einwilligung der betroffenen Telefonanschlussinhaber vorhanden sein muss.

Nachdem die Datenschutzaufsichtsbehörde in den vorliegenden Beschwerdefällen einen Nachweis über das Vorliegen einer schriftlichen Einwilligung nach § 4 a BDSG von dem Internet-Provider anforderte, musste dieser eingestehen, dass keiner der beauftragten Geschäftspartner oder einer der Sub-Unternehmer in auch nur einem Fall in der Lage war, einen Beleg für eine vorliegende Einwilligung vorzulegen, obwohl alle dazu vertraglich verpflichtet gewesen wären. Der Internetprovider, der für die Vermittlung jedes (angeblichen) Kunden eine Provision gezahlt hatte, hat die Zusammenarbeit mit diesen unseriös arbeitenden Marketingfirmen daraufhin sofort eingestellt.

Der Internet-Provider hat zur Vermeidung solcher rufschädigenden Ereignisse ein geeignetes Maßnahmenpaket geschnürt. Bei künftigen Marketing-Verträgen des Providers mit Dienstleistern und deren Subunternehmern wird besonderer Wert auf die präzise Formulierung der datenschutzrechtlichen Vorgaben nach § 11 BDSG gelegt werden. Alle aktuellen Vertragspartner werden ausdrücklich auf die Einhaltung der datenschutzrechtlichen Verpflichtungen hingewiesen. Zudem werden die diesbezüglichen Kontrollen der Auftragnehmer nach § 11 Abs. 2 Satz 4 BDSG durch den betrieblichen Datenschutzbeauftragten des Providers intensiviert. Zur Qualitätssicherung sollten künftig auch sog. "Second-Calls" von einem weiteren Spezialdienstleister durchgeführt werden, der sich die Angaben des ersten Call-Centers inhaltlich nochmals bestätigen lässt. Verstöße gegen die vertraglichen Vorgaben des Auftraggebers werden in Zukunft bei den Dienstleistern wirtschaftlich spürbarer verfolgt werden.

Die hessische Datenschutzaufsichtsbehörde hat die für die beteiligten Unternehmen zuständigen Datenschutzaufsichtsbehörden der betroffenen anderen Bundesländer nach § 38 Abs. 1 Satz 2 BDSG in Kenntnis gesetzt, um dort ebenfalls entsprechende Überprüfungen bei den beteiligten Adressmaklern und dem Call-Center nach der Datenherkunft und dem Vorliegen der für das Telefonmarketing erforderlichen Einwilligungen zu ermöglichen.

Die im Zusammenhang mit dem unzulässigen Telefonmarketing aufgetretenen datenschutzrechtlichen Verstöße wurden bei dem nach § 11 Abs. 1 Satz 1 BDSG hierfür verantwortlichen südhessischen Internet-Provider beanstandet. Die eingeleiteten Maßnahmen des Providers sind ebenso geeignet wie hoffentlich hinreichend und wurden begrüßt.

13.3 Anti-Cheat-Scanning bei Online-Spielen im Internet

Online-Spiele im Internet werden vor dem Hintergrund der in Deutschland immer noch ansteigenden Vernetzung der Haushalte mit Breitbandzugängen zum Internet und günstiger DSL-Flatrates nicht nur bei Jugendlichen immer beliebter. Auf den erfolgreichsten weltweiten Spiele-Plattformen sind oftmals mehrere Millionen Spieler aller Nationalitäten gleichzeitig in diesen künstlichen Welten unterwegs, um mittels virtueller Figuren mit- und gegeneinander "online" zu spielen. Bei einigen dieser Spiele sind mittlerweile mehr als einhunderttausend aktive Nutzer aus Deutschland angemeldet. Ei-

nes dieser großen Online-Spiele wird von einem in Hessen ansässigen, aber zu einem internationalen Konzern gehörenden Unternehmen in Deutschland als CD-Set über den Fach- und Einzelhandel vertrieben.

Im Berichtsjahr gingen beim Regierungspräsidium Darmstadt einige Anfragen und kritische Hinweise von Online-Spielern ein, in denen dem Unternehmen vorgeworfen wurde, als Betreiber der Online-Plattform dieses kostenpflichtigen Online-Rollenspiels die PCs der Spieler auf den Einsatz sog. "Cheat-Tools" (Betrugs-Software, die das Umgehen von Spielregeln ermöglicht) zu scannen und dabei auch andere personenbezogene Daten der Spieler auszuspionieren. Auch in den amerikanischen und deutschen "Online-Spiele-Foren" im WWW wurden diese Vorwürfe von der Spielergemeinde teilweise sehr emotional diskutiert. Viele Nutzer waren zwar selbst daran interessiert, dass das Unternehmen gegen Betrüger und Spielverderber in den Online-Welten vorgeht. Es herrschte allerdings große Verunsicherung darüber, ob das "Scannen" der Spieler-PCs lediglich dem Zweck dient, solche Cheat-Software zu erkennen oder ob bei diesem "Scanning" auch andere persönliche Informationen an das Unternehmen übermittelt würden. Zudem wurde oftmals bemängelt, dass die Spieler über Zweck und Umfang des Einsatzes eines "Anti-Cheating-Tools" auf den Spieler-PCs nicht ausreichend informiert würden und dem Scanning auch nicht zugestimmt hätten. Auf Grund dieses Sachverhalts wurde vom Regierungspräsidium Darmstadt eine datenschutzrechtliche Überprüfung der Angelegenheit eingeleitet.

Der Einsatz von Hack-Programmen und "Cheats" ist in den Lizenzvereinbarungen (End User Licens Agreement - EULA) und den Nutzungsbedingungen (Terms of Use - ToU) des Spiels strengstens untersagt, da der erfolgreiche dauerhafte Betrieb eines weltweit verteilten komplexen Server-Systems für die Online-Plattform eines "Massive Multiplayer Online Roleplaying Games" (MMORPG) zwingend davon abhängig ist, dass alle Spieler unter den gleichen Voraussetzungen spielen und keine "unbesiegbaren" Falschspieler in diesen virtuellen Welten ihr Unwesen auf Kosten zahlender Kunden treiben. Dennoch wurde der Betreiber immer wieder von verärgerten Kunden auf andere betrügende Mitspieler aufmerksam gemacht, die sich erkennbar nicht an Regeln des jeweiligen "Realms" (eine von vielen virtuellen Unter-Welten auf der Online-Plattform) halten müssen und z. B. unbesiegbar und unverwundbar sind oder gar bei Gefahr teleportieren (den Standort wechseln) können, ohne dass die Programme des Betreibers solche Funktionen vorsehen. Die für diese Betrügereien erforderlichen Hack- und Cheat-Programme sind einfach zu erhalten und werden im WWW offensichtlich sogar international gewerblich vertrieben.

Bei der weiteren Untersuchung stellte sich allerdings schnell heraus, dass die weltweite Online-Spiele-Plattform, auf der das zur Rede stehende MMORPG läuft, von einem US-amerikanischem Tochterunternehmen des Unterhaltungskonzerns betrieben wird. Von dort werden auch beim Anmelden des Spiele-Accounts und der Registrierung des CD-Keys auf der Online-Plattform die Scans zur Suche nach den nach der EULA und den ToU unerlaubten Cheats auf den PCs der Spieler veranlasst. Das deutsche Tochterunternehmen organisiert lediglich den Vertrieb des CD-Spiele-Sets an die Verkaufsstellen in Deutschland. Personenbezogene Daten der Spieler liegen dem deutschen Unternehmen nicht vor. Als verantwortliche Stelle für die Verarbeitung personenbezogener Daten i.S.d.§ 3 Abs. 7 BDSG und damit als Ansprechpartner für die Datenschutzaufsichtsbehörde kommt die deutsche Konzerntochter daher nicht in Betracht. Die für die Datenverarbeitung im Zusammenhang mit den PC-Scans durch das Anti-Cheating-Scan-Tool verantwortliche Stelle, bei der auch die personenbezogenen Daten der weltweit angemeldeten und zahlenden Nutzer des Spiels gespeichert werden, ist ohne Zweifel das in den USA ansässige Tochterunternehmen.

Wie bereits im Fünfzehnten Tätigkeitsbericht der hessischen Datenschutzaufsicht dargelegt wurde, kann deutsches Datenschutzrecht bei richtlinienkonformer Auslegung nach Art. 4 Abs. 1c EG-Datenschutzrichtlinie (EG-DSRL) gerade bei Telediensten im WWW auch auf Stellen Anwendung finden, die ihren Sitz nicht im Gemeinschaftsgebiet haben, insoweit wird auf die Ausführungen unter Nr. 7.6 des Fünfzehnten Berichtes der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden (Drs. 15/4659), verwiesen. Die Arbeitsgruppe nach Art. 29 EG-DSRL hat diese Position mittlerweile

bzgl. der Verwendung von Cookies, Javascript und vergleichbarer Software in ihrem Arbeitspapier WP 56 vom 30. Mai 2002 festgehalten.

Aber selbst wenn daher davon ausgegangen werden kann, dass für die Datenerhebung und Verarbeitung beim "Anti-Cheat-Scanning" deutscher User-PCs durch eine amerikanische Stelle deutsches Datenschutzrecht gilt, macht es diese Konstellation der Datenschutzaufsichtsbehörde nicht gerade leicht, die deutschen datenschutzrechtlichen Anforderungen an die Transparenz und Zulässigkeit der Verarbeitung personenbezogener Daten durch einen ausländischen Anbieter eines Teledienstes durchzusetzen. Mittel aufsichtsbehördlichen Zwangs lassen sich in dieser Situation gegenüber einem weltweit agierenden amerikanischen Unternehmens kaum entfalten. Die theoretisch vorhandenen Kontroll- und Prüfungsrechte einer deutschen Datenschutzaufsichtsbehörde nach § 38 Abs. 3 und 4 BDSG sind bei einer amerikanischen Stelle ebenfalls kaum umsetzbar.

Durch die entgegenkommenden Vermittlungsbemühungen der deutschen Vertriebstochter des Konzerns gelang es dem Regierungspräsidium Darmstadt dennoch, den Kontakt mit dem amerikanischen Betreiber der Online-Plattform herzustellen. Es fand ein langes und intensives Gespräch zwischen Vertretern der Datenschutzaufsichtsbehörde und einer beauftragten internationalen Rechtsanwaltskanzlei statt, bei dem auch Vertreter des amerikanischen Betreibers anwesend waren, die unter anderem zur Beantwortung technischer Fragstellungen eigens aus den USA angereist waren.

Bei dem Online-Anbieter in den USA wurden die, natürlich nicht zuletzt auch auf Grund der anfänglichen Desinformation dieses Anbieters, teilweise recht unkundigen und spekulativen Diskussionen um das eingesetzte Scan-Tool in den Online-Spiele-Foren genau beobachtet und auch sehr ernst genommen. Man war sogar entsetzt, in Verdacht geraten zu sein, die PCs zahlender Dauer-Kunden auszuspionieren und wies dies entschieden von sich. Das Unternehmen sei als einer der in den letzten Jahren weltweit erfolgreichsten Online-Spiele-Anbieter sehr an dauerhaften Kundenbeziehungen interessiert und man sei besorgt über das durch die "mangelhafte Kommunikation" möglicherweise verloren gegangene Vertrauen, insbesondere auch der zahlungskräftigen deutschen Online-Spieler. Schließlich sei man naturgemäß am weiteren kommerziellen Erfolg des Spiels sehr interessiert und wolle jede Verunsicherung der User vermeiden, die diesen Erfolg gefährden könnte.

Die Aufsichtsbehörde nutze die Gelegenheit, den Vertretern des Plattformbetreibers die Bedenken der deutschen Kunden sowie die nach deutschem Datenschutzrecht erforderlichen Rahmenbedingungen zum zulässigen Einsatz eines solchen Anti-Cheat-Tools nahe zu bringen. Auch zu technischen Fragestellungen wurden detaillierte Auskünfte eingeholt.

Insbesondere wurde dem amerikanischen Anbieter verdeutlicht, dass nach dem deutschen Teledienstedatenschutzgesetz (TDDSG) auf jeden Fall ein ausführlicher und nicht zu übersehender Hinweis an die Nutzer des Spiels mit einer Unterrichtung gemäß § 4 Abs. 1 TDDSG über Art, Umfang und Verwendungszwecke erfolgen muss, wenn personenbezogene Daten "online" im Rahmen der Erbringung eines Teledienstes erhoben werden. Diese Transparenzpflicht gilt ganz unabhängig davon, ob die Datenverarbeitung beim "Scanning" als "inhaltliche Ausgestaltung eines Vertragsverhältnisses" im Sinne von § 5 TDDSG gesehen werden kann oder sich diese Datenverarbeitung außerhalb des Rahmens des § 5 TDDSG bewegt und daher eine Einwilligung nach §§ 3, 4 Abs. 2 und 3 TDDSG erforderlich wäre.

Erforderlich ist in diesem Sinne jedenfalls eine bessere und frühzeitige Information und Unterrichtung der User, mehr und auffälligere Hinweise und Unterrichtungen im Sinne von § 4 Abs. 1 TDDSG nicht nur in den ToU und EULAs. Die Kenntnisnahme dieser vertraglichen Regelungen sollte zusätzlich möglichst noch durch eine bewusste Handlung des Betroffenen im Sinne von § 4 Abs. 2 Nr. 1 TDDSG bestätigt werden.

Außerdem wurde die Datenschutzaufsichtsbehörde von den Technikern des Unternehmens detailliert über die Funktionsweise des verwendeten "Anti-Cheating-Scan-Tools" in Kenntnis gesetzt. Es wurde nachvollziehbar erläutert, dass das Tool lediglich einen Hash-Wert aus dem Inhalt bestimmter spielrelevanter Stellen des Arbeits- bzw. Prozessorspeichers und der aktuel-

len Prozessliste bildet und mittels dieses Hashwerts vor jeder Online-Sitzung überprüft, ob verbotene Cheats installiert sind oder nicht. Andere Inhalte des User-PCs würden beim Scanning vollkommen unberührt gelassen, insbesondere würden keinerlei vom Online-Spiel unabhängige personenbezogene Nutzungs- oder Bestandsdaten ausgespäht und übermittelt. Das Tool habe sich bereits in der Anfangsphase des Einsatzes als sehr effektiv erwiesen. Viele andere Online-Plattform Betreiber setzen mittlerweile ähnliche Anti-Cheating-Programme ein.

Bei einer Testinstallation des Spiels durch die EDV-Experten der Aufsichtsbehörde haben sich auch keine belastbaren Anhaltspunkte dafür ergeben, dass sich das amerikanische Unternehmen durch die Scans des Anti-Cheating-Tools außer dem Hash-Wert irgendwelche personenbezogene oder sonstige Daten von der Festplatte der User verschafft. Und obwohl inzwischen alle Kunden - und damit auch die technisch versierteren Online-Spieler - unübersehbar auf das Anti-Cheat-Scanning hingewiesen werden, liegen der Datenschutzaufsichtsbehörde keinerlei Beschwerden oder hinreichende Hinweise von Online-Spielern vor, aus denen auf einen Missbrauch personenbezogener Daten durch den Anbieter geschlossen werden könnte.

Schon während des Gesprächs wurde von den Vertretern des Anbieters signalisiert, dass die Forderungen der Datenschutzaufsichtsbehörde ernst genommen würden und dass das Unternehmen bereit sei, die Vorschläge der deutschen Aufsichtsbehörde zur transparenteren Ausgestaltung der Datenerhebung und Datenverarbeitung zügig weltweit umzusetzen. Das Unternehmen hat dann auch recht schnell reagiert und mit den ersten Patches und Updates im Jahr 2006 weltweit entsprechende Änderungen vorgenommen. Neue User und auch Spieler mit bereits bestehenden Accounts werden im Gegensatz zu früher nun unmissverständlich und unübersehbar i.S.d.§ 4 Abs. 1 TDDSG auf den Einsatz eines Anti-Cheating-Scan-Tools vor jeder Online-Spiele-Sitzung aufmerksam gemacht und müssen zudem per Mausklick bestätigen, dass Sie über das Scanning informiert wurden. Zudem beabsichtigt das Unternehmen einen sog. "Launcher" einzuführen, mit dem Kunden ihren PC vor der Online-Sitzung auf das Vorhandensein unzulässiger Cheats und Schadprogramme selbst prüfen können, ohne dass Daten an den amerikanischen Plattformbetreiber übermittelt werden.

Es wurde der Aufsichtsbehörde zudem zugesichert, dass die Kunden, die dem Scanning nicht zustimmen möchten, das ungespielte Spiel bei der Verkaufsstelle zurückgeben können und den Kaufpreis zurückerhalten.

Zum Redaktionsschluss dieses Berichtes waren die Verhandlungen und Gespräche mit der beauftragten internationalen Anwaltskanzlei über weitere datenschutzrechtliche Details im Zusammenhang mit der Verarbeitung personenbezogener Daten bei diesem MMPORG zwar noch nicht abgeschlossen, der konstruktive Verlauf der bisherigen Gespräche macht aber durchaus Hoffnung auf die weitere datenschutzfreundlichere Ausgestaltung dieses Teledienstes.

14. Videoüberwachung und Webcams

14.1 Videoüberwachung im Behindertenheim

Der Vorstand eines Wohnheims für behinderte Menschen bat die Aufsichtsbehörde um Beratung hinsichtlich der Zulässigkeit einer geplanten Videoüberwachung.

Bei einer Besprechung mit dem Vorstand und einer Begehung der Anlage stellte sich die Situation wie folgt dar:

In der Einrichtung werden u. a. geistig und mehrfach behinderte Menschen in Wohngruppen betreut. Auf Grund von Verhaltensauffälligkeiten ist bei mehreren Kindern und Jugendlichen ein erhöhter Aufsichtsbedarf vorhanden. Daher hat man diesen besonders problematischen Personenkreis zusammen in einer Wohngruppe untergebracht. Mit Aggressionen zwischen den Gruppenmitgliedern ist nach bisherigen Erfahrungen stets zu rechnen, auch zur Nachtzeit. In der Zeit von 21.00 bis 6.00 Uhr hält sich in dieser Wohngruppe daher eine Nachtwache auf. Der Mitarbeiter ist allerdings für mehrere Wohngruppen in verschiedenen Gebäuden zuständig. Durch regel-

mäßige Rundgänge (viermal pro Nacht) ist sichergestellt, dass auch die anderen Gruppen kontinuierlich betreut werden.

Da die verhaltensauffälligen Kinder und Jugendlichen in dieser Zeit unbeaufsichtigt sind, hatte der Vorstand die Installation von Videokameras in den Fluren und Aufenthaltsbereichen, nicht in Schlafräumen und Sanitärbereichen, dieser Wohngruppe ins Auge gefasst, war sich aber über die Zulässigkeit der Überwachung unsicher. Nach der Vorstellung des Vorstands sollte die Übertragung von einem für einen anderen Wohngruppenbereich zuständigen Nachtdienst auf dem zu diesem Zweck dort aufgestellten Monitor überwacht werden, damit dieser Mitarbeiter dann bei etwaigen Vorkommnissen in der Wohngruppe den auf dem Rundgang befindlichen Betreuer sofort alarmieren kann. Es war vorgesehen, die Kameras tagsüber auszuschalten.

Die Aufsichtsbehörde bewertete die beabsichtigte Videoüberwachung nach Interessenabwägung in Anbetracht der besonderen Umstände als zulässig, sofern folgende Einschränkungen beachtet werden:

1. Die Videokameras werden ausschließlich in der einen Wohneinheit, für deren Bewohner ein erhöhter Aufsichtsbedarf besteht, installiert. Die Anbringung erfolgt nur in den Verkehrsbereichen (Flure, Gemeinschaftsraum).
2. Die Videokameras werden nur während der Rundgänge der Nachtwache eingeschaltet. Tagsüber und bei Anwesenheit der Nachtwache in der Wohngruppe bleiben die Kameras ausgeschaltet.
3. Die Videoüberwachung erfolgt ausschließlich als Echtzeitübertragung, Aufzeichnungen werden nicht gefertigt.

14.2 Interaktive Webcam

Ein Druck- und Verlagshaus überraschte auf seiner Internet-Seite mit einer besonderen "Spielerei". Eine Webcam, die vom Dach des Geschäftsgebäudes aus Live-Bilder der Umgebung in das WWW lieferte und mit einer interaktiven Steuerungsmöglichkeit für den Nutzer versehen war. Nach Aufrufen der Kamerasteuerung ließ sich die Webcam von jedem Rechner aus nach Belieben schwenken, neigen und zoomen.

Dies war einer Bürgerin suspekt, nachdem ihr durch geschicktes Zoomen bildschirmfüllende Nahaufnahmen von den Fenstern benachbarter Wohnhäuser gelungen waren. Es war ihr auch möglich, sich im Aufnahmebereich bewegende Personen zu erkennen, so dass in diesen Fällen gegenüber dem Druck- und Verlagshaus eine unerlaubte Verarbeitung personenbezogener Daten beanstandet werden musste.

Mit dem ausgedruckten "Beweismaterial" konfrontiert, erklärte das Unternehmen gegenüber der Aufsichtsbehörde, dass die Kamera bereits abgeschaltet worden sei. Die Webcam sei ohne Beteiligung des betrieblichen Datenschutzbeauftragten installiert worden und solle nun nicht mehr in Betrieb genommen werden.

14.3 "Live-Übertragungen" aus einer Modeboutique

In einem dritten Fall beschwerte sich ein Bürger über eine deutlich sichtbare Überwachungskamera, die zur Beobachtung einer belebten Verkehrsstraße an der Hauswand eines Modegeschäfts installiert worden war.

Die Kamera war Bestandteil eines Marketing-Konzepts, mit dem der Geschäftsinhaber den Absatz seiner Modewaren im Internet vorantreiben wollte. Durch "Live-Bilder" von dem Ladengeschäft und dessen Umgebung sollten Besucher der WWW-Seite einen Einblick in das Unternehmen erhalten und sich dabei von dessen Seriosität bzw. Leistungsfähigkeit überzeugen können. Dazu hatte der Inhaber - neben der bereits erwähnten Kamera an der Außenfassade - vier Webcams im Verkaufsraum installiert. Zwei Geräte waren auf das Schaufenster und die Eingangstür gerichtet, wodurch nicht nur Passanten auf dem Fußweg aufgenommen wurden, sondern auch die Straße und die gegenüberliegende Häuserfront. Auf der Internet-Seite standen "rund um die Uhr" aktuelle Bilder aus unterschiedlichen Blickwinkeln und wechselnden Zoom-Bereichen zur Verfügung. So konnten beispielsweise das Personal beim Einräumen gelieferter Waren oder die Kunden beim Aussuchen von Kleidungsstücken beobachtet werden.

Bei allem Verständnis für kreative Marketing-Konzepte konnte die Aufsichtsbehörde den Weiterbetrieb der Installation doch nicht unbeanstandet lassen.

Dem Verantwortlichen wurde zunächst aufgegeben, die an der Hauswand angebrachte Kamera abzuschalten, da eine rechtliche Grundlage für die Beobachtung des öffentlichen Straßenraumes nicht gegeben war. Die Überwachung diente weder der Aufgabenerfüllung einer öffentlichen Stelle, noch der Wahrnehmung des Hausrechts und ließ sich insbesondere nicht für Marketingzwecke rechtfertigen.

Aber auch soweit Aufnahmen aus dem Geschäft vorgesehen waren, mussten die "Live-Übertragungen" per Webcam kritisch bewertet werden. Mit dieser grundsätzlichen Thematik hatte sich die Aufsichtbehörde bereits in den Vorjahren zu befassen (siehe hierzu ausführlich unter Nr. 7.7 des Vierzehnten Berichtes der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Drs. 15/2950). Zusammenfassend liegt die besondere Problematik in der weltweiten Verbreitung der Bilder und deren nahezu unbegrenzbare Verfügbarkeit für den Internet-Nutzer bei Entfallen jeglicher Kontroll- und Löschungsmöglichkeiten. Zur Wahrung des Persönlichkeitsrechts der Betroffenen hielt es die Aufsichtsbehörde im konkreten Fall für geboten, das weitere Einstellen von Bildern in das WWW von mehreren Voraussetzungen abhängig zu machen.

Die Webcam sollte so konfiguriert werden, dass keine Personen oder Gegenstände, durch welche Personen bestimmt werden können, auf der Internet-Seite erkennbar sind.

Andernfalls müsse für die Betroffenen rechtzeitig ersichtlich sein, dass sie aufgenommen werden. Weiterhin bedürfe es in diesem Fall deren Einwilligung, bevor der Aufnahmebereich der Kamera betreten wird. Schließlich müsse sichergestellt sein, dass der Wille der Betroffenen, nicht gefilmt zu werden, jederzeit respektiert werden kann.

Dabei machte die Aufsichtsbehörde auch deutlich, dass Einwilligungen im Rahmen eines bestehenden Arbeitsverhältnisses in Bezug auf deren Wirksamkeit äußerst kritisch zu bewerten sind, da oftmals nicht von einer Freiwilligkeit ausgegangen werden kann. Nachdem Arbeitsgerichte bereits im Falle von Videoaufzeichnungen von einem schwerwiegenden Eingriff in das Persönlichkeitsrecht ausgehen, ist fraglich, ob sich in einem Streitfall der Arbeitgeber auf eine Einwilligung zur Übertragung in das WWW wird berufen können.
Nach ausführlicher Erörterung dieser Punkte stellte der Geschäftsinhaber die "Live-Übertragungen" schließlich ein.

15. Werbung, Direktmarketing

15.1 Werbung "auf Empfehlung"

Die im Berichtsjahr bei der Aufsichtsbehörde eingegangenen Anfragen und Beschwerden zur Werbewirtschaft konzentrierten sich erneut überwiegend auf die "klassischen" Themenbereiche des Kundendatenschutzes. Nicht immer erhielten die Bürgerinnen und Bürger in zufrieden stellender Weise Auskunft über die zu ihrer Person gespeicherten Daten - mancher Widerspruch gegen die werbliche Nutzung der Adressdaten blieb auch im Jahr 2005 unberücksichtigt. In diesen Fällen konnte die Aufsichtsbehörde den Betroffenen fast immer zu ihrem Recht verhelfen.

Dem Versenden personalisierter Werbung wird - innerhalb der mittlerweile vielfältigen Möglichkeiten zur Kontaktaufnahme mit der Kundschaft - von Seiten der Unternehmen nach wie vor hohe Bedeutung beigemessen. Auch wenn hierbei von Direktwerbung gesprochen wird, bedeutet dies keineswegs, dass die Werbeaussendungen immer "auf direktem Weg" vom Anbieter zum umworbenen Empfänger versendet werden.

So wunderte sich ein Bürger über den Werbebrief eines Kreditkartenunternehmens, der einen vorbereiteten Antrag für den Abschluss einer Pflegeversicherung bei einer Versicherungsgesellschaft enthielt. Neben der vollständigen Adresse war in den Unterlagen auch bereits der altersabhängig zu ermittelnde Monatsbeitrag in konkreter Höhe eingetragen.

Da der Betroffene zwar Inhaber einer Kreditkarte war, aber bislang keinerlei geschäftliche Beziehungen zu der Versicherungsgesellschaft aufgenommen hatte, befürchtete er, dass das Kartenunternehmen seine Kundendaten zur Erstellung dieses Vertragsangebots übermittelt hatte.

Auf Nachfrage der Aufsichtsbehörde teilten die beteiligten Unternehmen mit, es handele sich bei der beschriebenen Werbeaktivität um ein "Empfehler-Mailing" im Rahmen ihrer Kooperation, was nachfolgend näher beschrieben werden soll.

Bei Abschluss des Kartenvertrags wird der Neukunde darüber informiert, dass für werbliche Zwecke keinerlei personenbezogene Daten an Dritte weitergegeben, allerdings Angebote kooperierender Firmen versendet werden. Nach Zusammenstellung der für den Vertragspartner "interessanten" Kundenadressen - und anschließendem Abgleich mit internen Sperrlisten und der "Robinson-Liste"- werden die Werbebriefe vom Kreditkartenunternehmen versandfertig gemacht. Dazu hat der Vertragspartner sein Werbematerial bereits in Blankoform zur Verfügung gestellt. Einzelne Werbeaktionen werden auch im Wege der Auftragsdatenverarbeitung über "Lettershops" abgewickelt, die dann das Werbematerial erstellen und versenden. Zur Berechnung individueller Tarife stellt das Versicherungsunternehmen ein Rechenmodul zur Verfügung, welches anhand des Eintrittsalters und in Abhängigkeit des Geschlechts den jeweiligen Versicherungsbeitrag ermittelt. Die Eingabe der Kundendaten in das Modul erfolgt im Rechenzentrum des Kreditkartenunternehmens. Auf Grund dieser klaren Trennung wird sichergestellt, dass keinerlei personenbezogene Daten in den Kenntnisbereich des Vertragspartners gelangen. Das Versicherungsunternehmen "erfährt" erst, wer zur Zielgruppe des Mailings gehörte, wenn der Empfänger auf das Angebot eingeht und - dann direkt an dieses gerichtet - antwortet.

Nach eingehender Prüfung wurde das "Empfehler-Mailing"-Verfahren in der beschriebenen Weise aus datenschutzrechtlicher Sicht akzeptiert. Allerdings war zu beanstanden, dass einzelne Werbebriefe nicht mit einen ausreichenden Widerspruchshinweis versehen waren - ein Umstand, der vorliegend als besonders schwerwiegend zu bewerten war, da dies zu Unklarheiten über die Identität der verantwortlichen Stelle führen konnte. Als problematisch wurde auch gesehen, dass der Betroffene durch die Antwort auf das Mailing dem werbenden Unternehmen bestimmte Merkmale "seiner" Zielgruppe - wie z.B. "Inhaber einer xy-Kreditkarte" - übermittelt. Das Kreditkartenunternehmen wurde daher aufgefordert, die Empfänger der Werbebriefe in geeigneter Weise darüber zu informieren.

15.2 Die Bekanntenempfehlung - eine Notlüge beim unzulässigen Telefonmarketing

Durch die 2004 erfolgte Novellierung des Gesetzes zur Bekämpfung des unlauteren Wettbewerbs (UWG) wurde klargestellt, dass das Telefonmarketing gegenüber Verbrauchern nach §§ 3, 7 Abs. 2 Nr. 2 UWG eine unzumutbare Belästigung darstellt und daher wettbewerbsrechtlich unzulässig ist, wenn nicht die Einwilligung des Verbrauchers vorliegt.

Da aus datenschutzrechtlicher Sicht eine Telefonnummer als personenbezogenes Datum im Sinne von § 3 Abs. 1 BDSG zu bewerten ist, ist die Verarbeitung der Telefonnummer zu Werbezwecken auch datenschutzrechtlich relevant. Ein gesetzlicher datenschutzrechtlicher Erlaubnistatbestand für die Verarbeitung und Nutzung von Telefonnummern zu Werbezwecken kann allerdings in § 28 Abs. 1 Satz 1 Nr. 1-3 BDSG nicht gesehen werden. Es existiert meist kein Vertragsverhältnis mit dem Betroffenen bzw. ein solches würde auch keine Telefonwerbung rechtfertigen. Gerade vor dem Hintergrund der wettbewerbsrechtlichen Unzulässigkeit einer solchen Werbemaßnahme nach dem UWG besteht ganz deutlich Grund zur Annahme, dass schutzwürdige Interessen der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung ihrer Telefonnummer überwiegen. Das Einwilligungserfordernis des UWG kann also nicht unter Berufung auf § 28 BDSG "ausgehebelt" werden. Als Rechtfertigung für eine Verarbeitung der Telefonnummern zu Werbezwecken kann daher nur eine Einwilligung in Frage kommen.

Trotz dieser eindeutigen Rechtslage ist kein Rückgang bei den eingehenden Beschwerden gegen solche unverlangten Werbeanrufe zu verzeichnen.

Wenn sich betroffene Bürgerinnen und Bürger an die Datenschutzaufsichtsbehörde wenden, werden Sie bei der Durchsetzung ihrer Rechte auf Auskunft über die Datenherkunft (§ 34 Abs. 1 BDSG) und auf Löschung bzw. Sperrung ihrer Telefonnummer für Werbeanrufe (§ 35 Abs. 2, 3 BDSG) unterstützt. Bei zivil- oder wettbewerbsrechtlichen Fragen können die Wettbewerbszentrale (www.wettbewerbszentrale.de) und die Verbraucherzentralen (www.vzbv.de) weiterhelfen.

Als besonders dreist stellte sich bei den Nachforschungen der Datenschutzaufsichtsbehörde in einem solchen Fall ein freier Handelsvertreter einer großen Vermögensberatungsgesellschaft heraus. Ein von einem unverlangten Werbeanruf betroffener Bürger erhielt auf Nachfrage nach der Herkunft seiner Daten inkl. Telefonnummer die Auskunft, die Daten habe der Vertreter von einem "Vereinskameraden" erhalten. Obwohl der Betroffene anschließend schriftlich versicherte, dass er in keinem Verein Mitglied sei und sein Auskunftsersuchen unter Hinweis auf die eindeutige datenschutzrechtliche und wettbewerbsrechtliche Gesetzeslage wiederholte, erteilte die Vermögensberatung keine Auskunft über die Datenherkunft nach § 34 Abs. 1 BDSG. Stattdessen wurde der Beschwerdeführer darauf hingewiesen, dem Unternehmen würde eine besondere "sozialpolitische Rolle" zukommen, die natürlich auch in Form von telefonischen "Informationen und Empfehlungen" wahrgenommen würde. Der Betroffene bat die Datenschutzaufsichtsbehörde daher um Prüfung.

Die interne Prüfung des Sachverhalts, die von dem betrieblichen Datenschutzbeauftragten des Vermögensberatungsunternehmens mit großem Engagement durchgeführt wurde, klärte die Angelegenheit vollständig auf. Der freie Handelsvertreter des Unternehmens gab zu, zur Neukundengewinnung einfach das örtliche Telefonbuch genutzt zu haben. Er hatte bei der Nachfrage des betroffenen Bürgers bezüglich der Datenherkunft spontan nach der "Ausrede" gegriffen, es handele sich um eine Empfehlung durch einen Vereinsfreund, da er sich der Unzulässigkeit seiner Telefonmarketing-Variante wohl durchaus bewusst war. Gerade diese offensichtliche "Notlüge" führte in der Folge allerdings dazu, dass der Betroffene sich an die Aufsichtsbehörde wandte.

Die Datenschutzaufsichtsbehörde beanstandete die unzulässige Verarbeitung der Daten des Beschwerdeführers.

Insbesondere wurde gegenüber dem Unternehmen auch klargestellt, dass seine behauptete "sozialpolitische Rolle" bei der datenschutzrechtlichen Bewertung kommerzieller Marketingmaßnahmen nicht zu einer Privilegierung bei der Verarbeitung personenbezogener Daten zu Werbezwecken führen kann. Der freie Unternehmensberater wurde von dem Unternehmen auf die Rechtswidrigkeit seines Handelns hingewiesen und zur künftigen Unterlassung dieser unlauteren Werbemaßnahmen aufgefordert.

Besonders betont werden muss an dieser Stelle die sehr hilf- und erfolgreiche Arbeit des betrieblichen Datenschutzbeauftragten des Vermögensberatungsunternehmens, durch dessen Einschaltung die Angelegenheit in kürzester Zeit geklärt werden konnte.

15.3 Unerbetener Werbeanruf zum Versicherungsabschluss

Zwei Kundinnen eines Versandhandelsunternehmens wandten sich an die Aufsichtsbehörde, weil die zum gleichen Konzern gehörende Bank ihre Telefonnummern für einen unerbetenen Werbeanruf genutzt hatte. Die Beschwerdeführerinnen waren beide Kundinnen des Versandhandelsunternehmens und Inhaberinnen einer Kreditkarte dieser Bank.

Der Werbeanruf des Call-Centers hatte die Empfehlung einer "Familienversicherung" zum Inhalt, deren Vermittlung durch die Bank erfolgen sollte. Die Anrufe erfolgten dabei im Auftrag und nach Weisung der Bank. Als Bonus wollte die Bank die ersten zwei Monatsprämien der Versicherung übernehmen. Die Versicherung sollte telefonisch vermittelt und abgeschlossen werden und eine Abbuchung der Versicherungsgebühr über die Kreditkarte der Beschwerdeführerinnen von dem Kundenkonto des Versandhandelsunternehmens erfolgen.

Die Beschwerdeführerinnen beklagten sich, angerufen worden zu sein. Sie waren außerdem der Auffassung, in dem Telefongespräch lediglich der unverbindlichen Zusendung eines Angebots zugestimmt, nicht aber telefonisch einen Versicherungsvertrag abgeschlossen zu haben. Beide führten aus, ihre Kreditkartennummer bei dem Gespräch nicht benannt zu haben. Trotzdem sei es zu einer Zusendung einer Versicherungspolice sowie der automatischen Abbuchung der Versicherungssumme von dem Kreditkartenkonto der Bank gekommen.

Die Aufsichtsbehörde griff das Problem des unerbetenen Anrufs auf.

Die Bank vertrat die Auffassung, zu dem Werbeanruf berechtigt zu sein. Ferner sei es zu einem telefonischen Vertragsabschluss gekommen und die Beschwerdeführerinnen hätten die Bank zur automatischen Abbuchung der Versicherungsgebühr von ihrem Kreditkartenkonto ermächtigt.

Die Nutzung der gespeicherten Nummer zur Vornahme unerbetener Werbeanrufe durch das von der Bank beauftragte Call-Center wurde durch die Aufsichtsbehörde beanstandet, da eine vorherige Einwilligungserklärung für telefonische Werbung nicht vorgelegt werden konnte.

Sie kann insbesondere nicht in der freiwilligen Angabe der Telefonnummer im Zusammenhang mit der Beantragung einer Kreditkarte bei der Bank gesehen werden. Auch § 28 Abs. 1 Satz 1 Nr. 2 BDSG rechtfertigt es nicht, die vorhandenen Kundendaten für eine telefonische Versicherungswerbung zu nutzen (siehe oben Ausführungen zu Ziff. 15.2).

Die Verwendung der Daten für die Telefonwerbung war somit unzulässig. Darüber hinaus erschien auch der behauptete Vertragsabschluss sowie die vermeintlich telefonisch eingeholte Einwilligung in die automatische Abbuchung der Versicherungsprämie nach Prüfung der Sachlage als zweifelhaft.

Nachdem die Aufsichtsbehörde das Vorgehen schriftlich beanstandet hatte, wurde die Kooperation der Bank mit der Versicherung eingestellt.

15.4 Telefonwerbung bei Kundenanfragen

Ein Kunde eines Versandhandelsunternehmens hatte sich an die Aufsichtsbehörde gewandt, weil er während eines Telefonats mit dessen Kundenservice überredet wurde, bei einer Gewinnspielplattform mitzuspielen. Konkret hatte er den Kundenservice angerufen, um ein kostenloses Stoffmuster zu erhalten. Nach Erledigung dieser Bestellung wurde er auf ein exklusives Gewinnspiel angesprochen, welches das Versandhaus in Partnerschaft mit einer Spielplattform anbietet. Bei der Abwicklung des dabei geschlossenen Vertrages kam es dann zu Unstimmigkeiten, zu deren Klärung die Behörde einbezogen wurde und so Kenntnis von der geschilderten Werbepraxis erlangte.

Die praktizierte Vermittlungstätigkeit wurde von der Aufsichtsbehörde gegenüber dem Versandhaus beanstandet, da durch die unerwartete und oftmals wohl auch ungewünschte Werbeansprache schutzwürdige Belange des Klientels über ein vertretbares Maß hinaus beeinträchtigt werden.

So konnte sich das Versandhandelsunternehmen zunächst nicht auf ein bestehendes bzw. sich anbahnendes Kundenverhältnis nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG berufen, da bei telefonischer Werbung für ein Partnerunternehmen, das Gewinnspiele anbietet, kein sachlicher Zusammenhang mit dem jeweils konkreten Vertragszweck erkennbar ist.

Ebenso sah die Aufsichtsbehörde die Voraussetzungen für eine Nutzung der Kundendaten zur Wahrung berechtigter Interessen nach § 28 Abs. 1 Nr. 2 BDSG als nicht gegeben, da ein überwiegend schutzwürdiges Interesse des Betroffenen zu erkennen ist, das sich aus den Wertungen der §§ 3,7 Abs. 2 Nr. 2 1. Alt. des UWG ergibt. Dabei verkannte die Aufsichtsbehörde nicht, dass deren Inhalt zunächst auf Fälle der "klassischen Telefonwerbung" abzielt und bei der zu bewertenden Konstellation die Initiative in Form eines Anrufs von den Betroffenen selbst ausging. Aus der Konstruktion des UWG wird indes deutlich, dass die darin genannten Beispielsfälle nicht abschließend sind und dem Rechtsanwender die Möglichkeit eröffnet wird, neuartige Wettbewerbsmaßnahmen sachgerecht zu beurteilen. Durch das "Umfunktionieren" des Anrufs in ein Werbegespräch sind wesentliche Elemente der

individuellen Telefonwerbung gegeben, so beispielsweise, dass die Werbung zur Kenntnis genommen werden muss, bevor der Kunde entscheiden kann, ob er das Gespräch fortsetzen möchte. Ein Anrufer, der sich vertrauensvoll in ein Beratungsgespräch begibt und dabei letztlich in finanzieller und zeitlicher Hinsicht für Werbung für völlig andere Produkte in Anspruch genommen wird, sieht sich einer Verfahrensweise ausgesetzt, die in keiner Weise der vom Verbraucher erwarteten geschäftlichen Übung entspricht. Dem Versandhändler wurde daher mitgeteilt, dass die Verwendung der Kundendaten für solche Marketingaktionen nur unter vergleichbaren Voraussetzungen, wie sie an die "klassische" Telefonwerbung zu stellen sind, zulässig seien, und insoweit der zuvorigen Einwilligung bedürften.

Nachdem die Aufsichtsbehörde die Vorgehensweise beanstandet hatte, wurde die Werbetätigkeit eingestellt.

15.5 Umfrage oder Werbung?

Eine private Musikschule ließ in Grundschulen über die Klassenlehrer ein Werbeschreiben für musikalische Früherziehung verteilen, die in den Räumlichkeiten der jeweiligen Schule stattfinden sollte. Die Eltern wurden unter dem Titel "Umfrage" aufgefordert, Name, Anschrift und Telefonnummer einzutragen und anzukreuzen, ob generell Interesse an einer Teilnahme bestehe. Abgefragt wurde auch der Name und das Geburtsdatum des Kindes und welche Klasse es besucht. Auf diese Weise angesprochen, beschwerte sich ein Elternteil über den "offiziellen Charakter" der Werbung, der durch den Begriff "Umfrage" i.V.m. der gewählten Vertriebsweise irreführend hervorgerufen worden sei.

Die Aufsichtsbehörde machte gegenüber den Verantwortlichen deutlich, dass die Aktionen ausschließlich der Neukundengewinnung dienen und mit Markt- und Meinungsforschung bzw. Sozialforschung nichts gemeinsam haben.

Der Musikschule wurde daher aufgegeben, das Werbematerial mit einem Datenschutzhinweis und einer schriftlichen Einwilligungserklärung für die beabsichtigte telefonische Kontaktaufnahme zu versehen.

Die Vordrucke wurden daraufhin neu gestaltet.

15.6 Teure Auskunft

Nicht einschüchtern ließ sich ein Reiseteilnehmer von der Reaktion des Veranstalters, als er um Auskunft nach § 34 BDSG zu den über ihn gespeicherten Daten gebeten hatte. Ein vom Reiseunternehmen beauftragter Rechtsanwalt ließ den Anfragenden wissen, dass für die Auskunft eine Bearbeitungsgebühr in noch unbekannter Höhe zu zahlen sei und er vorab grundsätzlich die Bereitschaft zur Zahlung erklären solle. Der Bürger leitete den Schriftwechsel direkt an die Aufsichtsbehörde weiter, die gegenüber dem Unternehmen unter Hinweis auf § 34 Abs. 5 Satz 1 BDSG klarstellte, dass die Auskunft unentgeltlich zu erfolgen habe. Das Vorkommnis wurde bei einer anschließenden Überprüfung vor Ort nochmals eingehend erörtert.
Das Unternehmen versicherte, in Zukunft kostenfrei zu beauskunften.

15.7 Mahnung per Telefon

Kundendienst besonderer Art leistete ein Autohaus, indem es einen ausstehenden Betrag mehrfach per Telefon anmahnte. Dies geschah jedoch nicht bei der Schuldnerin selbst, sondern an Ihrem Arbeitsplatz, wo eine Kollegin die Anrufe in Abwesenheit entgegennahm. Auch auf mehrfachen Hinweis, dass sie nicht die gewünschte Gesprächspartnerin sei, wurde die Arbeitskollegin über Details, wie die kurz bevorstehende Einschaltung eines Inkassobüros, informiert. Die "Schuldnerin" wendete sich darauf hin an die Aufsichtsbehörde, da der behauptete Zahlungsrückstand gar nicht bestehe und sie sich durch die Anrufe im Büro belästigt und verleumdet fühle. Gegenüber dem Autohaus musste deutlich gemacht werden, dass auch Kundendaten - und insbesondere sensible Informationen wie das Vorhandensein von Schulden -schutzwürdig sind und keinesfalls gedankenlos an Dritte übermittelt werden dürfen (vgl. auch oben unter Nr. 8.2). Da es sich bei dem Vorfall um einen erstmalig bekannt gewordenen Verstoß handelte, wurde von der Einleitung eines Ordnungswidrigkeitenverfahrens abgesehen.

16. Fußball WM 2006

Bereits seit Sommer 2004 hat sich das Regierungspräsidium Darmstadt mit der Fußball WM 2006 beschäftigt (siehe hierzu unter Nr. 11 des Achtzehnten Berichtes der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Drs. 16/4752).

Nachdem die Konzeption und der rechtliche Rahmen feststanden, musste überprüft werden, ob die rechtlichen Vorgaben der Aufsichtsbehörde eingehalten und ausreichende Maßnahmen zur Datensicherheit getroffen wurden. Kein einfaches Unterfangen bei einer derart umfangreichen Datenverarbeitung.

Ein sehr komplexes IT-System wurde nicht nur zur Sicherstellung des Kartenverkaufs sondern auch zur Akkreditierung eingesetzt. Eine solche Verarbeitung, die nicht auf Dauer ausgelegt ist, sondern nach Ende der WM nicht mehr benötigt wird, kann vom Veranstalter nicht alleine erledigt werden. Der Deutsche Fußball-Bund (DFB) bediente sich daher einer Vielzahl von verschiedenen Dienstleistern, wie Datenerfassern, Web-Seiten-Verwaltern, Rechenzentren usw. Die Datenverarbeitung wurde so ausgelegt, dass jeweils eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG vorliegt.

Die Aufsichtsbehörde hatte von Anfang an auf schriftliche Vertragsgestaltung und auf vollständige Weisungen, ebenfalls in Schriftform, bestanden. Diese Forderung beruht auf den Anforderungen des § 11 BDSG, mit dessen Inhalt die verantwortliche Stelle zunächst nicht ausreichend vertraut war. Der DFB versicherte jedoch, diese und andere datenschutzrechtliche Anforderungen einzuhalten und schaltete zur Unterstützung einen externen Datenschutz-Dienstleister ein, wie von der Aufsichtsbehörde empfohlen (siehe hierzu unter Nr. 11 des Achtzehnten Berichtes der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Drs. 16/4752). Es dauerte gleichwohl relativ lange, bis entsprechende Verträge nach § 11 BDSG abgeschlossen und der Aufsichtsbehörde vorgelegt wurden.

Zum Zweck des Kartenverkaufs schaltete der DFB einen Hauptauftragnehmer ein, der schon über ein deutschlandweit erprobtes Verkaufssystem für Veranstaltungstickets jeglicher Art verfügt. Dieses reichte aber für die speziellen Anforderungen bei der WM 2006 bei weitem nicht aus. Das Unternehmen ließ durch ein konzernangehöriges Unternehmen eine spezielle Software entwickeln und richtete eine Nebenstelle in unmittelbarer Nähe der verantwortlichen Stelle (DFB) ein. Wenngleich dieser Hauptauftragnehmer seinen Sitz außerhalb Hessens hat, wurden daher vom Regierungspräsidium Darmstadt umfangreiche Prüfungen bei dessen Zweigstelle in Hessen vorgenommen.

Dieser Dienstleister bedient sich weiterer Subauftragnehmer. Aufgrund der Forderungen der Aufsichtsbehörde wurden auch insoweit entsprechende Verträge nach § 11 BDSG geschlossen.
Es bedurfte auch einiger Anstrengungen der Aufsichtsbehörde, bis der DFB vollständige Verfahrensverzeichnisse erstellt hatte und eine Aufstellung aller an der Datenverarbeitung beteiligten Unternehmen vorgelegt wurde. Diese Dokumentationen waren aber erst die Grundlage zu einer Datenschutzüberprüfung, die dann stattfinden konnte. Zu erwähnen ist, dass die Aufsichtsbehörde im Vorfeld der eigentlichen Prüfungen bereits Beratungen und Vorprüfungen durchführte, um Fehler möglichst noch vor dem endgültigen Einsatz einzelner Verfahren vermeiden oder bereinigen zu können.

Der auch vom Veranstalter als Generalprobe angesehene Confederations-Cup wurde auch von der Aufsichtsbehörde zu ersten Überprüfungen genutzt. Geprüft wurden die mit dem Stadionbesuch verbundenen Datenverarbeitungsvorgänge (Zutrittskontrollen am Eingang, Klärung von Zweifelsfällen am Servicepoint) vor Ort. Es stellten sich kleinere Mängel im Bereich der Datensicherheit heraus, die aber laut Veranstalter bzw. dessen Dienstleistern bis zur WM abgestellt werden. Ebenso konnten Maßnahmen zur besseren Sicherung der Datenbestände in den Stadion-Rechnern veranlasst werden.
Im Bereich der Akkreditierung waren hauptsächlich Fehler bzw. Unzulänglichkeiten im vorliegenden Berechtigungskonzept festgestellt worden. Das Berechtigungskonzept wurde daraufhin überarbeitet und wird bei Gelegenheit nochmals vor Ort überprüft werden.

Zwischenzeitlich haben der DFB und dessen Dienstleister alle Akkreditierungsdaten aus dem Confederations-Cup gelöscht. Die Ticketdaten wurden gelöscht, mit Ausnahme von wenigen Datenarten, die aus steuerlichen und buchhalterischen Gründen aufbewahrt werden müssen; diese wurden aber für andere Zwecke gesperrt.

Bei allen Überprüfungen wurden zum einen zuständige Mitarbeiter befragt und zum anderen Einsicht in die Verarbeitung genommen. Stichprobenartig wurden die einzelnen Datenbanken durchgesehen und im Hinblick auf Einhaltung der Vorgaben aus der Dokumentation geprüft. Dabei wurde besonderes Augenmerk darauf gelegt, dass nicht mehr Datenarten verarbeitet werden, als dokumentiert sind. Geprüft wurde auch, ob Selektionen oder Sortierungen durchführbar sind, die über das erforderliche Maß hinausgehen.

Die Aufsichtsbehörde interessierte sich auch dafür, ob ausschließlich die zulässigen Datensätze zur Werbung genutzt werden (siehe hierzu unter Nr. 11.1.6 des Achtzehnten Berichtes der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Drs. 16/4752). Hierbei stellte sich heraus, dass bis zum Zeitpunkt der letzten Überprüfung überhaupt keine Daten für Werbezwecke genutzt oder weitergegeben wurden.

Natürlich wurden auch die Maßnahmen zur Zutrittskontrolle in die einzelnen Rechenzentren und den Server-Bereichen geprüft ebenso Maßnahmen zur Zugangskontrolle, einschließlich sicherer Übertragungswege.

Als Ergebnis bleibt festzuhalten, dass die Aufsichtsbehörde sehr umfangreiche Beratungen durchführen musste und sich zu einer Reihe von Prüfungen veranlasst sah, um eine ordentliche Datenverarbeitung gewährleisten zu können. Selbstverständlich bleibt die Verantwortung beim Veranstalter, die Aufsichtsbehörde kann keinesfalls alle Details der hochkomplexen Datenverarbeitung prüfen. Der DFB sowie dessen Hauptauftragnehmer waren kooperativ und letztlich engagiert und legten unmittelbar vor Redaktionsschluss dieses Berichts noch umfangreiche Unterlagen vor, die nun zu prüfen sind. Abgeschlossen sind die Überprüfungen daher noch nicht. Es wird bis zum Ende der WM 2006 und auch danach weitere Überprüfungen geben, bis die Aufsichtsbehörde sicher ist, dass die Verarbeitung beendet ist und alle Daten, soweit nicht mehr erforderlich, gelöscht sind.

17. Speicherung von Urlaubsnachsendeadressen bei Zeitungsverlagen

Zeitungsverlage speichern teilweise die Urlaubsnachsendeadressen ihrer Abonnenten über einen mehrjährigen Zeitraum und halten diese Daten zur weiteren Bearbeitung, etwa für spätere Nachsendeanträge, vor.

Dies ist jedoch nicht gerechtfertigt, da diese Daten gem. § 35 Abs. 2 Nr. 3 BDSG nach Erfüllung des jeweils einzelnen Geschäftszwecks grundsätzlich umgehend zu löschen sind. Soweit für buchhalterische Zwecke erforderlich, können diese jedoch für einen hierfür notwendigen Zeitraum weiter gespeichert bleiben, müssen jedoch für andere Zwecke gesperrt werden, wobei die Löschung umgehend nach Ablauf der Fristen für interne Abrechnungs- und Rechnungslegungszwecke zu veranlassen ist.

Im konkreten Fall hat die Aufsichtsbehörde die Verlagsanstalt hierauf hingewiesen und letztlich erreicht, dass die Standardsoftware um ein Modul zur Erfüllung der datenschutzrechtlichen Forderung nach § 35 Abs. 2 Nr. 3 i.V.m. § 35 Abs. 3 Nr. 1 BDSG ergänzt wurde. Demnach werden die Nachsendeadressen nach Erledigung des Nachsendeauftrags (Ablauf der Nachsendezeit und somit Erfüllung des einzelnen Geschäftsauftrags) nach § 35 Abs. 3 Nr. 1 BDSG zunächst für die weitere Nutzung gesperrt und lediglich zur Gewährleistung buchhalterisch und nach HGB notwendiger Aufbewahrungsfristen bereitgehalten. Nach Ablauf der oben genannten Fristen werden die Daten nach § 35 Abs. 2 Nr. 3 BDSG gelöscht.

Wiesbaden, 7. August 2006

Der Hessische Ministerpräsident:
Koch

Der Hessische Minister des Innern und für Sport:
Bouffier