16. Wahlperiode

Drucksache **16/4752**

HESSISCHER LANDTAG

05. 12. 2005

Vorlage
der Landesregierung

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

Vorgelegt mit der Stellungnahme zum Dreiunddreißigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten - Drucks. 16/3746 - nach § 30 Abs. 2 des Hessischen Datenschutzgesetzes in der Fassung vom 7. Januar 1999.

Eingegangen am 5. Dezember 2005 · Ausgegeben am 23. Dezember 2005
Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

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

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

Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich waren im Berichtszeitraum noch die drei Regierungspräsidien. Mit der Verordnung zur Regelung der Zuständigkeiten nach dem Bundesdatenschutzgesetz und anderen Gesetzen zum Datenschutz vom 10. Februar 2005 (GVBl. I S. 90) ist die Aufsicht nach § 38 Bundesdatenschutzgesetz für ganz Hessen seit dem 1. März 2005 auf das Regierungspräsidium Darmstadt übertragen worden. Bei Erscheinen dieses Tätigkeitsberichts gibt es in Hessen daher nur noch eine Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich - das Regierungspräsidium Darmstadt.

1.1 Bearbeitung von aktuellen Eingaben und Beschwerden

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

Im Berichtsjahr wurden von den Aufsichtsbehörden in Hessen in 528 Fällen Überprüfungen von nicht öffentlichen Stellen vorgenommen, die Datenverarbeitung nach § 28 BDSG für die Erfüllung eigener Geschäftszwecke betreiben oder personenbezogene Daten nach §§ 29, 30 BDSG zur personenbezogenen oder anonymisierten Übermittlung speichern und nutzen.

Im Vergleich zum Vorjahr (540 Fälle) ist damit die Zahl der Eingaben und Beschwerden annähernd gleich geblieben.

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 E-Mail mit entsprechenden Dateianhängen geschieht.

Die 528 Überprüfungen von Eingaben, Beschwerden und Pressemeldungen durch die Aufsichtsbehörden betrafen:

- in 95 Fällen die Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA),
- in 74 Fällen Telediensteanbieter (Anbieter von Internetzugängen, -diensten und -inhalten, unverlangte E-Mail-Werbung),
- in 58 Fällen Stellen und Unternehmen der Direktmarketing- und Werbewirtschaft,
- in 51 Fällen Handels- und Wirtschaftsauskunfteien,
- in 49 Fällen Banken, Kreditinstitute und EDV-Dienstleister im Zahlungsverkehr,
- in 41 Fällen den Datenschutz in Arbeitsverhältnissen und bei Arbeitsvermittlern,
- in 24 Fällen Versicherungsgesellschaften,
- in 15 Fällen die Videoüberwachung von Grundstücken, Häusern und Wohnungen,
- in 14 Fällen das Gesundheitswesen (Apotheken, Ärzte, Krankenhäuser, Senioren- und Pflegeheime),

- in 13 Fällen sonstige Stellen (z.B. Soft- und Hardware-Hersteller, Verkehrsunternehmen, Steuerberater, Weiterbildungseinrichtung),
- in 12 Fällen Unternehmen der Versandhandelsbranche,
- in 12 Fällen Vereine (Sport, Soziales, Kultur) sowie deren Landes- und Bundesverbände,
- in 12 Fällen Adresshandelsunternehmen,
- in 11 Fällen Inkassounternehmen,
- in 9 Fällen Unternehmen des Groß- und Einzelhandels,
- in 9 Fällen Vermieter sowie Wohnungs- und Immobilienverwaltungsfirmen,
- in 7 Fällen Unternehmen der Freizeit-, Touristik- und Reisebranche,
- in 6 Fällen Verlage und Presse,
- in 5 Fällen Kreditkartenunternehmen,
- in 4 Fällen Datenschutzbeauftragte,
- in 2 Fällen Anwaltskanzleien,
- in 2 Fällen Beratungsunternehmen,
- sowie in jeweils einem Fall eine politische Partei, ein Markt- und Meinungsforschungsunternehmen und eine Auslandsdatenverarbeitung.

Bei ca. 26 v.H. der Beschwerden konnte zeitnah festgestellt werden, dass diese begründet waren. In insgesamt 138 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 der jeweiligen Verarbeitungsverfahren bei den betroffenen Stellen führten.

Die bei den Überprüfungen beanstandeten 138 Verstöße gegen Datenschutzbestimmungen wurden festgestellt:

- in 28 Fällen bei der Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA), davon war in 15 Fällen ein Verstoß durch den Vertragspartner der SCHUFA ursächlich,
- in 28 Fällen bei Unternehmen der Direktmarketing- und Werbebranche,
- in 16 Fällen bei Kreditinstituten und Banken,
- in 11 Fällen bei Anbietern von Tele- und Mediendiensten im Internet (Access- und Content-Provider und Versender von Werbe-E-Mails),
- in 10 Fällen bei der Verarbeitung von Arbeitnehmer- und Bewerberdaten,
- in 7 Fällen bei Versicherungsgesellschaften,
- in 6 Fällen in der Versandhandelsbranche,
- in 6 Fällen bei Adresshändlern,
- in 4 Fällen bei Unternehmen der Freizeit-, Touristik- und Reisebranche,
- in 4 Fällen bei Vereinen und Verbänden,
- in 4 Fällen bei Handels- und Wirtschaftsauskunfteien,
- in 3 Fällen bei Inkassounternehmen,
- in 3 Fällen bei Verlagen und in den Medien,
- in 3 Fällen im Groß- und Einzelhandel,
- in 2 Fällen im Wohnungswesen (Vermieter),

  sowie in jeweils einem Fall bei einer politischen Partei, im Gesundheitssektor (Arzt, Krankenhaus), bei einem Steuerberater und einer Weiterbildungseinrichtung.

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

1.2 Erledigung von Eingaben und Beschwerden aus den Vorjahren

Von den noch aus den Vorjahren anhängigen Beschwerden, die oftmals sehr vielschichtige Verarbeitungszusammenhänge betrafen, wurden im Berichts-

jahr 166 Fälle abgeschlossen. Die Beurteilung dieser in der Regel nur mit hohem Ermittlungsaufwand aufklärbaren Eingaben durch die Aufsichtsbehörden ergab, dass davon 83 Eingaben begründet waren. Damit mussten die Aufsichtsbehörden bei 50 % dieser Fälle einen Datenschutzverstoß feststellen.

Die beanstandeten 83 Verstöße gegen Datenschutzbestimmungen wurden festgestellt

- in 22 Fällen bei Banken,
- in 15 Fällen bei Unternehmen der Werbewirtschaft und werbenden Einzelhändlern,
- in 10 Fällen bei der SCHUFA, davon in 2 Fällen bei den Vertragspartnern,
- in 7 Fällen bei Anbietern von Telediensten (Internetprovider),
- in 5 Fällen bei Arbeitgebern und Arbeitsvermittlern,
- in 4 Fällen bei Inkassounternehmen,
- in 3 Fällen bei Handels- und Wirtschaftsauskunfteien,
- in 3 Fällen in der Verkehrs- und Reisebranche,
- in 2 Fällen bei eingetragenen Vereinen und Verbänden,
- in 2 Fällen im Gesundheitswesen,
- in 2 Fällen bei der Video-Beobachtung öffentlich zugänglicher Räume,
- in 2 Fällen bei Versicherungsunternehmen

  sowie in jeweils einem Fall bei einem Versandhändler, einem Adresshändler, einem Handwerksbetrieb, einer politischen Partei, einem Kreditkartenunternehmen und einem Bezahlungsdienst.

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

Bei den im Berichtsjahr insgesamt durchgeführten Prüfungen von Eingaben, Beschwerden und Hinweisen auf Datenschutzverstöße bestand in 18 Fällen Veranlassung für eine Überprüfung vor Ort. Nur auf diese Weise ließ sich zuverlässig feststellen, ob ein Datenschutzverstoß vorlag.
Die Prüfdauer variierte dabei - je nach Komplexität der Datenverarbeitung und der Schwere des Vorwurfs - von kurzen ein- bis zweistündigen Prüfungen bis zu ganztätigen Prüfungen, Vor- und Nachbereitungszeit nicht eingerechnet.

1.4 Anlassunabhängige Überprüfungen

Im Berichtsjahr wurden neun anlassunabhängige Kontrollen durchgeführt.

Diese betrafen folgende Branchen/Bereiche

- Videoüberwachungssysteme, 3
- Handels- und Gewerbeunternehmen, 2
- Ärztliche Praxen/Kliniken/Laboratorien, 1
- Konzerndatenverarbeitungsdienstleister, 1
- Laborunternehmen, 1
- Verband. 1

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

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

Neben den dargestellten neun anlassunabhängigen Prüfungen wurden auch die 18 Überprüfungen aus konkretem Anlass (siehe oben Nr. 1.3 des Berichtes) überwiegend dazu genutzt, um die Datenverarbeitung der verantwortlichen Stellen umfassender zu prüfen. Die Prüfungen wurden nicht nur auf den konkreten Beschwerdegegenstand beschränkt.

Hier musste häufig festgestellt werden, dass Datensicherheitsmängel bestanden, Weisungen nach § 11 BDSG fehlten und dass bei der Bestellung des Datenschutzbeauftragten nicht auf die erforderliche Fachkunde geachtet worden war.
In den Fällen der Videoüberwachung von öffentlich zugänglichen Bereichen musste festgestellt werden, dass die Maßnahme weder zur Wahrnehmung des Hausrechtes noch zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich war. In anderen Fällen lagen zwar die Voraussetzungen des § 6b Abs. 1 BDSG vor, aber die Kennzeichnungspflicht des § 6b Abs. 2 BDSG wurde missachtet.

2. Bearbeitung von Anfragen zu datenschutzrechtlichen Problemstellungen und Beratungstätigkeit

2.1 Anfragebearbeitung und datenschutzrechtliche Beratung

Die Aufsichtsbehörden hatten im Berichtsjahr erneut eine hohe Anzahl von Anfragen und Beratungsersuchen zu bearbeiten. In 199 Fällen (im Vorjahr: 187 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 werden bis auf wenige Ausnahmen nicht statistisch erfasst.

Die statistische Auswertung der eingegangenen 199 Fälle ergab folgende inhaltliche Schwerpunkte:

32 Anfragen zum Arbeitnehmerdatenschutz:

Private Nutzung von betrieblichen E-Mail- und Internet-Anschlüssen, Protokollierung und Auswertung der Online-Aktivitäten von Mitarbeitern, Einsichtnahme in E-Mails durch Kollegen und Vorgesetzte, Ausgestaltung von Betriebsvereinbarungen, Veröffentlichung von Mitarbeiterdaten am schwarzen Brett und im Intranet von Unternehmen, Privatnutzung von Firmenhandys, sichere Zustellung von Gehaltsabrechnungen im Betrieb, Aufzeichnung der Inhalte von Telefongesprächen.

28 Anfragen von und zum betrieblichen Datenschutzbeauftragten:

Voraussetzungen der korrekten Bestellung von betrieblichen Datenschutzbeauftragten, Probleme bei der Bestellung externer Datenschutzbeauftragter, Aufgaben des betrieblichen Datenschutzbeauftragten, Anspruch auf Schulung, Schulung der Mitarbeiter, Erstellung eines Verfahrensverzeichnisses nach § 4g Abs. 2 BDSG, Datenschutzbeauftragte in Apotheken und bei Rechtsanwälten, Inkompatibilität von Datenschutzbeauftragten und Geldwäschebeauftragten, Meldung zum Register nach §§ 4d und 4e BDSG.

25 Anfragen zum Datenschutz im Internet:

Zulässigkeit von Whois-Diensten, Speicherung von Log-Dateien durch Inhalteanbieter im WWW, Filtern und Löschen unverlangter Werbe-E-Mails (Spam), Gefahren durch Schadsoftware (Viren und Würmer), allgemeine Fragen zur Internetsicherheit, Formulierung von Datenschutzhinweisen in WWW-Angeboten nach § 4 Abs. 1 TDDSG, "Double-Opt-In"-Verfahren für Online erhobene E-Mail-Adressen im Sinne des § 4 Abs. 2 TDDSG, Handel mit E-Mail-Adressen und deren werbliche Nutzung, datenschutzgerechter Einsatz so genannter "cookies", kein Anspruch für Urheberrechtsinhaber auf Herausgabe von Kundendaten gegenüber Internet-Providern nach dem Urheberrechtsgesetz, Koppelungsverbot nach § 3 Abs. 4 TDDSG.

19 Anfragen zur Auslands-Datenverarbeitung:

Datentransfer innerhalb der Europäischen Union, insbesondere zur Frage des anwendbaren Rechts; vor allem aber Fragen zur Datenübermittlung an so genannte "Drittstaaten", d.h. an Staaten außerhalb der Europäischen Union und des Abkommens über den Europäischen Wirtschaftsraum, insbesondere im Zusammenhang mit dem Transfer von Arbeitnehmerdaten an

außereuropäische Konzern-Muttergesellschaften. Auch Fragen zur Auslagerung von Datenverarbeitungen an Datenverarbeitungsdienstleister in Drittstaaten (China, Indien) und zur Weitergabe von Daten an amerikanische Behörden, Gerichte und Rechtsanwälte. Fragen nach dem Erfordernis der Genehmigung durch die Datenschutzaufsichtsbehörde (s. auch unten Nr. 3).

18 Anfragen aus dem Gesundheitssektor:

Umfang der ärztlichen Schweigepflicht des Werksarztes, Auswertung anonymisierter Patientendaten für die Marktforschung, webbasierte elektronische Gesundheitsakte, Archivierung von Patientenakten, Aufbewahrung von Patientenunterlagen nach Praxisauflösung, Datenverarbeitung zur Qualitätssicherung ambulanter Folgebehandlungen, Erhebung von Gesundheitsdaten zur wissenschaftlichen Auswertung, Formulierung von Patienteneinwilligungen.

12 Anfragen zum Datenschutz bei Banken:

Werbliche Nutzung von Bankdaten, Formulierung von Einwilligungserklärungen und Klauseln, Nutzung des Verwendungszwecks auf Buchungsbelegen, Geldwäschebeauftragter, Weitergabe von Kundendaten an Inkassounternehmen, Telefonbanking.

8 Anfragen zur Datenverarbeitung durch Vereine und Dachverbände:

Anfragen zur Zulässigkeit der Datenverarbeitung des Deutschen Fußball-Bundes anlässlich der Fußball-WM 2006 (s. unten Nr. 11), Veröffentlichung von Mitgliederdaten und -bildern im Internet, Errichtung einer zentralen Mitglieder-Datenbank, Daten über die Erkrankung bekannter Sport-Profis, Abschluss von Gruppenversicherungsverträgen zwischen Versicherungen und Dachverbänden.

7 Anfragen zur Meldepflicht nach §§ 4d, 4e BDSG:

Gesetzliche Voraussetzungen für die Meldung bei der Datenschutzaufsichtsbehörde, Fragen zum Umfang der Angaben nach § 4e BDSG und zur Nennung des betrieblichen Datenschutzbeauftragten im Rahmen der Meldepflicht.

7 Anfragen zu Handels- und Wirtschaftsauskunfteien:

Beratung von Handels- und Wirtschaftsauskunfteien zu datenschutzrechtlich zulässigen Verarbeitungen und Übermittlungen, Einrichtung zentraler branchenspezifischer Hinweissysteme, unzulässiger Aufbau und Betrieb diverser schwarzer Listen und Warndateien, insbesondere auch im Internet (s. Nr. 8.1 und 8.2).

6 Anfragen zum Datenschutz durch Technik:
Beratung bei Anfragen zum Schutz vor dem Abhören von Telefonaten, sicherer Betrieb von Funknetzen, sichere Übermittlung personenbezogener Daten durch geeignete Verschlüsselungsverfahren, sicherer WLAN-Betrieb, Abwehr von Angriffen auf betriebliche Kommunikationsstrukturen durch Hacker, Maßnahmen gegen Betriebsspionage, sicherer Umgang mit erhobenen biometrischen Daten.

5 Anfragen zur SCHUFA:

Grundsätzliches zur weitgehend unbekannten Arbeitsweise der SCHUFA und ihrer Vertragspartner, wie z.B. zu Löschfristen, zum SCHUFA-Scoring sowie zur SCHUFA-Selbstauskunft und deren Kosten.

5 Anfragen zur Videoüberwachung:

Beobachtung von Straßen, Gehwegen, Grundstückszufahrten, Wohnanlagen, Hausfluren und Treppenhäusern, Video-Aufzeichnungen in Nachbarschaftsstreitigkeiten, Fragen zu Löschfristen, zur Ausgestaltung des nach § 6b Abs. 2 BSDG erforderlichen Hinweises auf die Videobeobachtung, Überwachung des Behandlungszimmers einer Arztpraxis, Umgang mit der Videobeobachtung vor und in einem Gebäude mit Eigentumswohnungen (s. auch unten Nr. 12).

4 Anfragen zur Werbewirtschaft:

Informationen über die grundsätzliche Zulässigkeit des Adresshandels im Rahmen der §§ 28, 29 BDSG, Beratung zum Recht auf Auskunftserteilung nach § 34 Abs. 1 BDSG und Informationen zum Werbewiderspruch nach § 28 Abs. 4 BDSG sowie zur Löschung bzw. Sperrung von Daten, Beratung von Unternehmen zur Umsetzung der Pflicht zur Unterrichtung der Betrof-

fenen nach § 4 Abs. 3 BDSG, datenschutzrechtliche Besonderheiten der Couponwerbung.

2 Anfragen aus dem Bereich Miete und Wohnen:

Datenverarbeitung durch eine Hausverwaltung im Auftrag der Eigentümerversammlung zur Energiekostenoptimierung und -bezahlung, sichere elektronische Erfassung und Abrechnung von hausinternen Service-Dienstleistungen zur Verhinderung von Missbrauch durch Miteigentümer bzw. Mieter.

2 Anfragen zur Versicherungsbranche:

Datenschutzrechtlich zulässiger Umgang mit so genannten "Rennlisten", Formulierung und Tragweite von Einwilligungsklauseln.

Die weiteren Anfragen und Beratungsersuchen, die mit ihrem breiten Spektrum sehr anschaulich widerspiegeln, dass Datenschutzaspekte in der heutigen Informationsgesellschaft in fast jedem Lebensbereich der Bürgerinnen und Bürger eine Rolle spielen können, betrafen unter anderem die Markt- und Meinungsforschung, die Reise- und Touristikbranche, das Speditions- und Transportgewerbe, den Versandhandel, Inkassounternehmen, den Groß- und Einzelhandel, die Auftragsdatenverarbeitung bei der Fernwartung und Fernsicherung, die Veröffentlichung von Namensbüchern und Stammbäumen, den Umgang mit Personalausweisdaten sowie den Datenschutz in Rechtsanwaltskanzleien und bei Kfz-Sachverständigen.

2.2 Informationsmaterial und Orientierungshilfen

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

Auch die Homepage des Datenschutzdezernats beim Regierungspräsidium Darmstadt im Internet (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 wurden drei Genehmigungsanträge für die Übermittlung personenbezogener Daten in so genannte "Drittstaaten" gestellt.

In zwei Fällen konnte jedoch noch keine Entscheidung ergehen, weil die antragstellenden Unternehmen selbst noch weitere Klärungen vornehmen werden. In einem Fall gab hier die Beratung durch das Regierungspräsidium Darmstadt Veranlassung, die Verteilung der Verantwortlichkeiten im Konzern genauer zu beleuchten, im anderen Fall führten wesentliche Änderungen innerhalb des Konzerns dazu, das Genehmigungsverfahren zunächst ruhen zu lassen.

Im dritten Fall entschied sich das antragstellende Unternehmen schließlich, die EU-Standardvertragsklauseln vom Juni 2001 wörtlich zu verwenden, so dass die Genehmigungspflicht entfiel.

Eine Genehmigungspflicht besteht auch dann nicht, wenn die von der EU-Kommission anerkannten alternativen Standardvertragsklauseln (Entscheidung der EU-Kommission vom 27. Dez. 2004) verwendet werden; dies war Gegenstand zahlreicher Anfragen. Das Regierungspräsidium Darmstadt verwies hier auf die Ausführungen im 15. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden (Drucks. 15/4659, Nr. 7.2), die auch für diese alternativen Standardvertragsklauseln gelten.

4. Register der meldepflichtigen Verfahren nach § 4d BDSG

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

Am Ende des Berichtsjahres waren 95 Verfahren von 91 verantwortlichen Stellen im Melderegister eingetragen. Wie sich aus diesen Zahlen ergibt, haben nur vier verantwortliche Stellen mehr als ein Verfahren gemeldet.

Davon werden in 46 gemeldeten Verfahren geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung gespeichert (Adresshändler, Handels- und Wirtschaftsauskunfteien, meldepflichtig nach § 4d Abs. 4 Nr. 1 BDSG). 49 der eingetragenen Verfahren dienen dem Zwecke der anonymisierten Übermittlung (Markt- und Meinungsforschung, meldepflichtig nach § 4d Abs. 4 Nr. 2 BDSG).

5. Ordnungswidrigkeitenverfahren

Im Berichtsjahr wurden vom Regierungspräsidium Darmstadt fünf Verfahren nach dem Gesetz über Ordnungswidrigkeiten (OWiG) eingeleitet, wie sich aus der nachfolgenden Übersicht ergibt:

nach § 43	Grund der Einleitung	Rechtskraft:	Bußgeld
Abs. 1 Nr. 10 BDSG	Nichterteilung von Auskünften	Nein	
Abs. 1 Nr. 10 BDSG	Nichterteilung von Auskünften	Nein	
Abs. 1 Nr. 2 BDSG	nichtige Bestellung eines betrieblichen DSB wegen Untätigkeit	Nein	
Abs. 2 Nr. 1 BDSG	unbefugte Verarbeitung	Nein	
Abs. 2 Nr. 1 BDSG	unbefugte Verarbeitung	Ja	3.000 €

In einem der Verfahren, das nach § 43 Abs. 1 Nr. 10 BDSG wegen der Nichterteilung von Auskünften an die Aufsichtsbehörde entgegen § 38 Abs. 3 Satz 1 BDSG gegen den Vorstandsvorsitzenden eines Finanzdienstleistungsunternehmens eingeleitet wurde, konnte diesem lediglich das Anhörungsschreiben zugestellt werden. Kurz darauf waren die Internet-Seiten des Unternehmens nicht mehr abrufbar und - wie sich bei einer Überprüfung vor Ort herausstellte - auch die angemieteten Büroräume komplett leer geräumt. Da weder im Handels- noch im Gewerberegister Eintragungen vorhanden waren und auch der Vermieter keine Angaben zum Verbleib der Firma machen konnte, wurde das Verfahren eingestellt.

In einem weiteren Fall wurde bei der Bearbeitung einer Beschwerde gegen ein Unternehmen, das sein Lottotipp-System per Telefonmarketing vertreibt, der Geschäftsführer des Unternehmens aufgefordert, der Datenschutzaufsichtsbehörde die für die werbliche Nutzung der Telefonnummer des Petenten datenschutzrechtlich und wettbewerbsrechtlich erforderliche Einwilligungserklärung zur Überprüfung vorzulegen. Der Geschäftsführer vertrat zunächst die Auffassung, dass sich die Datenschutzaufsichtsbehörde diese Einwilligungserklärung selbst bei dem Adresshändler beschaffen solle, von dem auch er die Daten erhalten hatte. Die Einleitung eines Bußgeldverfahrens nach § 43 Abs. 1 Nr. 10 BDSG führte zu einem umgehenden Sinneswandel. Die Einwilligungserklärung wurde vorgelegt und es wurde zugesichert, dass bei künftigen Fällen eine sofortige Erledigung der Anforderungen der Aufsichtsbehörde erfolgen wird. Das Verfahren wurde daher im Rahmen der pflichtgemäßen Ermessensausübung nach § 47 Abs. 1 OWiG eingestellt.

Bei der unangemeldeten Überprüfung eines Service-Unternehmens in Frankfurt am Main musste der prüfende Aufsichtsbeamte feststellen, dass der betriebliche Datenschutzbeauftragte des Unternehmens seit Jahren keine ausreichende Tätigkeit entfaltet hatte und auch die Fragen zu den datenschutzrechtlichen Anforderungen an seine Tätigkeit und an sein Fachwissen nicht ausreichend beantworten konnte, obwohl es sich um einen Juristen und Informatiker handelte. Da er während der Prüfung vor Ort weder Kooperationsbereitschaft noch Einsicht bezüglich seiner Versäumnisse und seiner mangelhaften Fachkunde zeigte, wurde gegen den Geschäftsführer des Unternehmens ein Bußgeldverfahren nach § 43 Abs. 1 Nr. 2 BDSG wegen der Nichtigkeit der Bestellung seines untätigen und inkompetenten betrieblichen Datenschutzbeauftragten eingeleitet. Nachdem die Geschäftsführung auf diese drastische Art und Weise von den Defiziten im betrieblichen Datenschutz ihres Hauses erfahren hatte, wurde dieser betriebliche Datenschutzbeauftragte von seinen Aufgaben entbunden und eine kompetente externe Datenschutzbeauftragte bestellt. Diese setzte sich umgehend mit der Aufsichtsbehörde bezüglich ihrer Tätigkeit in Verbindung und begann unverzüglich, die Versäumnisse aufzuarbeiten. Das Verfahren wurde vor diesem Hintergrund unter Zurückstellung von Bedenken im Rahmen der pflichtgemäßen Ermessensausübung nach § 47 Abs. 1 OWiG eingestellt.

In einem weiteren Fall wurde einem Rechtsanwalt, der als Bevollmächtigter einer Vermieterin auftrat, die unzulässige Übermittlung personenbezogener Daten an den Arbeitgeber des Mietschuldners vorgeworfen. Da sich der Rechtsanwalt zunächst nicht sehr kooperativ zeigte, eine Dienstaufsichts- und Fachaufsichtsbeschwerde einlegte und unter Berufung auf sein Auskunftsverweigerungsrecht auch keine ihn entlastenden inhaltlichen Angaben zur Sache machen wollte, wurde ein Verfahren nach § 43 Abs. 2 Nr. 1 BDSG gegen ihn eingeleitet. Wie sich im Verlauf der weiteren Sachverhaltsermittlungen herausstellte, hatte sich der Mietschuldner bereits zuvor mit der Datenübermittlung an seinen Arbeitgeber einverstanden erklärt und seiner Vermieterin sogar die dortigen Kontaktdaten genannt, dies aber der Aufsichtsbehörde verschwiegen. Das Verfahren war daher einzustellen.

Aufgrund der Eingabe eines Steuerberatungsbüros, in der angegeben wurde, dass von einem Konkurrenten unbefugt Mandantendatensätze kopiert worden seien, wurde der Beschuldigte unangemeldet in seinem Büro aufgesucht und zu den Vorwürfen befragt. Da dieser Steuerberater zunächst alle Vorwürfe abstritt, wurde die EDV-Anlage des Steuerberaterbüros nach betriebsfremden Datensätzen durchsucht. Noch während der Einsichtnahme in die EDV nach § 38 Abs. 4 BDSG wies der Betroffene alle Anschuldigungen zurück. Erst als die Daten fremder Mandanten auf dem Bildschirm auftauchten, musste er einräumen, dass der Tatvorwurf der Wahrheit entsprach. Da es sich hierbei um eine unbefugte Verarbeitung nach § 43 Abs. 2 Nr. 1 BDSG handelte und der Steuerberater sowohl gegen die Verpflichtung auf das Datengeheimnis nach § 5 BDSG als auch gegen seine Geheimhaltungsverpflichtung nach dem Steuerberatungsgesetz verstoßen hatte, wurde eine Geldbuße in Höhe von 3000 € festgesetzt. Der Bußgeldbescheid hat inzwischen Rechtskraft erlangt.

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

Ausgesuchte Probleme und Einzelfälle

6. Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA)

6.1 Bestrittene Daten

Von Anfang an substantiiert bestrittene Daten, zumeist handelt es sich um bestrittene Forderungen, dürfen von den Vertragspartnern der SCHUFA nicht eingemeldet werden. Dies ist in den Technischen Anleitungen für das SCHUFA-Verfahren, die den Vereinbarungen zwischen der SCHUFA und ihren Vertragspartnern zugrunde liegen, entsprechend geregelt.

Entgegen manchen Bestrebungen gilt dies auch im Telekommunikationsbereich und wird auch von dem für Telekommunikationsunternehmen zuständigen Bundesbeauftragten für den Datenschutz so vertreten.

Dieser Grundsatz wird auch nicht durch eine Entscheidung des Oberlandesgerichts Frankfurt am Main (Az. 23 U 155/03 vom 19. November 2004) aufgehoben, das die Einmeldung einer umstrittenen geringfügigen Teilforderung für zulässig hielt, weil die besonderen Umstände des Einzelfalls eindeutig für eine ungerechtfertigte Zahlungsverweigerung sprachen. In diesem Fall hatte der Betroffene, entgegen seiner eigener Ankündigung, auch den weitaus überwiegenden, unbestrittenen Teil der Forderung nicht beglichen. Das Zivilgericht kam zu dem Schluss, dass in diesem besonderen Einzelfall das Interesse der SCHUFA-Vertragspartner, von der Zahlungsunwilligkeit des Betroffenen im Falle einer Geschäftsbeziehung mit ihm Kenntnis zu nehmen, das Interesse des Betroffenen an der Geheimhaltung der Negativdaten überwog und eine Übermittlung der Daten durch die SCHUFA daher rechtmäßig war.

Im Rahmen von Beschwerden über SCHUFA-Einträge machten Beschwerdeführer immer wieder geltend, dass sie gegen sich gerichtete Forderungen substantiiert bestritten hätten, dennoch hätten die Geschäftspartner solche

Forderungen bei der SCHUFA eingemeldet. In Fällen, in denen dies geschah, rechtfertigten sich die einmeldenden Kreditinstitute und Telekommunikationsunternehmen damit, dass Einwände übersehen worden seien bzw. automatisierte Abläufe zur unzulässigen Einmeldung geführt hätten.

Die SCHUFA löschte diese Einmeldungen nach eigener Prüfung und bestätigte zumeist, dass sie ihrem Vertragspartner nochmals die oben erwähnten Vorgaben der Technischen Anleitung deutlich gemacht habe.

Die Aufsichtsbehörde forderte die betroffenen, im Aufsichtsbezirk ansässigen SCHUFA-Vertragspartner auf, ihre technischen und organisatorischen Maßnahmen dahingehend zu ändern, dass solche unzulässigen Einmeldungen zukünftig unterbleiben. Die Fälle von Vertragspartnern außerhalb des Aufsichtsbezirks wurden an die zuständigen Aufsichtsbehörden zur weiteren Prüfung abgegeben.

Tritt ein Fehler auf, ist insbesondere bei automatisierten Abläufen zu prüfen, ob diese Verfahren den datenschutzrechtlichen Anforderungen gerecht werden.

Eine Datenübermittlung an eine Kreditschutzorganisation wie die SCHUFA setzt nach § 28 Abs. 1 Nr. 2 und Abs. 3 Nr. 1 BDSG grundsätzlich eine Interessenabwägung durch die übermittelnde Stelle (Bank, Kreditkartenunternehmen etc.) voraus. Dieser Interessenabwägung wird - je nach der Art der zu übermittelnden Daten - ein automatisiertes Übermittlungsverfahren nicht gerecht (Landgericht Stuttgart, Urteil vom 15. August 1997, Az. 9 S 145/97).

Bei einem Kreditkartenunternehmen offenbarte ein Beschwerdefall deutliche Defizite. Obwohl eine Kundin mehrfach, sogar durch ein Gerichtsverfahren, die erneute Übersendung der Kreditkartenabrechnung für einen bestimmten Monat gefordert hatte, da ihr diese nicht zugegangen sei, erfolgte eine Meldung an die SCHUFA.

Die Erkenntnisse aus der Beschwerdebearbeitung und der Prozessführung, bei der das Kreditkartenunternehmen sich zur erneuten Übersendung der Abrechnung bereit erklärte, führten nicht dazu, dass Einfluss auf das automatisierte Verfahren genommen wurde.

In diesem Fall war es daher nicht damit getan, dass der Fehler bedauert und die Löschung bei der SCHUFA veranlasst wurde. Auf Forderung der Aufsichtsbehörde initiierte die betriebliche Datenschutzbeauftragte des Kreditkartenunternehmens eine Prüfung der internen Verarbeitungsprozesse, worauf diverse Maßnahmen ergriffen wurden. Das Regierungspräsidium Darmstadt wird kritisch verfolgen, ob diese ausreichend sind.

Aber auch die SCHUFA ist gehalten, gegebenenfalls entsprechende Forderungen gegenüber ihren Vertragspartnern zu stellen.

Bei nachträglichem substantiierten Bestreiten einer Forderung, also nach Einmeldung der Forderung bei der SCHUFA, besteht die Aufsichtsbehörde darauf, dass eine Klärung des Sachverhalts entweder sofort erfolgt oder, wenn die Angelegenheit einer ausführlicheren Prüfung und Untersuchung beim Vertragspartner bedarf, der Hinweis "bestrittene Daten in Prüfung" angebracht wird.

Die Übermittlung dieses Hinweises wird von der Aufsichtsbehörde jedoch nur für einen begrenzten Zeitraum von höchstens vier Wochen akzeptiert, weil aus Beschwerden von Betroffenen bekannt ist, dass der Hinweis von einzelnen Vertragspartnern der SCHUFA wie ein Negativmerkmal gewertet wird, auch wenn er dies im eigentlichen Sinne nicht ist.
Die Frist gilt unabhängig davon, ob die Daten möglicherweise noch länger, z.B. bis zum Abschluss eines Klageverfahrens, gesperrt bleiben müssen.
Darüber hinaus muss die SCHUFA vor allem durch entsprechende vertragliche Regelungen (Prüf- und Meldepflichten) dafür sorgen, dass nachträgliches Bestreiten überhaupt durchgängig berücksichtigt wird, also nicht nur dann, wenn sich ein Betroffener direkt bei der SCHUFA beschwert.
Diesbezüglich muss noch eine Lösung gefunden werden.

6.2 Wiederkehrende Beschwerdeanlässe

In einigen Fällen beschwerten sich Betroffene über Personenverwechslungen. Beispielsweise wurden zwei Datensätze namensgleicher Personen mit

identischen Geburtsdaten bei der SCHUFA zusammengelegt. Die Wichtigkeit qualitätssichernder Maßnahmen wurde in diesen Fällen erneut deutlich. Zur Vermeidung von Verwechslungen brachte die SCHUFA Bearbeitungshinweise an, damit die Sachbearbeitung im Einzelfall vor einer Eigenauskunft oder einer Übermittlung von Daten an Dritte nicht versäumt, die tatsächliche Identität des Betroffenen zu klären.

Nachfolgend einige Beispiele für typische Fehler, die ihre Ursache bei den Vertragspartnern der SCHUFA hatten:

- Ein Kreditkartenunternehmen unterließ es, die Beendigung eines Kreditkartenvertrages einzumelden.
- Ein Kreditinstitut, das den Kauf von Pkws finanziert, unterließ es, die Erledigung eines Leasingvertrages einzumelden.
- Ein anderes Kreditinstitut verwechselte den Kreditnehmer mit einem namensgleichen Kunden und übermittelte dem Dritten sogar den Kfz-Brief, der dem Betroffenen zustand, weil es einen Umzug des Betroffenen annahm.
- Ein Kreditinstitut unterließ es, die Änderung der Forderungshöhe einzumelden, ein anderes löschte einen erledigten Kredit nicht.
- Kreditinstitute tätigten ohne Einwilligung der Betroffenen, in einem Fall sogar entgegen der ausdrücklichen Ankündigung des Kreditvermittlers, Anfragen an die SCHUFA.
- Bei einem Mobilfunkvertrag, der telefonisch zustande kam, übersah ein Telekommunikationsunternehmen, dass dabei keine Einwilligung in die SCHUFA-Klausel eingeholt worden war, und meldete zudem Forderungen aus Grundgebühren ein, die durch einen Fehler in der Sachbearbeitung entstanden waren. In diesem Fall zeigte sich, dass die Kündigung paralleler Telekommunikationsverträge durch den Kunden nicht richtig bearbeitet worden war.
- Ein Telekommunikationsunternehmen unterließ die Abmeldung eines Telekommunikationsvertrags nach ordentlicher Kündigung durch den Kunden.

Die Aufsichtsbehörde forderte neben der Aufklärung des Sachverhalts und der Berichtigung der Eintragungen auch grundsätzliche Maßnahmen der SCHUFA gegenüber ihren Vertragspartnern, damit solche Fehler zukünftig vermieden werden.

7. Banken

7.1 Authentifizierung mittels biometrischer Verfahren

Im Rhein-Main-Gebiet ist ein zu einem US-Konzern gehöriges Unternehmen ansässig, das ein interaktives Finanzinformationssystem betreibt. Banken auf der ganzen Welt nutzen dieses System, weil es integrierte Daten, Nachrichten, Analysen, Multimedia-Berichte und E-Mail auf einer einzigen Plattform anbietet. Das Kerngeschäft des Dienstleisters ist dabei die Bereitstellung von Finanzinformationen.

Dieses Unternehmen beabsichtigte nun, ein biometrisches Authentifizierungsverfahren einzuführen und hierfür Daten der Bankmitarbeiter, die das System nutzen, in den USA zu speichern.

Die Kritik von betrieblichen Datenschutzbeauftragten der Banken, die durch das Regierungspräsidium Darmstadt und andere Aufsichtsbehörden unterstützt wurde, führte zunächst dazu, dass die US-Muttergesellschaft eine Safe-Harbor-Zertifizierung vornahm.

Mit der Safe-Harbor-Zertifizierung waren jedoch nur die für den Drittstaatentransfer, das heißt den Datentransfer in Staaten außerhalb der Europäischen Union, geltenden besonderen Anforderungen des § 4b BDSG erfüllt. Zusätzlich war zu klären, ob die Datenverarbeitung überhaupt nach § 28 BDSG zulässig ist.

Die betrieblichen Datenschutzbeauftragten zahlreicher Banken aus dem ganzen Bundesgebiet hatten erhebliche Zweifel, ob diese Voraussetzungen erfüllt seien, und baten daher das Regierungspräsidium Darmstadt bzw. die für sie zuständigen Aufsichtsbehörden in Baden-Württemberg, Bayern und Nordrhein-Westfalen um Beratung.

Daraufhin lud das Regierungspräsidium Darmstadt den Finanzdienstleister sowie die anderen Aufsichtsbehörden und die Banken zu einer Besprechung ein.

Die Vertreter des Dienstleisters erläuterten das geplante Verfahren. Aus Merkmalen der Fingerkuppe der Nutzer sollte eine Binärzahl generiert und diese verschlüsselt in die USA übermittelt werden, wobei die Verschlüsselung durch ein anderes Unternehmen erfolgen sollte.

Hintergrund sei die Einführung eines neuen Lizenzmodells. Während bisher gerätebezogene (terminal based) Lizenzen für die Nutzung der Informations-/Börsenhandelsplattform vergeben worden seien, sollen künftig nutzerbezogene (user based) Lizenzen vergeben werden. Damit wolle man insbesondere den Bedürfnissen der Kundschaft nach mehr Mobilität nachkommen. Um eine größtmögliche Sicherheit des Services sowie den Schutz der Anwenderdaten zu gewährleisten, sei das verbesserte Authentifizierungssystem eingeführt worden. Zunächst habe sich der Anwender gegenüber dem System durch Eingabe seines Login-Namens und Passworts zu erkennen zu geben. Anschließend werde ihm vom System das gespeicherte Referenzmuster zugeordnet und das System prüfe anhand der biometrischen Daten, ob er die behauptete Identität besitzt.

Die Vertreter des Dienstleisters räumten ein, dass es unter anderem um den Schutz vor Lizenzmissbrauch gehe. Sie verwiesen darauf, dass demgegenüber die Gefahr eines Missbrauchs der biometrischen Daten der Nutzer aufgrund des gewählten Verfahrens äußerst gering sei.

Ein Restrisiko eines Missbrauchs personenbezogener Daten ist bei diesem System jedoch vorhanden.
Jedenfalls findet eine Verarbeitung personenbezogener Daten statt, die sich am Erforderlichkeits- und Verhältnismäßigkeitsgrundsatz des § 28 Abs. 1 Nr. 2 BDSG und dem Grundsatz der Datenvermeidung und Datensparsamkeit des § 3a BDSG messen lassen muss. Daher war die Frage zu stellen, ob ein biometrisches Verfahren überhaupt erforderlich ist, d.h. ob eine Authentifizierung mittels Token (ohne biometrische Daten), User ID und Passwort nebst einer Dokumentation und Kontrolle der Berechtigung bei den Banken denn nicht genügt, um das Interesse des Dienstleisters an einem Schutz vor Missbrauch des neuen Lizenzsystems zu befriedigen. Der Dienstleister verneinte dies. Es seien sehr wohl Fälle von Lizenzmissbrauch bekannt geworden, die gezeigt hätten, dass diese Maßnahmen unzureichend seien. Ob diese Argumentation zwingend ist, konnte von den Aufsichtsbehörden nicht vollständig nachvollzogen werden.

Es stellte sich jedoch heraus, dass eine weitere technische Alternative zur Verfügung steht, die in Luxemburg bereits den Kunden angeboten wurde. Hierbei würden die biometrischen Daten, genauer die verschlüsselten Binärzahlen, nicht zentral in den USA gespeichert, sondern direkt auf einem kompakten, tragbaren Gerät von Kreditkartengröße, das im Besitz der Nutzer bleibt. Letztlich erklärte sich die Konzernleitung in den USA bereit, diese alternative Technik auch in Deutschland anzubieten.

Im Hinblick darauf, dass die Nutzer bei der dezentralen Speicherung nach bisherigen Erkenntnissen "Herr" über ihre biometrischen Daten bleiben, sind die Anforderungen an die Erforderlichkeit der Maßnahmen im Sinne des § 28 Abs. 1 Nr. 2, § 3a BDSG nicht zu überspannen bzw. zu relativieren.

Nachdem weitere Unterlagen zu dieser neuen Technik vorgelegt wurden, teilte das Regierungspräsidium Darmstadt, nach Abstimmung mit den anderen Aufsichtsbehörden, dem Dienstleister und den Banken mit, dass dieses Authentifizierungsverfahren mit dezentraler Speicherung akzeptiert werden könne, vorbehaltlich einer etwaigen neuen Bewertung, falls sich neue Erkenntnisse ergeben.

Da die berechtigten Interessen des Dienstleisters (Schutz vor Lizenzmissbrauch, Zugriffskontrolle) durch die dezentrale Lösung ebenso gut befriedigt werden wie durch zentrale Speicherung, ist die zentrale Speicherung nicht "erforderlich" i.S.d. § 28 Abs. 1 Nr. 2 BDSG und auch § 3a BDSG gebietet es, die "dezentrale Kartenlösung" vorzuziehen. Mit der Zustimmung zu der "dezentralen Kartenlösung" lehnten die Aufsichtsbehörden daher zugleich die geplante Lösung mit zentraler Datenspeicherung ab.

Das Regierungspräsidium Darmstadt stellte in Übereinstimmung mit den anderen Aufsichtsbehörden gegenüber dem Dienstleister außerdem klar, dass durch die Einholung von Einwilligungen der Nutzer grundsätzlich keine Rechtfertigung für die zentrale Datenspeicherung geschaffen werden kann.
Eine Einwilligung kann nur dann ausnahmsweise als Rechtsgrundlage akzeptiert werden, wenn es die Rahmenbedingungen bei den Kunden tatsächlich erlauben, dass die Nutzer bei Verweigerung der Einwilligung den Service weiterhin im Rahmen einer gerätebasierten Lizenz nutzen können. Da ein Kunde verständlicherweise wirtschaftliche Überlegungen anstellen und daher grundsätzlich auf Dauer keine Mischung der beiden Lizenzmodelle wählen wird, weil dies teurer sein dürfte, kann die Einwilligung grundsätzlich nur solange als Rechtsgrundlage in Betracht kommen, wie ein Kunde seinen Beschäftigten tatsächlich noch beide Lizenzsysteme anbietet.

Auch wenn der Dienstleister die beim Kunden bestehenden Verhältnisse nicht unmittelbar zu verantworten hat, muss er diese doch berücksichtigen. Der Dienstleister muss sich zumindest erkundigen, denn er ist als verantwortliche Stelle - so seine eigene Einstufung - auch dafür verantwortlich, dass nur wirksame Einwilligungen eingeholt werden.

Im Ergebnis ist festzuhalten, dass es aufgrund des Engagements der betrieblichen Datenschutzbeauftragten und der Unterstützung durch die Aufsichtsbehörden gelungen ist, eine datenschutzfreundliche Technik durchzusetzen.

7.2 Vorlage von Protokollen der Wohnungseigentümergemeinschaft zur Legitimation bei der Bank

Die gesetzlichen Regelungen des Geldwäschegesetzes verpflichten die Banken bei Konten, die von dem Kontoinhaber auf fremde Rechnung verwaltet werden, den Namen und die Anschrift desjenigen festzustellen, für dessen Rechnung gehandelt wird (§ 8 Abs. 1 GwG). Ein solches Konto für fremde Zwecke unterhält auch der Verwalter einer Wohnungseigentümergemeinschaft (WEG) für das Hausgeldkonto. Die einzelnen Eigentümer zahlen hierauf ihre monatlichen Betriebskostenvorauszahlungen ein.

Der Verwalter einer Wohnungseigentümergemeinschaft führte ein Hausgeldkonto bei einer Direktbank. Von der Bank wurde er unter pauschalem Hinweis auf Regelungen in der Abgabenordnung und dem Geldwäschegesetz aufgefordert, ein aktuelles Protokoll der Eigentümergemeinschaft zu übersenden. Der Verwalter hatte erhebliche Bedenken, dieser Aufforderung nachzukommen. Protokolle der Eigentümerversammlung enthalten über die Namensangaben der Eigentümer hinaus auch Feststellungen über die persönliche, familiäre und wirtschaftliche Situation von einzelnen Eigentümern. Probleme und Maßnahmen, die das Objekt betreffen, werden in diesen Niederschriften ebenfalls dargestellt. Der Verwalter war der Auffassung, dass die Bank hier Informationen über die persönlichen und wirtschaftlichen Verhältnisse erlangen kann, an die sie auf normalem Weg nie herankäme.

Er sah sich bereits durch seinen Verwaltervertrag und das Wohnungseigentümergesetz an der Übersendung der Protokolle gehindert, denn hier sei er zur Vertraulichkeit verpflichtet. Dies zeige sich schon daran, dass Versammlungen der Wohnungseigentümergemeinschaften nicht öffentlich sind. Er fragte darüber hinaus auch nach der Rechtsgrundlage, wonach die Bank diese umfangreiche Datenerhebung durchführen darf.

Seine Bedenken legte der Beschwerdeführer der Bank ausführlich dar und fragte nach, ob nicht eine Liste mit den Namen der Eigentümer ausreichend sei.
Die Bank forderte jedoch, ohne auf seine Intervention einzugehen, erneut die Übersendung des Protokolls der Eigentümerversammlung und drohte bei Nichterfüllung die Beschränkung der Verfügungsmöglichkeit des Verwalters für seine Konten an.

Auf Nachfrage der Aufsichtsbehörde stellte sich heraus, dass die Bank sich generell bei Konten von Wohnungseigentümergemeinschaften die benötigten Daten durch Vorlage von aktuellen Protokollen beschaffte. Hierfür gibt es weder eine Ermächtigung in der Abgabenordnung, dem Geldwäschegesetz oder einer entsprechenden Ausführungsbestimmung. Die Anforderung von Eigentümerprotokollen mit den umfangreichen persönlichen Daten verstößt zudem gegen § 3a BDSG, den Grundsatz der Datenvermeidung und Datensparsamkeit. Für die nach dem Geldwäschegesetz geforderte Feststellung des

wirtschaftlich Berechtigten genügt die Vorlage einer Aufstellung, die sich auf den Namen und die Anschrift der Eigentümer beschränkt. Nach Beanstandung durch die Aufsichtsbehörde änderte die Bank das Verfahren.

7.3 Aktualisierung von Kundenadressen durch externes Unternehmen

Der Petent erhielt einen Anruf eines Bankkunden mit gleichlautendem Familiennamen, der ihm mitteilte, er habe eine Zinsmitteilung zugesandt bekommen, die offensichtlich für den Betroffenen bestimmt sei. Die Benachrichtigung der Bank war adressiert mit den Vornamen des Betroffenen und seiner Frau, dem identischen Familiennamen, gerichtet an die Anschrift des Anrufers. Da der Beschwerdeführer und seine Frau seit über 30 Jahren an dem gleichen Ort wohnten, war die Adressänderung, die die Bank ohne Rücksprache mit den Kunden durchgeführt hatte, nicht erklärbar. Auf Nachfrage bei der Bank stellte sich heraus, dass diese eine Überprüfung der Adressen ihrer Kunden durch ein Dienstleistungsunternehmen der Post hatte durchführen lassen. Hierbei wurden die Adressdaten der Bank mit der Umzugsdatenbank des Dienstleisters abgeglichen.

Die der Bank übermittelten Prüfergebnisse wurden aber offensichtlich fehlerhaft interpretiert. Im konkreten Fall stimmten die Daten des Dienstleisters mit denen der Bank nur annähernd überein. Erforderlich in einem solchen Fall ist eine manuelle Nachbearbeitung. Diese ist allerdings nicht erfolgt. Ohne kritische Prüfung wurden die neuen Daten übernommen. Eine Nachfrage bei den Kunden ist unterblieben.

Die Bank hat umgehend, um weitere fehlerhafte Zusendungen von Bankpost zu vermeiden, bei allen nicht vollständig übereinstimmenden Adressabgleichen die abgeänderten Adressen auf den ursprünglichen Datenbestand zurückgesetzt.

7.4 Kontoangaben des Überweisenden im Kontoauszug des Zahlungsempfängers

Kontodaten sind sensible Daten, deren Weitergabe der Inhaber auf das notwendige Maß beschränken will. Hinweistafeln in Bankfilialen weisen z.B. darauf hin, zur Vermeidung von Missbrauch keine Kontoauszüge in die Papierkörbe zu werfen.
Im Überweisungsverkehr werden typischerweise zur Ausführung des Zahlungsauftrags die Angaben des Begünstigten, dessen Bankverbindung, ein Geldbetrag und in der Regel ein Verwendungszweck benötigt (§ 676a Abs. 1 BGB). Soll die Überweisung von einem Konto erfolgen, benötigt die ausführende Bank die Kontodaten des Überweisenden. Dem Zahlungsempfänger reichen zur Zuordnung des Zahlungseinganges der Name des Absenders, Verwendungszweck und der Geldbetrag aus. Die Angabe der Kontonummer und der Bankleitzahl des Überweisenden durch Ausdruck im Kontoauszug des Empfängers sind Informationen, die dieser nicht benötigt. Sie dienen primär der Bank, die im Reklamationsfall eine Rücküberweisung nur mit Vorlage des Kontoauszuges tätigen kann, ohne weitere Unterlagen heranziehen zu müssen.

Wie bereits im 13. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden (Drucks. 15/1539, Nr. 5.5) ausgeführt, ist es mit den Anforderungen von Datenschutz und Bankgeheimnis nicht vereinbar, wenn die Kontodaten des Überweisenden im Kontoauszug des Empfängers ausgedruckt werden. Ein Kreditinstitut hat seine bisherige Praxis nach der damaligen Intervention der Aufsichtsbehörde zwischenzeitlich geändert.

7.5 Kundenbefragung bei Banken

Um die Zufriedenheit ihrer Kunden mit dem Leistungsangebot und dem Service des Hauses zu prüfen, veranlasste eine Bank eine Umfrage. Die Interviews und die Auswertung der Ergebnisse nahm ein hierauf spezialisiertes Markt- und Meinungsforschungsinstitut im Wege der Auftragsdatenverarbeitung nach § 11 BDSG vor (vgl. hierzu 13. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Drucks. 15/1539, Nr. 5.4). Die Information der Kunden über die bevorstehende Telefonaktion erfolgte durch die Bank selbst, verbunden mit dem Hinweis, dass sie der Weitergabe ihrer Daten an das Institut widersprechen können.

Die Beschwerdeführerin wollte an der Marketingaktion nicht teilnehmen. Am übernächsten Tag nach Erhalt der Ankündigung der Bank widersprach sie schriftlich der Teilnahme und verlangte des Weiteren die Sperrung ihrer Daten auch für künftige Marketingaktionen. Vier Tage später rief das Marktforschungsinstitut bei der Beschwerdeführerin an, um diese nach ihrer Meinung zu befragen. Nach weiteren vier Tagen erhielt die Betroffene die Eingangsbestätigung der Bank über ihren Widerspruch und die Bestätigung ihre Daten für weitere Werbeaktionen nicht zu nutzen.
Verärgert wendete sich die Beschwerdeführerin an die Aufsichtsbehörde.

Die Irritationen der Bankkundin waren durch eine zu gedrängte zeitliche Planung der Marketingaktion veranlasst. Die schriftliche Information der Kundin über die Telefonbefragung und die Weitergabe der Kundendaten an das Markt- und Meinungsforschungsinstitut erfolgten zeitgleich. Das Institut meldete sich bereits sechs Tage nach Erhalt des Briefes bei der Beschwerdeführerin. Obwohl diese unverzüglich nach Information durch die Bank der Teilnahme an der Telefonumfrage widersprochen hatte, konnte die Bank - auch bedingt durch arbeitsfreie Tage wie ein Wochenende und einen gesetzlichen Feiertag - die persönlichen Daten der Kundin weder von der Weitergabe an das Marktforschungsinstitut ausnehmen noch bei diesem rechtzeitig löschen lassen. Die Bank selbst erhielt das Widerspruchsschreiben erst nach dem Anruf des Marketingunternehmens bei der Kundin.

Durch einen ausreichend bemessenen Zeitpuffer zwischen der Information der Kunden und der Weitergabe der Daten an das Markt- und Meinungsforschungsinstitut wird die Verärgerung von Kunden vermieden. Bei der Zeitplanung eines solchen Projektes sollten z.B. Feiertage und Ferientermine berücksichtigt werden. Hiernach ist dann individuell, entsprechend den jeweiligen Voraussetzungen, eine angemessene Frist zwischen der Benachrichtigung der Kunden und der Datenweitergabe an das beauftragte Institut abzuwarten; diese sollte mindestens zwei Wochen betragen.
Die Bank erkannte das Problem und entschuldigte sich bei der Kundin. Der betriebliche Datenschutzbeauftragte der Bank sorgte dafür, dass alle beteiligten Stellen und verantwortlichen Bereiche in der Bank entsprechend informiert wurden und Vorsorge trafen, dass künftig eine angemessene zeitliche Planung erfolgt.

7.6 Kooperation zwischen Banken im Konzernverbund

Die Kundin einer Bank wandte sich an die Aufsichtsbehörde und teilte ihre Bedenken hinsichtlich einer möglichen Verwechslung ihrer kontoführenden Bank mit einer anderen Bank mit.

Es handelt sich um rechtlich selbständige Kreditinstitute, die zum gleichen Konzern gehören. Sie bieten ihre Bankgeschäfte in den gleichen Geschäftsräumen an. Die Einrichtung der Filiale sowie technische Geräte wie Kontoauszugsdrucker und Geldautomaten werden von den Kunden beider Banken gemeinschaftlich genutzt. An der Außenfassade der Filiale ist der identische Namensbestandteil beider Banken nebst einem Logo angebracht und nicht die vollständige rechtliche Firmenbezeichnung der beiden Banken.
Die Beschwerdeführerin beklagte, dass bei dieser Konstellation die Identität der Bank nicht zweifelsfrei offenbar werde. Der Kunde könne nicht erkennen, mit welcher Bank er ein Vertragsverhältnis eingehe bzw. ob er auch von dem Mitarbeiter "seiner" Bank beraten werde. Auch sei zu befürchten, dass die Kundendaten beliebig zwischen den beiden Banken ausgetauscht würden. Daher führte das Regierungspräsidium Darmstadt eine Prüfung in einer der größten Geschäftsstellen durch.

Die Aufsichtsbehörde legte hierbei besonderes Augenmerk auf die Einhaltung des § 4 Abs. 3 BDSG. Hiernach ist der Betroffene bei der Erhebung von personenbezogenen Daten über die Identität der verantwortlichen (erhebenden) Stelle, die Zweckbestimmung der Erhebung, Verarbeitung und Nutzung und die Kategorien von Empfängern zu unterrichten.
Diese Vorgabe wurde seitens der beiden Kreditinstitute beachtet. Kontoeröffnungsanträge, sämtliche Formulare des Zahlungsverkehrs, Vertragsvordrucke, die Visitenkarten der Mitarbeiter sowie das Preis- und Leistungsverzeichnis enthielten die exakte rechtliche Bezeichnung der jeweiligen Bank.

Technisch und organisatorisch ist sichergestellt, dass Kundenkontakte ausschließlich durch einen Mitarbeiter derjenigen Rechtseinheit erfolgen, mit

der der Kunde in Vertragsbeziehung steht. Jeder Mitarbeiter hat nur auf Kundendaten "seiner" Bank Zugriff.
Eine rechtseinheitenübergreifende Beratung und Betreuung findet nur statt, wenn der Kunde ausdrücklich eine entsprechende schriftliche Einwilligungserklärung abgegeben hat. Der Text dieser Verbundklausel basiert auf Absprachen, die schon vor Jahren zwischen den obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich und dem zentralen Kreditausschuss getroffen wurden. Angesichts dessen, dass es kein Konzernprivileg gibt (siehe auch unten Nr. 10) und im Hinblick auf das Bankgeheimnis darf eine Bank Kundendaten grundsätzlich nur mit Einwilligung weitergeben.

Die Aufsichtsbehörde konnte sich bei der Prüfung überzeugen, dass die beiden Kreditinstitute die Einhaltung dieser datenschutzrechtlichen Anforderungen durch entsprechende organisatorische und technische Arbeitsabläufe und Maßnahmen zur Auftragsdatenverarbeitung sichergestellt haben.

8. Handelsauskunfteien

8.1 Datenaustausch mit der Wohnungswirtschaft

Ob bzw. inwieweit Vermieter Bonitätsauskünfte über Mietinteressenten einholen dürfen, wurde in der Vergangenheit primär in Bezug auf die Beteiligung der Wohnungswirtschaft am SCHUFA-Verfahren erörtert (vgl. 16. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Drucks. 16/1680, Nr. 10.5).

Da das Problem jedoch auch andere Auskunfteien betrifft, wurde es im Düsseldorfer Kreis nun umfassender erörtert. Trotz kontroverser Diskussion bestand in wesentlichen Punkten Einigkeit.

Aus der Sicht des Datenschutzes sind auf branchenspezifische Daten beschränkte Auskunftssysteme vorzuziehen, bei denen die Daten gesicherte Rückschlüsse auf Mietausfallrisiken zulassen. Dies entspricht auch Vorstellungen, die zuletzt im Deutschen Bundestag diskutiert werden.

Eine uneingeschränkte Auskunft über bei branchenübergreifenden Auskunfteien gespeicherte Daten an potentielle Vermieter ist dagegen unzulässig.

Bei der Prüfung, in welchem Umfang nach § 29 BDSG an potentielle Vermieter personenbezogene Daten übermittelt werden dürfen, sind die schutzwürdigen Belange der Mietinteressenten im Hinblick auf die Bedeutung der Wohnung für die Lebensgestaltung in besonderer Weise zu berücksichtigen. Auskünfte über Eintragungen im Schuldnerverzeichnis sind stets zulässig.

Es bestehen auch Zweifel an der Zulässigkeit einer Beauskunftung aufgrund einer Einwilligung. Entsprechendes gilt auch für das Verlangen gegenüber dem Mietinteressenten auf Vorlage einer Selbstauskunft.

Die Diskussion, insbesondere über die konkrete Auslegung des § 29 BDSG, wird im Düsseldorfer Kreis fortgeführt werden.

Das Regierungspräsidium Darmstadt erhielt im Berichtsjahr mehrere Anfragen von Privatpersonen und Unternehmen, die Vermieterwarndateien errichten wollen.

Als zulässig sah die Aufsichtsbehörde die Beauskunftung folgender objektiv nachprüfbarer Negativmerkmale an:

- Daten aus öffentlichen Schuldnerverzeichnissen,
- rechtskräftige Titel zum Zahlungsverzug im Mietbereich,
- rechtkräftige Urteile zur fristlosen Kündigung wegen Zahlungsverzugs oder sonstiger Vertragsverletzungen,
- rechtskräftige Räumungsurteile wegen fristloser Kündigung.

Das Regierungspräsidium Darmstadt verwies im Übrigen auf die fortdauernden Diskussionen im Düsseldorfer Kreis und gab insbesondere bzgl. des Austausches weiterer Daten eine kritische Stellungnahme ab.

Zwei Unternehmer, die branchenspezifische Vermieterwarndateien betreiben wollen, haben bekundet, dass sie branchenspezifische Vermieterwarndateien

errichten wollen und sich zunächst auf die oben genannten Daten beschränken werden.

8.2 Spezielle Warndateien

Auch in diesem Berichtszeitraum wurden Anfragen zur datenschutzrechtlichen Zulässigkeit spezieller sonstiger Warndateien gestellt, bei denen die Initiatoren das Verfahren so geplant hatten, dass Prangerwirkungen und Missbrauchsgefahren dabei zumindest in Kauf genommen wurden.

In einem Fall wurde die Absicht bekundet, im Internet geschlossene Benutzergruppen einzurichten, um z.B. Kfz-Reparaturwerkstätten oder Handwerker allgemein, Betreiber von Internetshops oder sonstige Kaufleute vor säumigen Kunden zu warnen. Eine Geschäftsidee bezog sich sogar darauf, Arbeitgeber vor problematischen Arbeitnehmern zu warnen.

Die Anfragenden mussten darauf hingewiesen werden, dass sich solche Beauskunftungen an den Voraussetzungen für den Auskunfteibetrieb nach § 29 BDSG messen lassen müssen, was eine Reihe von technischen und organisatorischen Maßnahmen nach sich zieht. Insbesondere der Aufwand für die Einrichtung automatisierter Abrufverfahren nach § 10 BDSG so wie für die erforderlichen Schulungen und Kontrollen durch die Auskunftei wurden meist verkannt. Auskunfts- und Berichtigungsansprüche, Löschfristen, Zugangsberechtigungen sowie die Notwendigkeit der Bestellung eines betrieblichen Datenschutzbeauftragten mussten erläutert werden.

Ebenso deutlich musste darauf hingewiesen werden, dass nur objektiv nachprüfbare, für den Beauskunftungszweck relevante Negativmerkmale eingemeldet und diese nur beim Vorliegen konkreter berechtigter Interessen an die Vertragspartner übermittelt werden dürfen. Schließlich war den Anfragenden zu verdeutlichen, dass es nicht möglich ist, die Verantwortung für die korrekte Beauskunftung auf die Vertragspartner zu delegieren.

Die Anfragenden verzichteten unter den genanten Voraussetzungen auf die Umsetzung der geplanten Warndateien.

8.3 Adressenermittlung bei Meldeämtern als neue Dienstleistung

"Unbekannt verzogen" - mit dieser Mitteilung des Postzustellers erhalten Unternehmen häufig die an ihre Kunden versandten Rechnungen zurück.

Abhilfe kann eine Anfrage beim Einwohnermeldeamt verschaffen. Allerdings erfordert dies einen nicht unerheblichen Aufwand. Zunächst einmal muss das Unternehmen die Anschrift des zuständigen Einwohnermeldeamtes ermitteln. Dann sollte es, um schnell zu einer Auskunft zu gelangen, möglichst wissen, welche Gebühren jeweils fällig werden und welche Zahlungsweise in Betracht kommt. Die diesbezüglichen Regelungen sind im Bundesgebiet sehr unterschiedlich.

Ein im Rhein-Main-Gebiet ansässiges Unternehmen hatte hier die sehr erfolgreiche Geschäftsidee, sich auf solche Adressermittlungen zu spezialisieren.

Es berichtete dem Regierungspräsidium Darmstadt, dass der Anteil ausgebuchter Forderungen wegen "unbekannt verzogener Schuldner" jedes Jahr kontinuierlich ansteige, wie Untersuchungen zeigten. Es handele sich um ein Massenphänomen.

Das Unternehmen holt bei den Einwohnermeldeämtern so genannte "einfache Meldeauskünfte" (§ 34 Abs. 1 HMG) ein, also Auskünfte, die sich auf Vor- und Familienname sowie Anschrift beschränken und für jedermann auch direkt beim Einwohnermeldeamt erhältlich sind.

Um nicht innerhalb kürzester Zeit wegen der gleichen Person beim gleichen Einwohnermeldeamt anfragen zu müssen, speichert das Unternehmen die eingeholten Auskünfte für eine gewisse Zeit. Darum ist seine Dienstleistung nicht lediglich als Auftragsdatenverarbeitung nach § 11 BDSG, sondern als Auskunftstätigkeit nach § 29 BDSG einzuordnen.

Das Unternehmen erteilt keine Auskünfte an Privatpersonen, sondern nur an Unternehmen und Rechtsanwälte und nur, wenn ein berechtigtes Interesse an der Auskunft dargelegt wurde. Nach den Meldegesetzen ist dies für die

Einholung der einfachen Auskunft nicht erforderlich, aber nach § 29 Abs. 2 Nr. 1a BDSG für die Übermittlung aus der Datenbank.

Da das Unternehmen die Betroffenen ordnungsgemäß nach § 33 Abs. 1 Satz 2 BDSG von der erstmaligen Übermittlung benachrichtigt und es sich um Massengeschäft handelt, gehen ständig zahlreiche Anfragen von Betroffenen aus allen Bundesländern beim Regierungspräsidium Darmstadt ein. Bisher konnte in jedem Einzelfall ein berechtigtes Interesse an der Adressenübermittlung glaubhaft dargelegt werden. Das Unternehmen legte jeweils die entsprechenden Unterlagen der anfragenden Unternehmen bzw. Rechtsanwälte vor.

Wenn die betreffende Person vom Einwohnermeldeamt nicht eindeutig zuordenbar oder ermittelbar ist, muss eine weitere Anfrage erfolgen, und zwar die Anfrage nach dem Geburtsdatum und der Voranschrift. Hierbei handelt es sich um eine erweiterte Einwohnermeldeamts-Auskunft (§ 34 Abs. 2 HMG). Diese erfolgt durch manuelle Bearbeitung und Anfrage (unter Beifügung von Belegen für den Nachweis des berechtigten Interesses). Wenn das Einwohnermeldeamt mitteilt, dass eine Auskunftssperre besteht, erfolgt ebenfalls eine manuelle Anfrage. Die Antworten auf diese manuellen Anfragen werden nicht in der Datenbank gespeichert, sondern die Antwort wird unmittelbar an den Vertragspartner weitergeleitet. Dadurch wird den Anforderungen der Meldegesetze an die Erteilung von erweiterten Auskünften aus dem Einwohnermelderegister Rechnung getragen: Da diese nur im Hinblick auf das im Einzelfall konkret dargelegte berechtigte Interesse erteilt werden, dürfen sie auch nur für den betreffenden Einzelfall verwendet werden. Das Unternehmen ist nicht berechtigt, eigenmächtig zu entscheiden, ob in einem anderen gleich lautenden Fall ebenso ein berechtigtes Interesse besteht, da diese Entscheidung dem Einwohnermeldeamt obliegt.

Die Aufsichtsbehörde konnte sich durch Überprüfungen im Unternehmen überzeugen, dass das Unternehmen diese Beschränkungen beachtet.

Vertiefend zu erörtern ist lediglich, wie das Unternehmen den Anspruch der Betroffenen auf Auskunft über die Empfänger der Daten erfüllt bzw. in welchen Fällen die Auskunft unter Berufung auf das Geschäftsgeheimnis ausnahmsweise verweigert werden kann (§ 34 Abs. 1 BDSG).

Ob das dargestellte Geschäftsmodell des Unternehmens durch das Projekt RISER (Registry Information Service on European Residents) obsolet wird, bleibt abzuwarten. RISER ist ein Onlinedienst mit Sitz in Berlin, der helfen soll, im europäischen Binnenmarkt gesuchte Personen über die nationalen bzw. kleingliedrigen Melderegister zu finden. Dieser Dienst soll als Auftragsdatenverarbeitung nach § 11 BDSG gestaltet werden.

Auskünfte, die im Auftrag einer Person oder eines Unternehmens bei einem Einwohnermeldeamt eingeholt werden, sollen daher nur für diese eine Anfrage verwendet werden, also auch nicht für kurze Zeit gespeichert bleiben, um Anfragen zur gleichen Person beantworten zu können, die kurze Zeit später eingehen.

Die Konstruktion als Auftragsdatenverarbeitung ist grundsätzlich eine datenschutzfreundliche Lösung. Allerdings geht dies mit einem gewissen Verlust an Transparenz für die Betroffenen einher im Vergleich zum oben genannten Geschäftsmodell, denn bei RISER werden diese folglich nicht nach § 33 BDSG benachrichtigt.

8.4 Schuldnerermittlung im Zusammenhang mit dem elektronischen Lastschriftverfahren

Die oben genannte (Nr. 8.3) Auskunftei bietet auch eine Dienstleistung für Unternehmen an, die das elektronische Lastschriftverfahren einsetzen.
Wird bei Bezahlung an der Kasse mittels elektronischem Lastschriftverfahren eine Lastschrift nicht eingelöst, so muss der Händler mit dem dazugehörigen Beleg bei der Bank eine Auskunft über den Kontoinhaber einholen. Der Erlaubnistatbestand dieser Datenübermittlung ergibt sich aus der Einwilligung des Betroffenen auf dem Lastschriftbeleg. Die Dienstleistung der Auskunftei besteht nun darin, dass die Auskunftei in Vertretung, das heißt mit entsprechender schriftlicher Vollmacht, des Handelsunternehmens bei der jeweiligen Bank die Adressdaten ermittelt. Diese Datenverarbeitung ist völlig getrennt von der oben geschilderten Adressermittlung. Die Transak-

tionsbelege der nicht eingelösten Lastschriften, also die Original-Lastschriftbelege, werden vom Händler gesammelt und jeden Tag an die Auskunftei weitergegeben, von dieser durch Scannen erfasst und auf Datenträgern aufbereitet. Die Datenträger werden mit den Originalbelegen und der Vollmacht des jeweiligen Händlers an die Kreditinstitute weitergereicht. Sobald die Auskunftei die Adressen von den Banken erhalten hat, leitet sie diese an die jeweiligen Händler weiter.

Die Anschriften werden zugleich für kurze Zeit bei der Auskunftei gespeichert, aber dies nur, um etwaige Rückfragen der Händler beantworten zu können. Die Daten kommen nicht in einen Datenpool. Selbst wenn bei der Auskunftei zehn Anfragen am Tag zur gleichen Kontonummer und Bankleitzahl eingehen, startet die Auskunftei zehn Anfragen bei der Bank - es fallen also zehn Mal Bankgebühren an. Der Grund ist, dass die Bank eine Unterschriftenprüfung bei jedem Lastschriftbeleg macht; dies ist wichtig, um erkennen zu können, ob gestohlene bzw. gesperrte EC-Karten verwendet wurden.

Auch bei diesem Tätigkeitsgebiet des Unternehmens, das letztlich keine Auskunfteitätigkeit nach § 29 BDSG darstellt, ergaben sich im Ergebnis keine Beanstandungen.

8.5 Zentrale Sperr-/Warndatei für das elektronische Lastschriftverfahren

Das oben genannte Unternehmen (Nr. 8.3, 8.4) plant eine weitere Dienstleistung und bat die Aufsichtsbehörde um datenschutzrechtliche Beratung und Stellungnahme. Es will eine zentrale Sperr- und Warndatei errichten, um Handelsunternehmen einen Schutz vor Schuldnern zu bieten, die das elektronische Lastschriftverfahren missbrauchen, weil sie die Karte gestohlen haben oder weil kein Guthaben vorhanden ist und die Lastschriften somit nicht eingelöst werden. Die Kunden sollen die Wahl haben, ob sie nur die oben genannte (Nr. 8.4) Dienstleistung in Anspruch nehmen oder sich auch an der zentralen Sperr-/Warndatei beteiligen. Die Verarbeitungen sind insoweit getrennt.
Mehrere Varianten der Sperr-/Warndatei wurden ins Auge gefasst.

Als relativ unproblematisch bewertete die Aufsichtsbehörde eine reduzierte Form der Warndatei, bei der die übermittelten Daten auf die Bankleitzahl, die Kontonummer und die Kartenfolgenummer begrenzt werden und die angeschlossenen Partner verpflichtet werden, Veränderungen sofort in das Schutzverfahren einzumelden, z.B. wenn der entsprechende Betrag bezahlt ist. Ist die Zahlung erfolgt, so muss die bestehende Forderung in dem Datenbestand gelöscht werden und die angeschlossenen Teilnehmer erhalten umgehend eine Änderungsmeldung in Form einer Nachmeldung. Erfolgen keine Veränderungsmeldungen, so soll nach spätestens 360 Tagen eine Rückfrage bei den Händlern erfolgen.
Die Standard-Einwilligungserklärung auf der Rückseite der Lastschriftbelege reicht allerdings nicht aus, sondern müsste ergänzt werden.

In der Einwilligungserklärung müssten die zur Übermittlung vorgesehenen Datenarten konkret angegeben werden. Ferner müsste der Kreis der Empfänger ersichtlich sein.
Zu diesem Zweck sollen alle angeschlossenen Unternehmen ein bestimmtes Logo verwenden. Um den Kunden zu signalisieren, dass diese Unternehmen an dem Verfahren beteiligt sind, könnte in der Einwilligungsklausel hierauf Bezug genommen werden. Zusätzlich wäre eine Auflistung der beteiligten Unternehmen auf einer Website zu erwägen.

Außerdem müsste selbstverständlich die Auskunftei selbst in der Einwilligungsklausel genannt werden.

Die Auskunftei hatte ferner die Idee, in den Fällen, in denen letztlich doch noch eine Bezahlung erfolgt, eine weitere Speicherung für 6 bis 12 Monate (mit dem Merkmal der Bezahlung) vorzunehmen. Sie erläuterte das Interesse der beteiligten Unternehmen, da durch derart verzögerte Zahlungen erhebliche Kosten (insbesondere Rücklastgebühr) entstehen. Für die betroffenen Kunden könne sich berechtigterweise der Lernprozess ergeben, dass das elektronische Lastschriftverfahren keine Kreditkartenfunktion hat und es deshalb kein schutzwürdiges Interesse an verzögerter Einlösung von Lastschriften gibt.

Andererseits besteht das Problem, dass verzögerte Einlösungen möglicherweise darauf beruhen können, dass zunächst Einwendungen gegen das Grundgeschäft getätigt wurden (mangelhafte oder unvollständige Ware), die sofort durch das Unternehmen behoben wurden (z.B. durch Umtausch), sodass der Kunde den Widerspruch gegen die Lastschrift zurückzieht. Wenn das Handelsunternehmen es hier versäumte, diesen berechtigten Widerspruch unverzüglich an die Auskunftei zu melden, wäre der Kunde trotz "Bezahlvermerk" ungerechtfertigt belastet, wenn die Daten der Karte für 6 bis 12 Monate in der Sperr-/Warndatei bleiben.

Die Aufsichtsbehörde empfahl daher, dass nur das oben genannte "Grundmodell" der Warndatei verwirklicht werden sollte.

8.6 Datenklau bei der Bundesagentur für Arbeit?

Ein Fernsehjournalist äußerte gegenüber dem Regierungspräsidium Darmstadt den Verdacht, dass die Auskunftei, deren Haupttätigkeitsgebiet oben (Nr. 8.3) beschrieben wurde, sich auf unzulässige Weise Kenntnis von Daten verschafft habe, die nur von der Bundesagentur für Arbeit stammen könnten.

Dieser Verdacht gründete sich auf die Aussage einer Person, wonach deren Gläubiger von der Auskunftei nicht nur die Mitteilung erhalten habe, dass die betreffende Person arbeitslos gemeldet sei, sondern auch die Nummer erhalten habe, unter der die Registrierung bei der Bundesagentur für Arbeit erfolgt sei. Leider war der Journalist nicht bereit, die entsprechenden Unterlagen zu übergeben, obwohl dies die Aufklärung des Vorwurfs erleichtert hätte. Die Aufsichtsbehörde hatte die Auskunftei ca. 1,5 Jahre zuvor überprüft und dabei das oben (Nr. 8.2 und 8.3) beschriebene Tätigkeitsgebiet kontrolliert, wobei es keine Beanstandungen gegeben hatte. Aufgrund des vom Journalisten geäußerten Verdachts führte die Aufsichtsbehörde nun erneut eine sehr umfangreiche Überprüfung der gesamten Tätigkeit durch. Die Überprüfung erfolgte unangemeldet und ohne dem Geschäftsführer den Verdacht und damit den Anlass der Überprüfung mitzuteilen.

Bei der Überprüfung bestätigten sich zunächst die bisherigen Erkenntnisse über die oben genante Geschäftsgegenstände. Ferner stellte sich heraus, dass das Unternehmen nun einige Sonderdienstleistungen anbot, nämlich die Erteilung von Auskünften im Rahmen von Erbenermittlungen, Arbeitgeberermittlungen, Vollstreckungsauskünfte über Privatpersonen, etc. Diese Sonderdienstleistungen machen insgesamt nur einen sehr geringen Teil der Geschäftstätigkeit aus. Die Auskunftei wird hier auch nur als Vermittler von Dienstleistungen anderer Unternehmen tätig.

Wenn ein Unternehmen oder Rechtsanwalt eine titulierte Forderung beitreiben möchte, beschafft die Auskunftei bei entsprechendem Nachweis des berechtigten Interesses die Information, ob der Schuldner angestellt oder Lohnempfänger ist (gegebenenfalls unter Angabe des Arbeitgebers) oder ob er Rentner oder arbeitslos ist. Diese Auskünfte bezieht die Auskunftei von einem Unternehmen, das in einem anderen Bundesland seinen Sitz hat. Die von dort bezogenen Auskünfte werden lediglich an das anfragende Unternehmen weitergeleitet, aber nicht in einem Datenpool gespeichert. Nach intensiver Suche stellte das Regierungspräsidium Darmstadt fest, dass in einigen Auskünften tatsächlich die Angabe "arbeitslos gemeldet unter BA Nummer ...." enthalten war.

Der Geschäftsführer der Auskunftei teilte mit, dass sein Datenlieferant ihm erläutert habe, die Rechercheure würden dies durch direkte Befragung der Betroffenen erfahren. Das heißt, den Betroffenen würde vorgehalten, dass wegen ausstehender Zahlungen ermittelt würde. Wenn die Betroffenen dann sagen, sie seien arbeitslos, würden die Rechercheure fragen, ob die Betroffenen dies belegen könnten, ob sie beispielsweise die Stammnummer der Bundesagentur für Arbeit angeben könnten. Aufgrund dieser Erläuterungen, die der Auskunftei plausibel erschienen seien, habe man diese Auskünfte auch entsprechend an die anfragenden Unternehmen oder Rechtsanwälte weitergegeben.

Die für das Daten liefernde Unternehmen zuständige Aufsichtsbehörde stellte im Rahmen einer Überprüfung fest, dass auch dieses keine eigenen Ermittlungen durchführe, sondern den Auftrag nur an diverse Detekteien, mit

denen es kooperiere, weiterleite. So führten die Ermittlungen zu Detekteien in anderen Bundesländern.
Die dortigen Aufsichtsbehörden teilten nach ihren Recherchen mit, dass im Ergebnis nicht zweifelsfrei habe geklärt werden können, ob die Stammnummer durch die Betroffenen selber oder durch Bedienstete der Arbeitsämter beauskunftet wurde.

Der in Hessen ansässigen Auskunftei war jedenfalls kein Vorwurf zu machen.
Sie hatte auch bereits sofort die Weitergabe von BA-Nummern an ihre Kunden gestoppt, nachdem die Aufsichtsbehörde sie im Rahmen der unangemeldeten Prüfung darauf hingewiesen hatte, dass die Angaben ihrer Datenlieferanten nicht zweifelsfrei seien und überprüft werden müssten.

9. Versicherungen
9.1 Einrichtung eines konzerninternen Warnsystems

Ein Versicherungsunternehmen hatte mit der Einrichtung eines konzerninternen Warnsystems begonnen und bat das Regierungspräsidium Darmstadt um eine Bewertung der datenschutzrechtlichen Zulässigkeit.

Dieses System hat zum Hintergrund, dass in den vergangenen Jahren eine immer stärkere Rationalisierung und Effizienzsteigerung in der Schadensbearbeitung erfolgt ist und weiter angestrebt wird. Eine Schadensregulierung wird oftmals lediglich aufgrund einer telefonischen Schadensmeldung durchgeführt, ohne dass die Antragsteller Nachweise einreichen müssen. Ein Großteil der Schadensbearbeitung wird mittlerweile durch Call-Center vorgenommen, wo der einzelne Mitarbeiter keine nähere Kenntnis zu der antragstellenden Person hat und im Gegensatz zu einem langjährigen Sachbearbeiter auch nicht über erfahrungsbedingte Informationen zu der jeweiligen Person verfügt.

Diese Entwicklung bringt es mit sich, dass bei der Schadensbearbeitung betrügerische Absichten nicht ausreichend erkannt werden können.

Mit dem neuen Verfahren sollen betrugsverdächtige Schadensmeldungen bereits im Vorfeld automatisiert erkannt werden können mit der Folge, dass die Entschädigungsleistung der Versicherung in diesen Fällen zunächst nicht zur Auszahlung kommt. Die Fälle, bei denen Anhaltspunkte für ein möglicherweise betrügerisches Vorgehen erkannt werden, können einer vertieften Überprüfung eines speziellen Betrugssachbearbeiters unterzogen werden, der gegebenenfalls Nachweise zur Schadenshöhe und zum Schadensereignis fordert oder sonstige Ermittlungen anstellt. Damit kann sowohl dem beschriebenen Erfordernis der Rationalisierung und Entbürokratisierung bei der Schadensabwicklung Rechnung getragen als auch ein Schutz vor Betrug erzielt werden.

Zu diesem Zweck wurde von der Anbieterfirma zusammen mit einem Rückversicherer und fünf Erstversicherern ein System namens "intelligente Schadensprüfung" entwickelt, bei dem verschiedene, von dem Antragsteller angegebene Begrifflichkeiten mit Entscheidungsregeln verknüpft werden. Beispielsweise würde das System eine Auffälligkeit feststellen, wenn eine Person mehrfach einen Unfall mitten in der Nacht mit einem hochwertigen Fahrzeug in einem Gewerbegebiet ohne Zeugen melden würde.

Wird nach Eingabe der Schadensmeldung von dem automatisierten Betrugserkennungssystem ein Schaden als auffällig bewertet, erfolgt zunächst nur eine Kennzeichnung auffälliger Schadensfälle durch das System. Diese Schadenskennzeichnung wird wieder gelöscht, sofern der Spezialsachbearbeiter bei näherer Prüfung keine Auffälligkeiten feststellt.

Im anfragenden Konzern wurde das System im Berichtsjahr im Bereich Komposit in Einsatz gebracht, welcher die Versicherungsbereiche KFZ, Hausrat, Haftpflicht und Sachhaftpflicht umfasst, wobei der Einsatz zunächst nur in beschränktem Umfang erfolgte. So wurden zunächst lediglich "auffällige Schadensfälle" gekennzeichnet.

Eine Kennzeichnung einzelner an dem Schadensvorgang beteiligter Personen unterblieb, da die Versicherung insbesondere die rechtliche Zulässigkeit der Kennzeichnung von Personen, die an dem Schadensfall beteiligt waren, aber

nicht Versicherungsnehmer sind, vorab mit der Aufsichtsbehörde klären wollte.

Es ist nicht vorgesehen, die Kennzeichnung eines Schadensfalles und die geplante Kennzeichnung der dazugehörigen beteiligten Personen im weiteren Sinne auch innerhalb des Konzerns zu übermitteln. Auch eine Verwendung der vorgenommenen Kennzeichnungen bei Vertragsabschlüssen ist nicht vorgesehen, d.h. selbst wenn jemand in einen Schadensfall involviert war, der als auffällig gekennzeichnet war, führt dies nicht zur Vertragsablehnung, wenn diese Person später einen Versicherungsvertrag abschließen möchte.

Die Zulässigkeit der Kennzeichnung der betroffenen Schadensfälle begegnet unter diesen Umständen keinen datenschutzrechtlichen Bedenken. Ob die Zulässigkeit sich aus § 28 Abs. 1 Nr. 1 oder Nr. 2 BDSG ergibt, kann hier dahingestellt bleiben, da sie ein notwendiges Regulativ der arbeitsteiligen und unbürokratischen Schadensbearbeitung ist und ein legitimes Interesse der Versicherung an der Abwicklung der Bearbeitung im Rahmen des Vertragsverhältnisses besteht.

Von der geplanten Kennzeichnung von Personen können sowohl Kunden (z.B. Inhaber einer Hausratsversicherung) als auch Nichtkunden wie z.B. Halter, Fahrer, Antragsteller (Geschädigter), Zeugen sowie Sachverständige betroffen sein, bei denen der Verdacht besteht, dass sie in betrügerischer Absicht mit einem Unfallteilnehmer zusammengewirkt haben oder auf irgendeine Weise im Verdacht der Beteiligung an einem Versicherungsmissbrauch stehen.

Die Erhebung und Speicherung der Daten der Nichtkunden wird sich in der Regel nach § 28 Abs. 1 Nr. 2 BDSG richten, denn zur Erfüllung eigener Geschäftszwecke dürfen die Versicherungsunternehmen die Daten von Anspruchstellern und Zeugen oder Ähnlichen erheben und speichern, da es zur Wahrung ihrer berechtigten Interessen, nämlich der Vertragserfüllung, erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der jeweils Betroffenen an dem Ausschluss der Verarbeitung überwiegt.

Eine relevante Zweckänderung der Speicherung ist nicht ersichtlich, da nach wie vor lediglich eine Verwendung innerhalb des gleichen Unternehmens in dem gleichen Bereich und nicht im Rahmen der Versicherungsantragsprüfung erfolgt. Daher ist auch die Kennzeichnung von Personen, die in auffälliger Weise an einem Schadensfall beteiligt waren, noch von § 28 Abs. 1 Nr. 2 BDSG gedeckt.

An dieser Stelle stellt sich aber die Frage, ob eine Benachrichtigungspflicht aufgrund der Speicherung nach § 33 Abs. 1 BDSG entsteht, wonach der Betroffene zu benachrichtigen ist, wenn erstmals personenbezogene Daten über ihn für eigene Zwecke ohne seine Kenntnis gespeichert werden, oder ob das Transparenzgebot des § 4 Abs. 3 BDSG eine Unterrichtung des betroffenen Personenkreises gebietet.

Da Anspruchsteller, Zeugen, Sachverständige u.a. direkt mit der Versicherung in Kontakt treten, ist nicht davon auszugehen, dass die Speicherung ohne ihre Kenntnis erfolgt. Jede Person, die in einem Versicherungsfall Aussagen oder Angaben macht, wird auch davon ausgehen müssen, dass ihre Daten gespeichert oder automatisiert verarbeitet werden. Da auch eine Kennzeichnung von Nichtkunden im Grunde nur ein Ausgleich für das bei traditioneller "Sachbearbeitung" vorhandene Erfahrungswissen ist, erscheint eine spezielle Information nicht zwingend erforderlich.

Die Einrichtung des konzerninternen Betrugserkennungssystems wurde daher von der Aufsichtsbehörde unter den vorgenannten Voraussetzungen nach Abstimmung in einer vom Düsseldorfer Kreis gebildeten Arbeitsgruppe als zulässig erachtet.

9.2 Schweigepflichtentbindungserklärung bei Leistungsfall

In einem weiteren Beschwerdefall wandte sich eine Betroffene gegen die Formulierung einer Schweigepflichtentbindungserklärung, die Bestandteil eines Krankenversicherungsantragsformulars war, welches eine Versicherung aus dem Aufsichtsbezirk verwendete.

In dieser war unter anderem ausgeführt, dass "die Geltendmachung eines Leistungsanspruches die Bedeutung einer Schweigepflichtentbindungserklärung im Einzelfall habe."

Patientendaten unterliegen der ärztlichen Schweigepflicht.

Wollen Versicherungen im Rahmen einer Leistungsprüfung die Auskunft des behandelnden Arztes einholen, müssen sie zuvor eine Schweigepflichtentbindungserklärung einholen. Da die Weitergabe von Gesundheitsdaten auch in den Anwendungsbereich des BDSG fällt, ist die Datenübermittlung durch Ärzte und andere, die dem Geltungsbereich des § 203 StGB unterfallen, nach der Regelung des § 4 Abs. 1 BDSG nur zulässig, wenn die Erklärung die Voraussetzungen des § 4a BDSG für eine wirksame Einwilligung erfüllt. Bei sensitiven Daten - wie Gesundheitsdaten - hat das BDSG eine erhöhte Schutzbedürftigkeit des Betroffenen angenommen (§ 28 Abs. 6 BDSG). Deshalb gelten bei der Einwilligung in Bezug auf diese Daten verschärfte Anforderungen. Eine Erhebung, Verarbeitung und Nutzung ist nur dann zulässig nach § 4a Abs. 3 BDSG, wenn die Einwilligung ausdrücklich die sensiblen Daten umfasst.

Eine uneingeschränkte Erhebung von Gesundheitsdaten aufgrund einer bei Vertragsabschluss abgegebenen Schweigepflichtentbindungserklärung wurde durch die Einführung des § 4a BDSG damit beschränkt. Durch die BDSG Gesetzesnovelle ergab sich eine neue rechtliche Bewertung, die eine Überarbeitung der "alten", mit der Versicherungswirtschaft abgesprochenen Vorgehensweise erforderlich macht, denn nach § 4a Abs. 1 und Abs. 3 BDSG muss aus der Einwilligungserklärung für den Betroffenen klar erkennbar sein, welche Gesundheitsdaten von wem zu welchem Zweck erhoben, verarbeitet oder genutzt werden sollen.

Dementsprechend hat der Düsseldorfer Kreis in seiner Sitzung vom 6. und 7. Mai 2004 zu dieser Thematik mehrheitlich die Auffassung vertreten, dass für jede Rückfrage von Krankenversicherungen bei Ärzten, anderen Angehörigen von Heilberufen oder Krankenanstalten wegen der Erstattung von Rechnungen die Einwilligung gesondert für jeden Patienten einzuholen ist.

Daher wurde die Formulierung der Schweigepflichtentbindungserklärung in den Vertragsunterlagen von der Aufsichtsbehörde beanstandet und auf das Erfordernis hingewiesen, für jede Rückfrage einer Krankenversicherung bei Ärzten u.a. in einem Leistungsfall zunächst die Einwilligung in Form einer Schweigepflichtentbindungserklärung für den Einzelfall einzuholen.

9.3 Datenerhebung bei Ärzten vor Abschluss von Versicherungsverträgen

Ein Bürger hatte einen Antrag auf Abschluss einer Berufsunfähigkeitsversicherung bei einer Versicherung im Rhein-Main Gebiet gestellt.

Hierbei hatte der Betroffene eine datenschutzrechtliche Einwilligungserklärung abgegeben und eine Schweigepflichtentbindungserklärung unterzeichnet, die folgenden Wortlaut hatte:

"Ich ermächtige die Gesellschaft, zur Nachprüfung und Verwertung der von mir über meine Gesundheitsverhältnisse gemachten Angaben, alle Ärzte, Krankenhäuser und sonstigen Krankenanstalten sowie Pflegeeinrichtungen, bei denen ich in Behandlung oder zur Pflege war oder sein werde sowie andere Personenversicherer über meine Gesundheitsverhältnisse bei Vertragsabschluss zu befragen."

In dem Antragsformular der Versicherung hatte der Beschwerdeführer die gestellten Fragen zu seinem Gesundheitszustand konkret beantwortet und eine Erklärung zu seinem Gesundheitszustand abgegeben. Dieser Fragenkatalog beinhaltete unter anderem die Frage, ob eine Beeinträchtigung der Arbeits-, Erwerbs- oder Berufsfähigkeit bestehe und ob der Antragsteller in den letzten fünf Jahren untersucht, beraten oder behandelt wurde. Die Fragen waren also so konzipiert, dass die Beantwortung das für die Versicherung zu klärende Risiko umfassend erkennen ließ.

Wie in anderen, gleich gelagerten Fällen hatte die Versicherung die von dem Beschwerdeführer benannten Ärzte pauschal um Auskunft zu dem Gesundheitszustand gebeten. Das Anforderungsschreiben zum Gesundheitszustand

ließ dabei nicht erkennen, welche Gesundheitsdaten für den konkreten Geschäftszweck relevant und erheblich sein können und deshalb der Mitteilung und Erläuterung durch den Arzt bedürfen.

Eine der befragten Ärztinnen gab daraufhin Auskunft über eine über zehn Jahre zurückliegende Erkrankung, die aber ohne Restdefekt ausgeheilt war.

Im Einzelfall kann das für den betroffenen Antragsteller bedeuten, dass womöglich die Versicherung eine längst ausgeheilte Erkrankung - die unter Umständen für den Geschäftszweck irrelevant ist - speichert und an die zentralen Hinweissysteme der Versicherungswirtschaft gegebenenfalls als Sonderrisiko weitergibt, sofern der mitteilende Arzt keine Angaben über eine vollständige Ausheilung macht.

Die Aufsichtsbehörde beanstandete deshalb das Anforderungsschreiben der Versicherung und wies diese darauf hin, dass in der oben zitierten Schweigepflichtentbindungserklärung die Versicherung von dem Antragsteller lediglich dazu ermächtigt wurde, "zur Nachprüfung und Verwertung der von dem Antragsteller über seine Gesundheitsverhältnisse gemachten Angaben, alle Ärzte.., befragen" zu dürfen, jedoch eine weitergehende Schweigepflichtentbindung, die zu pauschalen Anforderungsschreiben berechtigt, sich aus der unterzeichneten Schweigepflichtentbindungserklärung nicht ableiten lässt und über diese inhaltlich hinausgeht.

Die Aufsichtbehörde bat, bei zukünftigen Anforderungsschreiben, in Anlehnung an den vom Antragsteller auszufüllenden Fragenkatalog, die an die Ärzte gerichteten Fragen zu konkretisieren.

9.4 Wirksamkeit der Einwilligungserklärung und Überlassung des Merkblattes zur Datenverarbeitung bei Abschluss von privaten Versicherungen

Die Gesamtproblematik der datenschutzrechtlichen Einwilligungserklärung nebst dem dazugehörigen Merkblatt zur Datenverarbeitung kann hier nicht umfassend erörtert werden. Es bedarf jedoch der Erwähnung, dass die Aufsichtsbehörden die im Jahr 1994 abgestimmte Einwilligungserklärung nebst dem Merkblatt zur Datenverarbeitung für nicht mehr in Einklang mit der geltenden Rechtslage halten (siehe bereits oben Nr. 9.3). Dies ist Gegenstand umfassender Erörterung in der Arbeitsgemeinschaft Versicherungswirtschaft des Düsseldorfer Kreises. Eines von vielen erörterten Problemen ist der Zeitpunkt der Aushändigung des Merkblatts zur Datenverarbeitung.

Im Berichtsjahr gab es zahlreiche Beschwerden, in denen die Beschwerdeführer vortrugen, sie hätten bei Beantragung oder Abschluss privater Kranken-, -Lebens-, und Berufsunfähigkeitsversicherungen das Merkblatt zur Datenverarbeitung nicht erhalten. Damit sei aber eine wirksame Einwilligungserklärung in die zahlreichen Datenverarbeitungen im Rahmen eines Versicherungsvertrages bzw. auch schon im Rahmen des Antragsverfahrens nicht abgegeben worden.

Es stößt bei den Versicherten zunehmend auf Widerstand, dass sie von Versicherungen bei Streitfragen auf das Merkblatt zur Datenverarbeitung verwiesen werden, obwohl sie dieses zu keinem Zeitpunkt ausgehändigt bekommen haben.

Der Umfang der Datenverarbeitung ergibt sich in verkürzter Form zunächst aus der datenschutzrechtlichen Einwilligungserklärung, die in jedem Versicherungsvertrag enthalten ist. Eine ausführlichere Beschreibung über Art und Umfang der Erhebung, Nutzung oder Verarbeitung der Daten enthält das Merkblatt zur Datenverarbeitung in der Versicherungswirtschaft.

Nach dem Wortlaut der 1994 zwischen den Aufsichtsbehörden und dem Gesamtverband der Versicherungswirtschaft (GDV) abgestimmten Einwilligungserklärung, die vom Bundesaufsichtsamt für das Versicherungswesen, der heutigen Bundesanstalt für Finanzdienstleistungsaufsicht, genehmigt wurde, soll dieses Merkblatt dem Versicherungsnehmer vor Vertragsabschluss überlassen werden.

So lautet die seinerzeit abgestimmte Formulierung:

"Diese Einwilligung gilt nur, wenn ich bei Antragstellung vom Inhalt des Merkblattes zur Datenverarbeitung Kenntnis nehmen konnte, das mir vor

Vertragsabschluß (mit weiteren Verbraucherinformationen), auf Wunsch auch sofort, überlassen wird."

Diese Formulierung halten die Aufsichtbehörden für überarbeitungsbedürftig.

Dem liegen folgende Erwägungen zugrunde:

Versicherungsverträge kommen üblicherweise zustande, indem der Kunde einen Antrag ausfüllt, der von dem Unternehmen angenommen wird. Da die Datenverarbeitung aber bereits bei Antragstellung erfolgt, müssen die im Merkblatt zur Datenverarbeitung enthaltenen Informationen dem Betroffenen rechtzeitig, das heißt vor Beginn der Datenerhebung und der weiteren Verarbeitung zur Kenntnis gebracht werden, denn anderenfalls ist der Betroffene nicht in der Lage, die Bedeutung der Verarbeitung abzuschätzen.

Nicht selten finden sich Interessenten für eine Versicherung in der misslichen Situation wieder, erhebliche Zuschläge bei Vertragsabschluss hinnehmen zu müssen oder bei mehreren - wenn nicht sogar allen - Versicherungsgesellschaften abgelehnt zu werden. Bei näherer Prüfung stellt sich dann heraus, dass das Scheitern des ersten Antrages in die zentralen Hinweissysteme der Versicherungswirtschaft (Uniwagnis) eingemeldet wurde. Auf diese Zusammenhänge aufmerksam zu machen, ist Aufgabe des Merkblattes zur Datenverarbeitung. Wird dies dem Antragsteller zum Zeitpunkt der Antragstellung aber vorenthalten, bleibt der Betroffene in Unwissenheit über die Konsequenzen, die sich aus der Datenverarbeitung ergeben können.

Gerade für diese Fälle wird deutlich, dass die Voraussetzungen einer freien und informierten Einwilligung nicht erfüllt sind, wenn der Antragsteller das Merkblatt erst bei einem - gar nicht stattfindenden Vertragsabschluss - überlassen bekäme (so genannte Police-Verfahren), denn nach § 4a BDSG muss dem Betroffenen vor Antragstellung, das heißt vor Unterzeichnung der Datenweitergabeklausel, das Merkblattes zur Datenverarbeitung überlassen worden sein. Auch für die Datenverarbeitungen, die keiner Einwilligung des Betroffenen bedürfen, sondern bereits aufgrund gesetzlicher Vorgaben zulässig sind, gebietet das Transparenzgebot des § 4 Abs. 3 Nr. 2 BDSG, dass der Versicherungsnehmer rechtzeitig über die beabsichtigten Verarbeitungen informiert wird.

Zwar eröffnet die derzeit bestehende Datenweitergabeklausel dem Betroffenen die Möglichkeit, sich selbst zu informieren, bevor er den Antrag unterzeichnet oder abgibt, denn auf seinen Wunsch wird ihm das Merkblatt sofort überlassen. Sofern er - wie in allen Beschwerdefällen - jedoch diesen Wunsch nicht äußert, gilt nach der Datenweitergabeklausel die Einwilligung auch dann als erteilt, wenn das Merkblatt noch vor Vertragsabschluss, das heißt vor Unterzeichnung durch die Versicherung, überlassen wird.

Dies ist zu spät, da die Daten bereits mit Antragstellung verarbeitet und an die Zentralen Hinweissysteme eingemeldet werden und sodann von jedem anfragenden Versicherungsunternehmen abgefragt werden können.

Im Übrigen haben die Aufsichtbehörden bei mehreren Versicherungen eine mangelnde Bereitschaft feststellen müssen, sich überhaupt an die eindeutige Formulierung der Einwilligungserklärung zu halten, die eine Überlassung des Merkblattes spätestens vor Vertragsschluss zwingend als Bedingung für das wirksame Zustandekommen der Einwilligung vorsieht.

So wurde von zahlreichen Beschwerdeführern vorgetragen, dass man ihnen das Merkblatt zu keinem Zeitpunkt überlassen habe, auch nicht im Rahmen eines Vertragsabschlusses. Teilweise wurde von den Versicherungen im Aufsichtsbereich vertreten, das Merkblatt müsse nur dann dem Kunden überlassen werden, wenn dieser es verlange. Dies ergebe sich aus der Formulierung der Erklärung, dass der Betroffene eine sofortige Überlassung fordern könne. Tue er dies nicht, müsse die Versicherung das Merkblatt auch nicht zu einem anderen Zeitpunkt überlassen.

Diese Auffassung ist, zumindest hinsichtlich der zwingend einwilligungsbedürftigen Sachverhalte, nicht akzeptabel, denn erhält der Kunde das Merkblatt überhaupt nicht, kommt eine Einwilligung nicht wirksam zustande.

In diesem Zusammenhang vertraten die Aufsichtsbehörden die Auffassung, dass die Dokumentationspflicht für die Überlassung des Merkblattes zur Datenverarbeitung nicht bei dem Kunden liegen könne. Da die Zulässigkeit einer Vielzahl von Datenverarbeitungen, die private Versicherungen im Rahmen eines Vertragsantrags- oder -abschlussverfahrens vornehmen, von dem Vorliegen einer wirksam erteilten Einwilligungserklärung abhängig ist, dürfte es im Interesse der Versicherungen liegen, im Streitfall die Wirksamkeit der Erklärung belegen zu können.

Diese gesamte Problematik bedarf im Zuge der von den Aufsichtsbehörden für erforderlich gehaltenen Neufassung der Einwilligungserklärung einer vertieften Diskussion und Abstimmung mit der Versicherungswirtschaft.

10. Austausch von Mitarbeiterdaten innerhalb eines Konzerns

Die Anzahl großer, häufig multinationaler Konzerne wächst ständig. Konzernstrukturen unterliegen oftmals einem permanenten Wandel. Neue Unternehmen kommen hinzu, konzernangehörige Unternehmen werden in mehrere juristische Einheiten aufgeteilt, zusammengelegt oder veräußert. Zugleich verstärken sich die Tendenzen zur Aufgabenteilung innerhalb eines Konzerns. Die Kostensenkung und Produktivitätssteigerung sind Beweggründe für eine konzernweite, über die einzelnen juristischen Personen (Unternehmen) hinausgehende, Optimierung der Geschäftstätigkeit, beispielsweise durch eine entsprechend ausgerichtete Personalverwaltung. Nicht zuletzt aufgrund der Verfügbarkeit geeigneter Datenverarbeitungssysteme zur Personalplanung nehmen konzernweite Personalwirtschaftslösungen zu.

Während Konzerne sich also als wirtschaftliche Einheit verstehen und dementsprechend agieren, ist für das Datenschutzrecht das einzelne Unternehmen als juristische Person maßgeblich. Dieses ist Normadressat des BDSG (vgl. § 1 Abs. 2 Nr. 3, § 2 Abs. 4). Die gesellschaftsrechtlichen und wirtschaftlichen Zusammenhänge bleiben in der Betrachtungsweise des BDSG grundsätzlich unberücksichtigt. Gesellschaftsrechtliche Beherrschungsverträge haben als solche keine unmittelbare Bedeutung für den Datenschutz. Das BDSG enthält demnach kein Konzernprivileg. Bereits bei der Verabschiedung des ersten BDSG hat sich der Gesetzgeber trotz entsprechender Forderungen aus Wirtschaftskreisen bewusst gegen ein Konzernprivileg entschieden. Auch auf EU-Ebene konnte sich die Wirtschaft mit ihrer Forderung nach einem Konzernprivileg in der EG-Datenschutzrichtlinie nicht durchsetzen (siehe hierzu ausführlich Evelyn Ruppmann, Der konzerninterne Austausch personenbezogener Daten, Frankfurter Studien zum Datenschutz, Band 16, S. 88 ff.). Überlegungen, ob die Formulierung in Art. 2 Buchst. d EG-Datenschutzrichtlinie nicht doch Umsetzungsspielräume bietet, sind jedenfalls dadurch obsolet, dass sich der Bundesgesetzgeber bei der letzten Novelle des BDSG erneut gegen eine Privilegierung der Datenverarbeitung innerhalb von Konzernen entschieden hat.

Die Frage der Zulässigkeit von Datenweitergaben richtet sich daher nach den allgemeinen Vorschriften des Bundesdatenschutzgesetzes, insbesondere § 11 BDSG und §§ 4, 28 BDSG. Die praktizierte Konzerneinheit steht damit in einem gewissen Spannungsverhältnis zur datenschutzrechtlichen Rechtslage.

Aufgrund einer Initiative aus dem "Düsseldorfer Kreis" wurde eine spezielle Arbeitsgruppe gebildet, um die bestehenden Auslegungsfragen zu erörtern. Ziel war es, herauszuarbeiten, wie praxisgerechte Lösungen auch ohne Konzernklausel gefunden werden können, gleichzeitig aber auch die Grenzen aufzuzeigen. Um von vornherein den Praxisbezug herzustellen, erhielten auch Vertreter der Wirtschaft (betriebliche Datenschutzbeauftragte) und der Anwaltschaft Gelegenheit, sich neben den Vertretern von Datenschutzaufsichtsbehörden zu beteiligen. Es ergab sich eine sehr intensive und fruchtbare Zusammenarbeit. Die Erörterungen konzentrierten sich auf die Weitergabe von Personaldaten.

Die erste Sitzung fand beim Berliner Beauftragten für Datenschutz und Informationsfreiheit statt, die zweite und abschließende Sitzung beim Regierungspräsidium Darmstadt unter dessen Leitung. Das Ergebnis ist in einem vom Regierungspräsidium Darmstadt verfassten und mit den Teilnehmern abgestimmten Arbeitsbericht dargestellt, der auf der Internet-Seite des Regierungspräsidiums Darmstadt abrufbar ist:
(http://www.rpda.de/dezernate/datenschutz/download/Arbeitsbericht-Endfassung.pdf).

Obwohl gewisse Divergenzen in der Rechtsauslegung blieben, bestand vor allem bei einigen exemplarisch behandelten Fallgestaltungen, die sich typischerweise in Konzernen ergeben können, Einigkeit, dass der hierfür erforderliche Datenaustausch datenschutzgerecht realisiert werden kann. Der Arbeitsbericht wurde bewusst als solcher veröffentlicht. Die aufgezeigten Lösungswege sollen in der Praxis "erprobt" und diskutiert werden, bevor sich der Düsseldorfer Kreis mit der Thematik befasst.

Da im Rhein-Main-Gebiet viele Konzerne bzw. konzernangehörige Unternehmen ihren Sitz haben, bitten viele betriebliche Datenschutzbeauftragte und Rechtsanwälte das Datenschutzdezernat des Regierungspräsidiums Darmstadt um Beratung zu Fragen des konzerninternen Datentransfers. Anlass für solche Anfragen ist häufig, dass ein Drittstaatentransfer geplant wird. Hierbei wird vielfach erst bewusst, dass nicht nur die Beachtung der besonderen Anforderungen der §§ 4b, 4c BDSG, sondern auch die Erfüllung der "normalen" Anforderungen des BDSG schwierige Fragen aufwirft. Sowohl für die Unternehmen als auch für die Aufsichtsbehörde stellt der Arbeitsbericht hier eine erste Arbeitshilfe für die komplexen Fragestellungen dar.

11. Datenverarbeitung im Rahmen der Fußball-Weltmeisterschaft 2006

11.1 Ticketverkauf

11.1.1 Verantwortliche Stelle

Der internationale Fußball-Verband (FIFA, Federation Internationale de Football Association) ist zwar der eigentliche Hauptveranstalter der WM, aber der Ticketverkauf erfolgt durch den Deutschen Fußball-Bund (DFB), konkret durch das bei ihm angesiedelte Organisationskomitee (OK) im eigenen Namen. Der DFB ist also der verantwortliche Vertragspartner und damit die verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes für die Datenverarbeitung zum allgemeinen Kartenverkauf.
Dies gilt jedenfalls für den Direktverkauf an Jedermann, der über Internet und per Post abgewickelt wird. Hierauf bezieht sich die folgende Darstellung.
Andere Vertriebswege, insbesondere die Ticketverteilung über Sponsoren, werden am Ende (siehe unten Nr. 11.1.8) kurz angesprochen.

11.1.2 Personalisierung der Tickets

Bei der Fußball-WM 2006 erfolgt erstmals für Fußballspiele in Deutschland eine Personalisierung der Tickets, das heißt die Tickets werden eindeutig einer Person und einem konkreten Platz im Stadion zugeordnet. Hierfür werden auf dem Bestellformular personenbezogene Daten (Name, Adresse etc.) des Bestellers und derjenigen Personen, für die der Besteller Tickets mitbestellt, erhoben. Konsequenterweise ist eine Übertragung des Tickets nur mit vorheriger schriftlicher Zustimmung des DFB/OK möglich unter Angabe der personenbezogenen Daten des Ticketerwerbers. Ferner werden die Tickets mit einem speziellen Chip versehen, der die Zuordnung des Tickets zu einer bestimmten Person sicherstellt ("RFID-Chip", siehe unten Nr. 11.1.3).

Es gibt mehrere Gründe für das gewählte Verfahren.
FIFA und DFB haben als Veranstalter und Ausrichter der Fußball-WM 2006 die Pflicht, für den ordnungsgemäßen Ablauf und die sichere Durchführung der Veranstaltung zu sorgen. Die "Entschließung des Rates der Europäischen Union vom 6. Dezember 2001 betreffend ein Handbuch mit Empfehlungen über die internationale polizeiliche Zusammenarbeit und Maßnahmen zur Vorbeugung und Bekämpfung von Gewalttätigkeiten und Störungen im Zusammenhang mit Fußballspielen von internationaler Dimension" beschreibt dies in Kapitel 6 unter anderem als eine Anforderung an den Veranstalter.

Dem Ticketverfahren des Veranstalters kommt bei der Erfüllung dieser Anforderung eine besondere Bedeutung zu. Nach der Empfehlung Nr. 1/2001 des Ständigen Ausschusses zur Gewaltkonvention des Europarates soll es unter anderem

- eine wirksame und effiziente Trennung rivalisierender Fans,
- die Verhütung des Schwarzmarkthandels und des Kartenbetrugs,
- die Unterstützung der Politik der Stadionverbote,
- die Finanzierung

gewährleisten.

Die Personalisierung der Tickets ist ein zentraler Bestandteil des Sicherheitskonzepts des Veranstalters bzw. Ausrichters und dient der Erfüllung vorgenannter Punkte.

Die Sicherheit im Stadion soll unter anderem dadurch gewährleistet werden, dass bekannte Hooligans vom Ticketerwerb ausgeschlossen werden. Daher erfolgt zunächst ein Abgleich der Ticketbesteller mit den Stadionverbotsdateien. Die Erteilung von Stadionverboten beruht auf dem nationalen Konzept "Sport und Sicherheit". Alle von den Vereinen der 1. und 2. Bundesliga sowie von den Regionalligen ausgesprochenen Stadionverbote werden in einer gemeinsamen Datei gespeichert. Stadionverbote erfolgen auf der Grundlage des Hausrechts, wobei die Vereine sich gegenseitig ermächtigt haben, ein Stadionverbot auszusprechen, das alle Stadien betrifft. Wird ein Stadionverbot verhängt, erfolgt eine formularmäßige Mitteilung an den Betroffenen, der dagegen zivilrechtlich vorgehen kann (vgl. zu weiteren Einzelheiten den Tätigkeitsbericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2004, Nr. 4.1.1, S. 50, 51).

Ferner erfolgt unter Umständen ein Abgleich mit entsprechenden oder ähnlichen Dateien ausländischer Fußballverbände, sofern diese vorhanden sind und dem DFB zur Verfügung gestellt werden. Damit diese Verbote nicht unterlaufen werden, werden die Tickets der konkreten Person zugeordnet.

Die Personalisierung der Tickets nebst Chip-Einsatz bietet auch die Möglichkeit der Ticketsperrung bei Personen, die bereits ein Ticket bzw. eine entsprechende Berechtigung erhalten haben, aber während der WM als gewalttätig auffallen oder wegen des Verdachts terroristischer Anschläge strafrechtlich verfolgt werden.

Die Trennung rivalisierender Fangruppen im Stadion soll erreicht werden, indem im Bestellformular erfragt wird, in welchem Fanblock jemand sitzen möchte (siehe unten Nr. 11.1.5). Dadurch können bereits beim Zutritt in das Stadion die Zuschauerströme entsprechend gesteuert werden.

Mit der Personalisierung der Tickets und der damit verbundenen Beschränkung der Übertragbarkeit kann auch der Schwarzmarkthandel unterbunden werden. Zugleich soll gewährleistet werden, dass möglichst große Bereiche der Bevölkerung eine Chance haben, ein Ticket zum regulären Preis zu erhalten. Dieses Ziel wird zusätzlich unterstützt durch die Beschränkung auf maximal vier Karten pro Spiel und Käufer. Die Unterbindung des Schwarzmarkthandels bietet erst die Gewähr, dass die Tickets nicht doch in die Hände von Personen gelangen, gegen die ein Stadionverbot verhängt wurde oder die wegen des Verdachts terroristischer Anschläge strafrechtlich verfolgt werden.

Nach dem BDSG ist die Personalisierung von Tickets grundsätzlich kritisch zu sehen. Nach § 3a BDSG besteht das Gebot der Datenvermeidung und der Datensparsamkeit, die verantwortlichen Stellen sollen so wenig personenbezogene Daten wie möglich verarbeiten. Nach § 28 Abs. 1 Nr. 1 und 2 BDSG soll eine Datenverarbeitung nur erfolgen, soweit sie für die Erfüllung des eigentlichen Vertragszweckes erforderlich ist. Es wäre mit dem BDSG nicht vereinbar, wenn es generell dazu käme, dass jegliche Teilnahme am gesellschaftlichen Leben nur bei Angabe der Personalien möglich wäre. Eine darüber hinausgehende Datenverarbeitung lässt das BDSG unter engen Voraussetzungen nach Abwägung mit den schutzwürdigen Interessen des Betroffenen zu (vgl. § 28 Abs. 3 Nr. 1 und 2). Es ist daher sorgfältig abzuwägen zwischen dem Interesse der Kartenkäufer, dass möglichst keine bzw. so wenig wie möglich personenbezogene Daten erhoben werden bzw. dass diese gegebenenfalls nach Ticketzusendung gelöscht bzw. gesperrt werden, und den Interessen des Kartenverkäufers oder der Allgemeinheit an der Speicherung der Daten.

Angesichts der ganz besonderen Dimension der Gefahren für Leib und Leben ist die Personalisierung der Tickets und die zu diesem Zweck beabsichtigte Datenspeicherung der Ticketerwerber bis zum Ablauf der WM 2006 gerechtfertigt und mit den oben genannten Bestimmungen des BDSG vereinbar. Der Besucher im Stadion hat das Recht auf einen störungsfreien Ablauf der Veranstaltung.

Eine Personalisierung der Tickets nützt natürlich nur, wenn eine Ausweiskontrolle am Stadion erfolgt oder erfolgen kann. Der Besucher muss daher damit rechnen, dass Ausweiskontrollen am Stadioneingang durchgeführt werden, Stichproben sind nach derzeitigem Kenntnisstand geplant. Nach dem Prinzip der "skalierbaren Sicherheit" kann und soll jedenfalls eine Anpassung an die konkreten Sicherheitserfordernisse erfolgen, sei es je nach Spielgegner und "Hooliganpotenzial" der Zuschauer und je nach allgemeiner Sicherheitslage (Hinweise auf terroristische Anschläge). Je nach Erfordernis können die Stichproben intensiviert werden, bis zur Kontrolle aller Zuschauer.

In den Allgemeinen Geschäftsbedingungen zum Ticketverkauf sind entsprechende Kontrollen vorbehalten. Die Identitätsprüfung kann durch Abgleich des Personalausweises mit den hinterlegten Bestelldaten erfolgen (mittels RFID, siehe nachfolgende Beschreibung unter Nr. 11.1.3). Darüber hinaus können die Personalien auch auf das Ticket aufgedruckt werden, sodass hierüber ein zusätzlicher erster Abgleich möglich wäre.

Mit der Personalisierung der Tickets wird daher ein wichtiger Beitrag zur Sicherheit in den Stadien erbracht. Unter Berücksichtigung dessen, dass dem DFB und den Sicherheitsbehörden die Verantwortung für die Sicherheit obliegt, besteht für die Datenschutzaufsichtsbehörde keine Veranlassung und Rechtfertigung, das gewählte Konzept und die dadurch bedingte Datenverarbeitung zu beanstanden.

Diese Bewertung zur Personalisierung des Ticketverkaufs bezieht sich ausschließlich auf die Fußball-WM 2006 mit ihrem ganz speziellen Gefährdungspotential und nicht auf andere Fußball- oder sonstige Großveranstaltungen.

11.1.3 RFID-Technik

Die Eintrittskarten für die WM 2006 sollen mit einem speziellen Chip versehen werden, der die genannten Zielsetzungen unterstützt. Es handelt sich um eine neue Technik, die Radio Frequency Identifikation (RFID).
Weitere Informationen zu dieser Technik und zu deren grundsätzlichen datenschutzrechtlichen Problemen können den Ausführungen des Hessischen Datenschutzbeauftragten in seinem 33. Tätigkeitsbericht (Drucks. 16/3746) unter Nr. 8.4 entnommen werden.

Aufgrund des Einsatzes der RFID-Technik sind die Tickets fälschungssicher, können technisch gesperrt werden, wenn ein Ticket als verloren oder gestohlen gemeldet wurde oder wenn aus Sicherheitsgründen einer Person, die bereits ein Ticket erhalten hat, der Zugang zum Stadion verwehrt werden soll, und sie dienen der elektronischen Zugangskontrolle an den Stadioneingängen einschließlich der Fangruppentrennung.

Für die datenschutzrechtliche Bewertung sind mehrere Aspekte von Bedeutung.

Es wird ein Chip gemäß ISO 14443 eingesetzt, der nur dann von einem Lesegerät ausgelesen werden kann, wenn ein geringer Abstand zwischen Chip und Lesegerät besteht (maximal 10 bis 15 cm). Auf dem Chip sind lediglich eindeutige Angaben zur Registrierung beim Ticketverkauf - eine Zuordnung - und die Spielinformation in verschlüsselter Form gespeichert, keine weiteren personenbezogenen Daten und insbesondere nicht die Pass- und Personalausweisnummer des Käufers (vgl. die Informationen auf der offiziellen Internet-Seite zum Verkauf der Tickets für die WM 2006 in FAQ 47 [http://fifaworldcup.yahoo.com/06/de/tickets/faq.html]).

Der Chip fungiert als "Schlüssel" zu den Zugangskontrolldaten, die aus dem Ticketsystem verschlüsselt in das Zugangskontrollsystem des jeweiligen Stadions übermittelt wurden, und dient dem Abgleich mit diesen Daten. Dies geschieht dadurch, dass der Besucher das Ticket mit dem RFID an das Lesegerät hält, welches sich an den Drehkreuzen bei den Stadioneingängen befindet. Mit Hilfe des RFID erfolgt der Abgleich mit der Datenbank, ob es sich um ein gültiges Ticket handelt. Wenn ja, öffnet sich das Drehkreuz. Wenn nein, ist der Zutritt verwehrt. Die Lesegeräte können auch so eingestellt werden, dass das vom DFB bzw. dessen Dienstleister eingesetzte Bedienpersonal zugleich die Personalien der betreffenden Person lesen und mit dem vorzulegenden Personalausweis abgleichen kann.

Auf dem Chip selbst findet keine weitere Datenverarbeitung statt, es wird lediglich der Zutritt zum Stadion registriert, sobald der Ticketinhaber die Drehsperre passiert hat. Damit wird gewährleistet, dass auch bei Ausfall des Netzwerkes die so genannte "Anti-Pass-Back-Funktion" (Vermeidung von unberechtigten Doppeleintritten) erhalten bleibt.

Nach dem Spielbesuch kann der Ticketinhaber selbstverständlich das Ticket und damit den Chip ohne weiteres vernichten. Das beispielsweise beim Einsatz von RFID-Chips beim Kleidungsverkauf bestehende Problem, dass der Chip nicht vernichtet werden kann oder dass damit Gewährleistungsansprüche verloren gingen, stellt sich hier nicht.

Die teilweise geäußerte Befürchtung, mittels der RFID-Technik könnte genau verfolgt werden, wann und wohin sich der Besucher im Stadion begibt, es könnten also Bewegungsprofile erstellt werden, ist nach der technischen Spezifikation, insbesondere aufgrund des Einsatzes eines Chips gemäß ISO 14443, nicht begründet.
Das Regierungspräsidium Darmstadt wird dies auch vor Ort überprüfen.

In datenschutzrechtlicher Hinsicht ist maßgeblich, dass für den Besucher Transparenz über die Datenverarbeitung hergestellt wird. Auf entsprechende Forderung des Regierungspräsidiums Darmstadt hat der DFB daher eine ausführliche Datenschutzinformation in das Ticket-Bestellformular aufgenommen. In Form so genannter FAQs (frequently asked questions = häufig gestellte Fragen) werden weitere Informationen gegeben (siehe insbesondere FAQs 14-16 sowie 42-53 a.a.O.).

Der DFB erfüllt damit seine gesetzliche Unterrichtungspflicht nach § 4 Abs. 3 BDSG und unterrichtet in Anlehnung an § 6c BDSG auch über den RFID-Einsatz. § 6c BDSG gilt zwar nur für mobile personenbezogene Speicher- und Verarbeitungsmedien, worunter die eingesetzte Chip-Technologie wohl nicht fallen dürfte; gleichwohl hatte das Regierungspräsidium Darmstadt den DFB aufgefordert, sich an den Transparenzgeboten des § 6c BDSG zu orientieren.

Durch den RFID-Einsatz erfolgt im Grunde keine weitere Beeinträchtigung des informationellen Selbstbestimmungsrechtes als durch die Personalisierung der Tickets. Im Ergebnis ist der RFID-Einsatz damit nicht zu beanstanden.

Da alle WM-Stadien mit RFID-Lesegeräten ausgestattet werden und es sich hierbei um nicht unerhebliche Investitionen handelt, besteht möglicherweise die Absicht, diese Technik auch nach der Fußball-WM einzusetzen. Von der für den jeweiligen Stadionbetreiber zuständigen Datenschutzaufsichtsbehörde wird gesondert geprüft werden müssen, inwieweit gegebenenfalls ein reduzierter Einsatz der Technik gerechtfertigt ist. Die Fälschungssicherheit und "Anti-Pass-Back"-Funktion beispielsweise kann ganz ohne Personalisierung der Tickets durch RFID gewährleistet werden.

11.1.4 Erhebung der Personalausweis- und Passnummern

Das Bundesministerium des Innern hatte im Zusammenhang mit der Personalisierung der Tickets unter anderem auch die Erhebung der kompletten Personalausweis- und Passnummern gefordert bzw. empfohlen. Daher wurde der für Bundesbehörden zuständige Bundesbeauftragte für den Datenschutz vom Regierungspräsidium Darmstadt eingebunden. Er war frühzeitig über die Problematik informiert und nahm auch an einem Gespräch beim Regierungspräsidium Darmstadt mit DFB und FIFA teil. Der Bundesbeauftragte für Datenschutz hatte das komplette Ticket-Bestellformular Anfang Dezember 2004 vom Regierungspräsidium Darmstadt erhalten. Mit Schreiben vom 26. Januar 2005 äußerte er gegenüber dem Bundesministerium des Innern, dass die Erhebung der kompletten Personalausweis- und Passnummern unzulässig sei, da jedenfalls ein Teil dieser Nummern zur Erreichung des Zwecks ausreiche.

Das Bundesinnenministerium und der DFB haben daraufhin nochmals erläutert, dass die Speicherung der kompletten Nummern erforderlich sei und welche Bedeutung ihr bei der Zutrittskontrolle zukomme:

"Die Kontrolleure sind mit Besuchern aus einer Vielzahl von Ländern mit dementsprechend unterschiedlichen Ausweispapieren in fremden Sprachen, teilweise auch in anderen Alphabeten, konfrontiert. Die vollständige Perso-

nalausweisnummer ist nach Angaben des DFB das einzige Merkmal, das sich bei allen Ausweisen schnell und einfach erkennen und mit dem hinterlegten Datum vergleichen lässt. Auch wenn zu einem gewissen Grad eine Identifizierung anhand einer verkürzten Ausweisnummer in Verbindung mit den anderen beim Ticketverkauf angegebenen Daten möglich ist, würde dies die für die Kontrolle erforderliche Zeitspanne in nicht vertretbarem Maße verlängern und die Wahrscheinlichkeit der eindeutigen Identifizierung zu sehr verringern."

Damit sichergestellt wird, dass die Pass- und Personalausweisnummern nicht entgegen dem Pass- und Personalausweisgesetz als "Ordnungsmerkmale" genutzt werden, hat das Regierungspräsidium Darmstadt dem DFB aufgegeben, dass in der Anwendungssoftware für die Ticketdatenbank jede Möglichkeit zur Nutzung als Ordnungsmerkmal ausgeschlossen bleibt. Das heißt, programmtechnisch ist sicherzustellen, dass die Datenbank weder nach Ausweisnummern geordnet noch gezielt nach einer Nummer gesucht werden kann. Im Hinblick darauf, dass sich auf den Rechnern der Anwender in der Regel weitere Standardsoftware befindet, wurde vorsorglich vorgegeben, dass beim Einsatz dieser Software sicherzustellen ist, dass die allgemeinen Suchfunktionen und Sortiermöglichkeiten nicht auf die Daten der Ticketdatenbank angewendet werden können. Zu Zwecken der Replikation darf nur Software eingesetzt werden, die keine Möglichkeit zur weiteren Verarbeitung bietet.

11.1.5 Weitere Transparenzanforderungen

Das Bestellformular enthält auch den Hinweis, dass es sich bei der Angabe der Telefonnummer, der Faxnummer und der E-Mail-Adresse um freiwillige Angaben handelt. Hierbei wird auch darauf hingewiesen, dass diese Angaben zur Kontaktaufnahme bei Unklarheiten bzgl. der Bestellung, Information über Spielverlegung etc. und über Zusatzveranstaltungen im Rahmen der WM verwendet werden sollen. Eine Nutzung zu werblichen Zwecken erfolgt also nicht, es sei denn, der Betroffene hat eingewilligt (siehe unten Nr. 11.1.6). Die Mail-Adresse wurde bei Online-Bestellungen und nur bei diesen, also nicht bei Bestellungen per Brief oder Fax, zwar als Pflichtangabe gekennzeichnet, damit die Bestellung Online eingesehen werden kann und umfassende Informationen zur Bestellung übermittelt werden können. Wie aus FAQ 16 hervorgeht, wird die Kennzeichnung als "Pflichtangabe" aber relativiert, denn der Antrag wird auch ohne diese Angabe bearbeitet und bei der Auslosung berücksichtigt. Will ein Besteller seine Einwilligung in die werbliche Nutzung erteilen, wird die E-Mail-Adresse für das vom Regierungspräsidium Darmstadt geforderte double-opt-in (siehe unten) benötigt.

Beim Datenfeld "Fan von..." soll - wie im Formular erläutert - angegeben werden, welches Nationalteam der Besteller und die anderen Personen, für die er Tickets bestellt, unterstützen. Dies dient der Fangruppentrennung, wie oben bereits ausgeführt (siehe oben Nr. 11.1.2). Das Formular sieht jedoch als Auswahlfeld auch die Angabe "neutral" für diejenigen Personen vor, die nicht in einem Fanblock, sondern im "neutralen" Bereich sitzen möchten.

11.1.6 Werbliche Nutzung

Auch die Frage der werblichen Nutzung der im Bestellformular angegebenen Daten hat das Regierungspräsidium Darmstadt eingehend mit dem DFB erörtert. Das Bestellformular enthält daher eine entsprechende Einwilligungsklausel mit dem ausdrücklichen Hinweis, dass die Erteilung dieser Einwilligung freiwillig ist und jederzeit ohne Einfluss auf den Ticketverkauf widerrufen werden kann.

Nur wenn der Besteller ankreuzt, dass er mit der Nutzung zu Werbezwecken einverstanden ist, erfolgt eine solche. Bei Online-Bestellungen ist auf die Forderung des Regierungspräsidiums Darmstadt ein so genanntes "double-opt-in" vorgesehen, d.h. die Einwilligung wird nur wirksam, wenn der Besteller noch mal per E-Mail bestätigt, dass er tatsächlich in die werbliche Nutzung einwilligt.

Die im letzten Absatz des Bestellformulares enthaltenen Formulierungen ("….Zustimmung zur Speicherung der persönlichen Daten…unbedingt erforderlich……Ich erkläre mich mit den Datenschutzbestimmungen einverstanden.") sollen den Betroffenen verdeutlichen, dass eine Kartenbestellung nur unter Angabe der Pflichtdaten möglich ist. Ein Widerspruch zur Einwil-

ligungserklärung in die werbliche Nutzung im vorletzten Absatz besteht nicht, denn die Einwilligungserklärung ist eindeutig so formuliert und gestaltet (mit Ankreuzkästchen), dass klar ist, dass die Kartenbestellung völlig unabhängig von der Abgabe der Einwilligung in diese spezielle Nutzung der Daten ist.

Das Regierungspräsidium Darmstadt hat also von vornherein durchgesetzt, dass eine werbliche Nutzung nur mit Einwilligung erfolgt. Teilweise scheint in der Öffentlichkeit der fälschliche Eindruck entstanden zu sein, dass dies erst nach Beginn des Ticketverkaufs durch eine Klage der Verbraucherzentrale Bundesverband erreicht wurde.

Die Verbraucherzentrale Bundesverband forderte jedoch keine inhaltliche Änderung, sondern nur, dass das Formular "optisch noch eindeutiger gestaltet wird". Man einigte sich hier auf die marginale Änderung, dass der Freiwilligkeitshinweis unter die Ankreuzmöglichkeit gesetzt wird, statt - wie ursprünglich - als einleitender Satz unter der Überschrift "Einwilligung unter die werbliche Nutzung".

Wie sich aus dem Wortlaut der Einwilligungserklärung ergibt, werden nur die Daten des "Bestellers/Antragstellers" für werbliche Zwecke genutzt, also nur die Daten desjenigen, der das Formular ausfüllt, nicht aber die Daten der anderen Personen, für die er Karten mitbestellt. Dies wird durch die Begriffsbestimmungen in den FAQ 25 und 26 bestätigt.

Da einige "Marketing-Partner" (Sponsoren etc.) ihren Sitz außerhalb der Europäischen Union und der Vertragsstaaten des Europäischen Wirtschaftsraumes haben dürften, das heißt außerhalb des Geltungsbereichs der EG-Datenschutzrichtlinie, hat das Regierungspräsidium Darmstadt auch dieses spezielle Thema mit dem DFB erörtert. Der DFB selbst wird zwar keine personenbezogenen Daten an Stellen außerhalb der EU übermitteln, es ist aber nicht ausgeschlossen, dass die FIFA dies tun könnte. Aufgrund der Forderung des Regierungspräsidiums Darmstadt enthält die Einwilligungsklausel folgenden Passus:

"Eine Übermittlung in Staaten außerhalb der EU erfolgt nur, wenn beim Empfänger ein angemessenes Datenschutzniveau besteht oder vertraglich für ausreichende Garantien gesorgt wird."

Dies orientiert sich an den Vorgaben der EG-Datenschutzrichtlinie für einen solchen Datentransfer an Stellen außerhalb der EU.

11.1.7 Datensicherheit

Selbstverständlich wurde auch das Thema Datensicherheit mit dem DFB erörtert. Der DFB hat aufgrund dieser Erörterungen erkannt, dass eine eingehende Aufarbeitung notwendig ist und dass diese Aufgabe am besten bewältigt werden kann, wenn er sich professioneller Hilfe bedient. Daher hat der DFB einen erfahrenen externen Dienstleister damit beauftragt, ein Datensicherheitskonzept zu erstellen. Dieses soll alle Schritte der Datenverarbeitung erfassen, vom Ticketverkauf und der Ticketverlosung - insoweit ist das Konzept bereits fertig gestellt - bis zur Datenübermittlung in die Stadien und die dortige Verarbeitung.

11.1.8 Andere Vertriebswege

Tickets werden auch über die ausländischen Fußball-Verbände und über Sponsoren verteilt. Hierbei sollen nach Kenntnisstand bei Redaktionsschluss für diesen Bericht im Wesentlichen die gleichen Daten erhoben werden wie beim Direktverkauf.

Bei diesen Datenerhebungen gelten somit - soweit das BDSG anwendbar ist - die gleichen datenschutzrechtlichen Anforderungen wie beim Direktverkauf.

Das Regierungspräsidium Darmstadt hat daher den DFB aufgefordert, durch vertragliche Regelungen mit den Sponsoren dafür zu sorgen, dass eine einheitliche Umsetzung der oben genannten Anforderungen an die Transparenz der Datenverarbeitung und bzgl. der werblichen Nutzung der Daten gewährleistet ist.

Soweit der DFB bzw. die Polizei eine Videoüberwachung in den Stadien plant, wird sich das Regierungspräsidium Darmstadt mit dem Hessischen Datenschutzbeauftragten abstimmen.

Das Regierungspräsidium Darmstadt wird die Erfüllung der gesetzlichen Anforderungen weiterhin verfolgen und kontrollieren.

11.2 Akkreditierung
11.2.1 Personenkreis, Zuverlässigkeitsüberprüfung, Hintergrund

Im Rahmen der WM 2006 ist es erforderlich, dass Personen, die bestimmte Funktionen im Stadion erfüllen, eine Akkreditierung und damit Zugangsberechtigung erhalten. Dies betrifft Mitarbeiter des Organisationskomitees und der FIFA, Spieler, Schiedsrichter, Medienvertreter (Journalisten, Fotografen), Servicepersonal (Reinigungskräfte, Gärtner etc.) und freiwillige Helfer (Volunteers). Insgesamt wird es sich um ca. 150.000 bis 200.000 Personen handeln.

Die Akkreditierung kann für alle Spiele und alle Stadionbereiche erfolgen oder differenziert nur für ein Spiel oder bestimmte Bereiche.

Der Unterausschuss "Führung, Einsatz, Kriminalitätsbekämpfung" des Arbeitskreises II ("Inneres, Sicherheit") der Innenministerkonferenz hatte eine Projektgruppe gebildet, die ein polizeiliches Rahmenkonzept für die WM 2006 erarbeitete.

Die Projektgruppe wies darauf hin, dass die zuständigen Polizeiführer bei der WM 2006 innerhalb kürzester Zeit umfassende Lagebeurteilungen durchzuführen und komplexe Entscheidungen zu treffen haben werden. Von erheblicher Bedeutung für fundierte Entscheidungen werde sein, dass die Polizeiführer davon ausgehen können, dass die Zuverlässigkeit derjenigen Personen, die über besondere Zugangs- und Aufenthaltsrechte in den Sicherheitsbereichen der Stadien verfügen (akkreditierte Personen), zuvor festgestellt worden ist.

Daher soll der gesamte Personenkreis im Rahmen des Akkreditierungsverfahrens einer polizeilichen Zuverlässigkeitsüberprüfung unterzogen werden. Eine Differenzierung, d.h. die Ausnahme eines Teils der zu akkreditierenden Personen von der Zuverlässigkeitsüberprüfung, komme aus polizeilichen Gründen nicht in Betracht. Die Projektgruppe betont, dass diese Zuverlässigkeitsüberprüfung ein Kernelement der gesamten Sicherheitskonzeption für die WM 2006 darstellt. Dieses ist eine Forderung und Bedingung der FIFA für die Austragung der Fußball-WM 2006 in Deutschland.

Die Akkreditierung für die WM beginnt voraussichtlich im September 2005.

11.2.2 Einwilligung, Information

Diese Zuverlässigkeitsüberprüfungen dürfen nicht hinter dem Rücken der Betroffenen durchgeführt werden, sondern nur, wenn die Betroffenen bereits bei der Stellung des Akkreditierungsantrages informiert wurden und zugestimmt haben. Sie müssen wissen und entscheiden können, ob sie unter diesen Voraussetzungen einen Akkreditierungsantrag stellen.

Eine wirksame Einwilligung setzt eine umfassende Information voraus. Da der DFB verantwortliche Stelle für die Datenübermittlung an die Polizei ist - so auch seine eigene Einschätzung -, wäre es an sich Sache des DFB, einen entsprechenden Text für eine informierte Einwilligung zu entwerfen. Der DFB war dabei jedoch auch auf die Informationen der Polizei über den konkreten Ablauf und Umfang der Zuverlässigkeitsüberprüfung angewiesen. Daher beauftragte die Projektgruppe das Innenministerium Baden-Württemberg (Landespolizeipräsidium) mit der Erarbeitung eines Entwurfs. Dieses stimmte sich mit dem Regierungspräsidium Darmstadt ab.

In einigen Punkten war der Entwurf bei Redaktionsschluss für diesen Bericht noch zu ergänzen bzw. zu präzisieren, wobei dies von den definitiven Entscheidungen der Sicherheitsbehörden zum Umfang und Ablauf des Verfahrens abhängt. Sollte auch der Verfassungsschutz in die Überprüfung einbezogen werden, was ursprünglich nicht beabsichtigt war, müsste selbstverständlich auch hierüber informiert werden.

Bei Redaktionsschluss für diesen Bericht hatte das Innenministerium Baden-Württemberg mit der Überarbeitung und Ergänzung des Entwurfs begonnen. Dieser wird mit der Projektgruppe und dem Regierungspräsidium Darmstadt abgestimmt werden, welches erneut den Düsseldorfer Kreis beteiligen wird.

Eine besondere Situation besteht, wenn die zu akkreditierenden Personen das Akkreditierungsformular nicht selbst ausfüllen, sondern deren Arbeitgeber dies für sie erledigt. Dies wird voraussichtlich bei Service-Personal, eventuell bei Medienvertretern und unter Umständen noch bei weiteren Personen der Fall sein.

Selbstverständlich darf die Transparenz des Verfahrens hierunter nicht leiden und das Einwilligungserfordernis darf nicht missachtet werden. Der Arbeitnehmer muss daher zum einen umfassend darüber informiert werden, welche Daten sein Arbeitgeber an den DFB übermittelt und er muss zum anderen - wie bei einem direkten Akkreditierungsantrag - über die Datenverarbeitung beim DFB und insbesondere über die Zuverlässigkeitsüberprüfung informiert werden und in beides einwilligen.

Auf Forderung des Regierungspräsidiums Darmstadt hat der DFB einen entsprechenden Entwurf gefertigt. In einigen Punkten bestand, abgesehen von der ohnehin erforderlichen Überarbeitung der Datenschutzinformation für die Zuverlässigkeitsüberprüfung, bei Redaktionsschluss für diesen Bericht noch Klärungs- und Ergänzungsbedarf. Das Regierungspräsidium Darmstadt wird dies weiter verfolgen.

Die vom Arbeitgeber eingeholten Einwilligungen sollen bei diesem verbleiben, bis drei Monate nach dem Ende der WM aufbewahrt und dann vernichtet werden.

Damit sichergestellt ist, dass die Unternehmen alle diese Vorgaben beachten, hat der DFB auf Forderung des Regierungspräsidiums Darmstadt eine entsprechende Erklärung entworfen, die von den Verantwortlichen in den Unternehmen zu unterzeichnen ist. Um Missbrauch zu vermeiden, müssen diese auch versichern, dass sie die Akkreditierungen nur im Rahmen des Erforderlichen, das heißt nur für diejenigen Personen beantragen werden, die nach der bisherigen Planung für Arbeitseinsätze im Rahmen der WM 2006 vorgesehen sind. In diesen Erklärungen lässt sich der DFB das Recht einräumen, stichprobenhafte Überprüfungen durchzuführen. Ferner wird darauf hingewiesen, dass die Kontrollbefugnisse der zuständigen Datenschutzaufsichtsbehörden unberührt bleiben.

11.2.3 Information der Betroffenen bei Bedenken

Ist die Zuverlässigkeitsüberprüfung abgeschlossen, ist nach bisherigem Konzept der Projektgruppe vorgesehen, dass das zuständige Landeskriminalamt dem DFB (Organisationskomitee) je nach Ergebnis die Zuverlässigkeit bescheinigt ("keine Bedenken") oder mitteilt, dass Bedenken gegen eine Akkreditierung bestehen ("Bedenken"). Die Einzelheiten bzw. Gründe für die Bedenken werden dabei aber dem DFB nicht genannt.

Der jeweilige Arbeitgeber des Servicepersonals würde bei negativem Ergebnis der Zuverlässigkeitsüberprüfung also die Mitteilung erhalten "Akkreditierung abgelehnt" mit der expliziten oder impliziten Begründung "wegen Bedenken aufgrund der Zuverlässigkeitsüberprüfung".

Es besteht jedoch die Sorge, dass es zu unberechtigten und vorschnellen arbeitsrechtlichen Konsequenzen kommen könnte, insbesondere wenn bei der Zuverlässigkeitsüberprüfung versehentlich unzutreffende bzw. überholte Informationen zu Grunde gelegt wurden. Mag dies auch nachträglich wieder aufgeklärt werden können, sind dem Betroffenen möglicherweise doch Nachteile entstanden. In einigen Bereichen, in denen spezielle gesetzliche Vorschriften Zuverlässigkeitsüberprüfungen durch die zuständigen Behörden (Luftsicherheits- bzw. Atombehörde) vorschreiben und regeln (vgl. § 12b Atomgesetz und § 7 Luftsicherheitsgesetz), hat der Gesetzgeber diese Behörden verpflichtet, den Betroffenen vor der Entscheidung Gelegenheit zu geben, sich zu den eingeholten Auskünften zu äußern, soweit diese Zweifel an seiner Zuverlässigkeit begründen und Geheimhaltungsvorschriften nicht entgegenstehen.

Diese spezialgesetzlich geregelten Überprüfungen gehen vom Umfang her weit über das hinaus, was nach bisherigem Stand bei der WM geplant ist. Die darin enthaltene gesetzgeberische Wertung, dass die schutzwürdigen Belange der Betroffenen es grundsätzlich gebieten, dass diese über das Ergebnis der Zuverlässigkeitsüberprüfungen unterrichtet werden, bevor gegenüber dem Arbeitgeber die Akkreditierung abgelehnt wird, sind jedoch auch bei der WM zu berücksichtigen.

Auch die Projektgruppe hat sich daher mit dieser Problematik befasst, ist jedoch zu dem Ergebnis gelangt, dass eine direkte Information der Betroffenen faktisch nicht durchführbar ist, weil für die Überprüfung von annähernd 200.000 Personen lediglich ein Zeitraum von etwa drei Wochen zur Verfügung steht. Wenn relevante polizeiliche Erkenntnisse zu einer Person vorliegen, muss eine individuelle Beurteilung zur Frage erfolgen, ob eine Empfehlung oder eine Ablehnung ausgesprochen werden soll. Dies beansprucht entsprechende Sorgfalt und Zeit.

Soweit aber die Zeitvorgaben des DFB oder der FIFA zu enge Grenzen für die Zuverlässigkeitsüberprüfung setzen, halten die Datenschutzaufsichtsbehörden es für erforderlich, dass der DFB im Interesse der Betroffenen auf eine Vergrößerung des Zeitfensters hinwirkt.
Durch eine zeitliche Streckung dürfte sich auch das von der Projektgruppe geschilderte Problem, dass ein Arbeitgeber allein schon aus dem Fehlen der Akkreditierung zwangsläufig auf das Vorhandensein von "Bedenken" bezüglich der Zuverlässigkeit schließen kann, erledigen.

Aufgrund der Abstimmung im Düsseldorfer Kreis hat der Vorsitzende des Düsseldorfer Kreises ein entsprechendes Schreiben an den DFB gerichtet.

Bei Redaktionsschluss für diesen Bericht war noch kein abschließendes Ergebnis erzielt.

Ein vertiefendes Gespräch mit allen Beteiligten (DFB, FIFA, Sicherheitsbehörden, Regierungspräsidium Darmstadt, weitere Aufsichtsbehörden) wird erwogen. Möglicherweise können die beim Confederationscup gewonnenen Erfahrungen zu einer einvernehmlichen Lösung beitragen.

11.2.4 Spezielle gesetzliche Regelung?

Zwischen den Datenschützern im Bundesgebiet wurde diskutiert, ob die Einwilligungen eine ausreichende Rechtsgrundlage, insbesondere für Datenabgleiche bei den Sicherheitsbehörden darstellen, ob diese Abgleiche durch das jeweilige Polizeirecht gedeckt sind oder ob eine spezielle Rechtsgrundlage erforderlich sei. Soweit ersichtlich, ist nur in Rheinland-Pfalz eine spezielle Regelung im Polizeirecht vorhanden.

Da die rechtzeitige Schaffung spezieller gesetzlicher Regelungen im Bund und den Ländern nicht möglich erschien, bestand Einigkeit, die gemeinsamen Bestrebungen auf die datenschutzgerechte Ausgestaltung des Verfahrens zu konzentrieren.

Aus datenschutzrechtlicher Sicht sind Einwilligungen im Arbeitnehmerbereich in der Tat kritisch zu sehen, da es aufgrund der arbeitnehmertypischen Abhängigkeit an der Freiwilligkeit fehlen kann. Welche Auswirkungen die Verweigerung der Einwilligung zum Akkreditierungsverfahren im Einzelfall haben wird, lässt sich kaum voraussehen. Die Verweigerung hat keine Nachteile für den Arbeitnehmer, wenn sie sich nicht auf das Arbeitsverhältnis auswirkt, z.B. wird eine Reinigungskraft statt bei der WM zur Reinigung eines öffentlichen Gebäudes eingesetzt. Gleichwohl ist nicht zu verkennen, dass es negative Konsequenzen haben könnte. Allerdings ist zu berücksichtigen, dass es auch andere Bereiche gibt, in denen die Einwilligungen nicht völlig frei sind, z.B. bei Versicherungsverträgen oder Bankdarlehen. Einen Kreditvertrag kann man faktisch nicht zu vernünftigen Konditionen erhalten, wenn man nicht bereit ist, die SCHUFA-Klausel zu unterschreiben. Eine private Krankenversicherung kann nur abschließen, wer bereit ist einzuwilligen, dass seine Gesundheitsangaben durch Nachfrage bei Ärzten überprüft werden (siehe oben Nr. 9.3). Letztlich ist die Freiwilligkeit relativ, maßgeblich war in diesen Fällen für die Aufsichtsbehörde, ob ein so genannter "legitimer Zwang" im Sinne einer legitimen Koppelung besteht. Hier spielen also Wertungen und Abwägungen zwischen den widerstreitenden Interessen eine Rolle.

Angesichts des besonderen Gefährdungspotentials bei der WM 2006 würde man die Einwilligung schwerlich als unwirksam oder unzureichend einstufen können.

Bezüglich des Datenabgleichs bei der Polizei hatte der Hessische Datenschutzbeauftragte schon in der Vergangenheit in besonderen Fällen, die nicht durch spezielle Regelungen abgedeckt waren, anerkannt, dass Zuverlässigkeitsüberprüfungen notwendig sind und hat keine Einwände erhoben (vgl. 28. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Drucks. 15/1101, unter Nr. 5.4).

Die Fußball-WM 2006 ist ein singuläres Ereignis und rechtfertigt als solches nicht die Schaffung einer speziellen gesetzlichen Regelung. Andererseits könnten zukünftig auch andere Großereignisse vergleichbar umfangreiche und sensible Datenverarbeitungen erforderlich erscheinen lassen. In diesem Fall könnte durch eine spezielle Rechtsgrundlage Rechtssicherheit geschaffen würde. Dies wird bei künftigen Gesetzgebungsvorhaben zu erwägen sein.

12. Datenschutzkonforme Videoüberwachung

Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist und wird wohl noch zukünftig ein Dauerthema für die Aufsichtsbehörden darstellen.

Auf der einen Seite sind die Befürworter und Anwender, auf der anderen Seite stehen diejenigen Betroffenen gegenüber, die ihre Persönlichkeitsrechte durch die mögliche Beobachtung beeinträchtigt sehen. Ohne auf einzelne der zahlreichen den Aufsichtsbehörden vorgetragenen Beschwerden näher einzugehen, sollen hier die wesentlichen Probleme beleuchtet werden. Zunächst ist ein einheitlicher Trend dahingehend zu beobachten, dass die Aufnahmegeräte (Videokameras) kleiner werden und mit digitaler Technik ausgestattet sind. Hinzu kommt in weiten Bereichen der Bevölkerung und Unternehmen ein ausgeprägtes Sicherheitsbedürfnis, welches allerdings auf einem sehr niedrigen Kostenniveau befriedigt werden soll. Oft wird weder die Frage, warum an diesem Ort ein besonderes Risiko für die persönliche Sicherheit und im Hinblick auf die Sicherung von Sachwerten vor Zerstörung, Gewaltanwendungen, Diebstahl und Vandalismus vorhanden ist, noch die weitere Frage nach alternativen Möglichkeiten einer Absicherung geprüft, sondern an erster Stelle der Sicherheitsmaßnahmen die Videoüberwachung gesehen.

Den Aufsichtsbehörden werden oftmals Sachverhalte vorgetragen, bei denen es zu einer sofortigen Einstellung der Videobeobachtung kommen muss, weil weder ein berechtigtes und überwiegendes Interesse für einen festgelegten Zweck vorliegt, noch die Wahrnehmung des Hausrechts dieses einschneidende Mittel begründen könnte.

Im Berichtszeitraum gab es zahlreiche Beispiele für die voreilige Installation von Videoüberwachungssystemen.

Ein Hausbesitzer beobachtete vorsichtshalber nicht nur seinen Hauseingang, sondern gleich den Bürgersteig und den daneben befindlichen Zugangsbereich einer Imbisseinrichtung, weil an der Eingangstür zu seinem Haus einmal ein Papierkorb angezündet worden war.

Ein Bordellbesitzer war auch im Bereich Objektüberwachung tätig und hatte hier noch Monitore und Kameras übrig, die er dann für die Beobachtung des Eingangs zu einem Gebäudekomplex verwendete, in dem sich neben dem Bordellbetrieb noch eine Vielzahl von Mietwohnungen befindet. Seine Begründung war, dass er, wenn ein Besucher anläutete, bequem vom Sessel aus beobachten konnte, wie der Besucher aussieht und ob er geeignet dafür ist, dass ihm Einlass gewährt wird oder nicht. Auf den Hinweis, dass er neben seinen Besuchern auch die übrigen Bewohner des Hauses und deren Besucher beobachtete, antwortet er nur, dass es kurzweilig sei, auf dem Monitor beobachten zu können, dass sowohl Hausbewohner wie auch Besucher des Öfteren zögerten, ob sie nicht doch mal die Klingel seines Gewerbebetriebes betätigen sollten, bevor sie sich dann doch für die Wohnungsklingel entscheiden würden.

Daneben werden der Aufsichtsbehörde aber auch häufig Vorgänge geschildert, die schwierige Probleme in der Güterabwägung mit sich bringen. Wenn eine Sicherheitsbehörde dem Hausbesitzer zur Installation einer Vi-

deoüberwachung rät, weil nach dem fünften Einbruch in das Gebäude oder der zehnten Graffitiverwüstung der Hauswand keine Möglichkeiten anderer Art zur Einschränkung derartiger Vorkommnisse gesehen werden, ist die Entscheidung, wie weitgehend der Eingriff in die Persönlichkeitsrechte einer Vielzahl Unbeteiligter zumutbar ist, angesichts der berechtigten Bedürfnisse der von den Zerstörungen Betroffenen sehr schwierig. Dies gilt insbesondere, weil in den meisten dieser Fälle nachweisbar ist, dass nach der Installation des Videoüberwachungssystems z.B. Zerstörungen nicht mehr vorgekommen sind. Wird die Videoüberwachung dann zu sehr eingeschränkt und es kommt wieder zu Zerstörungen, kann es leicht zu ungerechtfertigten Urteilen wie "der Datenschutz ist mal wieder Täterschutz" kommen.

Wird die Videoüberwachung als erforderlich angesehen, wird von der anderen Seite darauf verwiesen, dass der Datenschutz nicht greife. Ein Beispiel sei nachfolgend genannt.

Im Regierungsbezirk Darmstadt befindet sich eine Kleinstadt, in welchem der Vandalismus so zugenommen hatte, dass die zuständige Polizeibehörde und die betroffenen Geschäftsleute sich nicht mehr weiter zu helfen wussten und als letztes Mittel schließlich Videoüberwachungssysteme installierten. Nun sind in dieser Kleinstadt auf etwa 100 Meter Länge einer Geschäftsstraße - und dieses auf mehreren Straßen - im Durchschnitt zehn Videokameras zu finden. Seit Beginn der Installation herrschen wieder "normale" Verhältnisse auf den Geschäftsstraßen. Problematisch ist, dass viele Kameras Teile des öffentlichen Raumes wie Bürgersteig und Parkplätze in ihren Beobachtungsbereich mit einbeziehen. Das absolute Verbot der Beobachtung öffentlicher Räume durch Private und die Beschränkung auf den Privatbereich aber würde den Zweck der Einrichtung infrage stellen, da die Identifizierung eines Täters nicht mehr möglich wäre, wenn nur die Gebäudeteile, die nicht mehr zum öffentlichen Bereich gehören, beobachtet würden. Hilfreich ist hier das Urteil des Amtsgerichts Berlin vom 18. Dezember 2003 (Az. 16 C 427/02), wonach es gerechtfertigt sein kann, einen öffentlichen Weg in der Breite von einem Meter ab der Hauswand des unmittelbar angrenzenden Geschäftshauses in die Videoüberwachung einzubeziehen. Dies wird in die Abwägung einbezogen werden und es wird nun Zug um Zug der in der Beobachtung befindliche öffentliche Raum soweit wie möglich und erforderlich eingeschränkt und somit hoffentlich eine ausreichende Lösung gefunden.

13. Datenverarbeitung in einer internationalen Hotelgruppe

Ein Hotelgast hatte in seinem Hotelzimmer ein Informationsblatt vorgefunden, in dem darauf hingewiesen wurde, dass seine Daten zum Zwecke des Direktmarketings unter Umständen an Hotels auf der ganzen Welt weitergegeben würden. Auf dem Informationsblatt waren eine E-Mail-Adresse, Postanschrift und Fax-Nummer eines Unternehmens in den USA angegeben, an das er sich wenden könne, falls er diese Weitergabe und Nutzung seiner Daten nicht wünsche.

Empört fragte der Hotelgast, ob diese Datenweitergabe denn zulässig sei und ob er sich denn nicht wenigstens an eine Stelle in Deutschland wenden könne.

Bei der Prüfung der Aufsichtsbehörde stellte sich heraus, dass das Unternehmen, welches das Hotel betreibt, zu einer großen internationalen Hotelgruppe gehört. Die Unternehmen der Gruppe sind zum Teil nur durch Kooperationsverträge (Franchising) verbunden. Da das Informationsblatt in allen Unternehmen der Gruppe in Deutschland verwendet wurde, führte das Regierungspräsidium Darmstadt Verhandlungen mit einem deutschen Rechtsanwalt, der die gesamte Gruppe vertrat. Dies gestaltete sich langwierig, da der Bevollmächtigte sich mit der US-"Zentrale" der Hotelgruppe abstimmen musste und es auch zu Abstimmungen innerhalb der Gruppe kam.

Bei diesem Unternehmen in den USA befindet sich der zentrale Buchungs- und Reservierungs-Server der Hotelgruppe. Da dieses Unternehmen und dessen Tochtergesellschaften in den USA Safe-Harbor-zertifiziert sind, war die Übermittlung der Buchungs-/Reservierungsdaten an dieses Unternehmen nicht zu beanstanden. Aufgrund der Safe-Harbor-Zertifizierung ist davon auszugehen, dass ein angemessenes Datenschutzniveau i.S.d. § 4b Abs. 2 und 3 BDSG bei dem Datenempfänger besteht.

Den Anforderungen des § 4 Abs. 3 Nr. 1 BDSG wurde jedoch nicht genügt, indem lediglich der unvollständige Name des US-Unternehmens und dortige

Kontaktdaten im Informationsblatt genannt wurden, wobei auch nicht die Postanschrift der US-Zentrale, sondern lediglich eines "EU-Datenschutzbüros" in den USA angegeben war.

§ 4 Abs. 3 Nr. 1 BDSG verlangt, dass der betroffene Hotelgast über die Identität der verantwortlichen Stelle unterrichtet wird. Verantwortliche Stelle ist aber zunächst diejenige juristische Person, die das Hotel betreibt, welches die Daten des Kunden erhebt. Der Hotelgast kannte aber nur den "Markennamen", unter dem das Hotel betrieben wird. Aufgrund des Franchisekonzeptes wird dieser Name von vielen Hotels verwendet. Die jeweils dahinter stehenden Einzelunternehmen firmieren unter ganz anderen Bezeichnungen, z.B. "xy Hotelbetriebs GmbH". Auch für die Aufsichtsbehörde war daher einiger Ermittlungsaufwand erforderlich, um die primär verantwortliche Stelle festzustellen. Der Bevollmächtigte verwies im Prüfungsverfahren darauf, dass sich Hotelgäste Namen wie "xy Hotelbetriebs GmbH" nicht merken könnten, auch sei es für die Hotelgruppe von Nachteil, wenn statt eines einheitlichen Formulars sehr viele verschiedene Formulare gedruckt werden müssten. Nach § 4 Abs. 3 Nr. 1 BDSG ist es jedoch unerlässlich, dass die Hotelgäste Kenntnis über die primär verantwortliche Stelle erhalten, bei der sie ihre Rechte nach § 6 Abs. 1 BDSG geltend machen können und nicht nur an eine zentrale Stelle verwiesen werden.

Schließlich einigte man sich darauf, dass ein neues Informationsblatt erstellt wird und hierauf die "lokalen" GmbHs, also Betreiber des jeweiligen Hotels, durch Aufdruck auf einem Freifeld angegeben werden. Eine einheitliche "Anlaufstelle" für die gesamte Hotelgruppe kann darüber hinaus genannt werden - als zusätzliches Serviceangebot. Dies geschah auch, in dem im neuen wie im alten Merkblatt zusätzlich eine US-Stelle genannt wurde.

Bezüglich der werblichen Nutzung ist im neuen Informationsblatt klargestellt, dass Hotelgäste bereits bei der Datenerhebung ihren Widerspruch geltend machen können. Dies ist auf jeden Fall die datenschutzfreundlichere Lösung, als die Hotelgäste – wie im alten Merkblatt – nur an eine Stelle in den USA zu verweisen. Die Hotelgäste haben nun also die Wahl.

Ursprünglich war vorgesehen, dass die Daten von den USA aus auch an andere Hotels der Gruppe zu Werbezwecken weitergegeben werden könnten. Auf diese Weise hätte es zu Übermittlungen in andere Drittstaaten außer den USA kommen können. Durch ein "Inter-Company-Agreement" (Unternehmensrichtlinie) sollte sichergestellt werden, dass alle Unternehmen der Gruppe zumindest das Maß an Schutz personenbezogener Daten gewährleisten, das in den Grundsätzen von Safe Harbor gefordert wird. Nachfragen der Aufsichtsbehörde bzgl. dieser Regelungen gaben den Anstoß für eine neue grundsätzliche Diskussion innerhalb der Unternehmensgruppe. Als Ergebnis teilte der Bevollmächtigte mit, dass keine Weiterübermittlung an andere Unternehmen für Werbezwecke erfolgt.

Über den zentralen Buchungs- und Reservierungsserver werden Daten nur noch an andere Unternehmen (Hotels der Gruppe) übermittelt, soweit dies für die Hotelreservierung erforderlich ist (beispielsweise: In einem Hotel der Gruppe in Frankfurt bucht ein Gast ein Hotelzimmer in Mexiko). Diese Übermittlungen in andere Drittstaaten (Mexiko im Beispielsfall) bewegen sich daher im Rahmen des § 4c Abs. 1 Nr. 1 BDSG. Der "Umweg" über den zentralen Rechner in den USA ist aufgrund der Safe-Harbor-Zertifizierung gerechtfertigt. Im neuen Merkblatt ist dies entsprechend beschrieben.

Da die Hotels der Gruppe über das gesamte Bundesgebiet verstreut sind und daher nicht ausschließlich die Zuständigkeit des Regierungspräsidiums Darmstadt gegeben ist, legte der Bevollmächtigte zu Recht Wert darauf, dass das neue Merkblatt von allen Aufsichtsbehörden im Bundesgebiet akzeptiert werde. Bei der daraufhin herbeigeführten Abstimmung im Düsseldorfer Kreis bestand Einigkeit, dass mit dem neuen Merkblatt die datenschutzrechtlichen Pflichten erfüllt werden und dass dieses spätestens beim Einchecken zur Verfügung gestellt werden muss.

Wiesbaden, 30. November 2005

Der Hessische Ministerpräsident:
Koch

Der Hessische Minister des Innern und für Sport:
Bouffier