18. Wahlperiode

Drucksache **18/1015**

HESSISCHER LANDTAG

01. 09. 2009

Vorlage
der Landesregierung

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

Vorgelegt mit der Stellungnahme zum Siebenunddreißigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten (Drucks. 18/106) nach § 30 Abs. 2 des Hessischen Datenschutzgesetzes in der Fassung vom 7. Januar 1999.

Eingegangen am 1. September 2009 · Ausgegeben am 8. September 2009
Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

Überblick und Statistiken

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

1.1 Bearbeitung von aktuellen Eingaben und Beschwerden

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

Im Berichtsjahr wurden von der Aufsichtsbehörde **in 850 Fällen** (im Vorjahr: 658) Überprüfungen von nicht öffentlichen Stellen vorgenommen, die Datenverarbeitung nach § 28 BDSG für die Erfüllung eigener Geschäftszwecke betreiben oder personenbezogene Daten nach §§ 29, 30 und § 6b BDSG zur personenbezogenen oder anonymisierten Übermittlung speichern und nutzen.

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

Die **850 Überprüfungen** aufgrund von Eingaben, Beschwerden und Pressemeldungen durch das Regierungspräsidium Darmstadt betrafen:

- in 143 Fällen Telemedienanbieter (Anbieter von Internetdiensten und Internetinhalten),
- in 142 Fällen eine große Auskunftei,
- in 118 Fällen Unternehmen im Adresshandel- und Direktmarketingbereich,
- in 102 Fällen Banken, Kreditinstitute und EDV-Dienstleister im Zahlungsverkehr,
- in 59 Fällen den Datenschutz in Arbeitsverhältnissen und bei Arbeitsvermittlern,
- in 54 Fällen (andere) Handels- und Wirtschaftsauskunfteien,
- in 52 Fällen die Videoüberwachung von Grundstücken, Häusern und Wohnungen,
- in 25 Fällen Versicherungsgesellschaften,
- in 25 Fällen Unternehmen der Freizeit-, Touristik- und Reisebranche,
- in 21 Fällen Unternehmen des Groß- und Einzelhandels,
- in 20 Fällen das Gesundheitswesen (Ärzte, Krankenhäuser, Senioren- und Pflegeheime),
- in 19 Fällen Inkassounternehmen,
- in 16 Fällen Vereine (Sport, Soziales, Kultur) sowie deren Landes- und Bundesverbände,
- in 13 Fällen Kreditkartenunternehmen,
- in 12 Fällen Vermieter sowie Wohnungs- und Immobilienverwaltungsfirmen,
- in 5 Fällen den Verlags- und Medienbereich,
- in 4 Fällen Unternehmen der Versandhandelsbranche,
- in 3 Fällen politische Parteien,
- in 2 Fällen Markt- und Meinungsforschungsunternehmen,
- in 2 Fällen Anwaltskanzleien,
- in 1 Fall die Auslandsdatenverarbeitung,
- in 12 Fällen sonstige Stellen (z. B. Briefzusteller, wegen fehlendem Verfahrensverzeichnis, nicht bestelltem Datenschutzbeauftragten)

Bei ca. **20 v.H.** der Beschwerden konnte zeitnah festgestellt werden, dass diese begründet waren: In insgesamt **168 Fällen** wurden bei den Nachfor-

schungen der Aufsichtsbehörde unzulässige Erhebungen und Verarbeitungen personenbezogener Daten und andere Verstöße gegen Vorschriften des Datenschutzrechts und des Rechts der Telemedien festgestellt, die zu Beanstandungen der jeweiligen Erhebungs- und Verarbeitungsverfahren bei den betroffenen Stellen führten.

Die bei den Überprüfungen beanstandeten **168 Verstöße** gegen Datenschutzbestimmungen wurden festgestellt:

- in 36 Fällen bei Kreditinstituten und Banken,
- in 32 Fällen bei Auskunfteien (29 Fälle betrafen dieselbe Auskunftei), davon war in 22 Fällen ein Verstoß durch den Vertragspartner der Auskunfteien ursächlich,
- in 28 Fällen bei Unternehmen im Adresshandel- und Direktmarketingbereich,
- in 22 Fällen bei Anbietern von Telemedien (Anbieter von Internetdiensten und Internetinhalten),
- in 20 Fällen bei der Videoüberwachung,
- in 6 Fällen bei der Verarbeitung von Arbeitnehmer- und Bewerberdaten,
- in 4 Fällen bei Unternehmen der Freizeit-, Touristik- und Reisebranche,
- in 4 Fällen im Groß- und Einzelhandel,
- in 4 Fällen bei Versicherungsgesellschaften,
- in 3 Fällen bei Vereinen (Sport, Soziales, Kultur) sowie deren Landes- und Bundesverbänden,
- in 2 Fällen bei Unternehmen aus dem Verlags- und Medienbereich,
- in 2 Fällen bei politischen Parteien,
- in 2 Fällen im Gesundheitswesen,

sowie in jeweils einem Fall bei einem Versandhändler, im Bereich Wohnen und Miete und einer sonstigen Stelle.

Ein Teil der eingeleiteten Überprüfungen konnten im Berichtsjahr noch nicht abgeschlossen werden. Die Erledigung dieser Fälle wird in den nächsten Tätigkeitsbericht einfließen.

1.2 Erledigung von Eingaben und Beschwerden aus den Vorjahren

Von den noch aus den Vorjahren anhängigen Beschwerden, die oftmals sehr vielschichtige Verarbeitungszusammenhänge betrafen, wurden im Berichtsjahr **185 Fälle** abgeschlossen. Die Beurteilung dieser in der Regel nur mit hohem Ermittlungsaufwand aufklärbaren Eingaben durch das Regierungspräsidium ergab, dass davon **89 Eingaben** begründet waren. Damit musste die Aufsichtsbehörde bei fast **50 v.H.** dieser Fälle einen Datenschutzverstoß feststellen.

Die beanstandeten **89 Verstöße** gegen Datenschutzbestimmungen wurden festgestellt:

- in 20 Fällen bei der Video-Beobachtung,
- in 11 Fällen bei Unternehmen der Werbewirtschaft und werbenden Einzelhändlern,
- in 9 Fällen bei einer Auskunftei,
- in 9 Fällen bei Anbietern von Telemedien (Anbieter von Internetdiensten und Internetinhalten),
- in 7 Fällen bei Arbeitgebern und Arbeitsvermittlern,
- in 6 Fällen bei Unternehmen der Freizeit-, Touristik- und Reisebranche,
- in 4 Fällen bei Kreditinstituten und Banken,
- in 3 Fällen im Gesundheitswesen,
- in 3 Fällen bei Inkassounternehmen,
- in 3 Fällen bei Versandhändlern,
- in 2 Fällen im Groß- und Einzelhandel,

- in 2 Fällen im Verlags- und Medienbereich,
- in 2 Fällen bei Versicherungsunternehmen,

sowie in jeweils einem Fall bei der Auslandsdatenverarbeitung, wegen fehlendem Verfahrensverzeichnis, nicht bestelltem Datenschutzbeauftragten, bei einem Verein, sowie bei vier sonstigen Stellen.

1.3 Anlassabhängige und anlassunabhängige Überprüfungen vor Ort nach § 38 Abs. 4 BDSG

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

Einen besonderen Schwerpunkt bildeten zum einen die Überprüfung von Videoüberwachungseinrichtungen, da hierzu erneut eine große Zahl von Beschwerden und Anfragen einging (die Tendenz ist hierzu seit Jahren steigend, Einzelfälle siehe unter Ziffern 12.2 und 13.).
Weitere Schwerpunkte lagen bei der aufwändigen Überprüfung von Lebensmittelhändlern (Discounter) im Hinblick auf deren Mitarbeiterüberwachung (Beauftragung von Detekteien, Videoüberwachung, siehe hierzu Ziffer 12.1), bei der Überprüfung von Einrichtungen der ärztlichen Kooperation (siehe hierzu Ziffer 14.1) sowie bei der Überprüfung von Auskunfteien, welche im Jahr 2009 fortgeführt wird.

Insgesamt wurden im Berichtsjahr 44 Kontrollen vor Ort durchgeführt.

Diese betrafen folgende Branchen/Bereiche:

- Videoüberwachungssysteme	20
- Ärztliche Praxen/Kliniken/Laboratorien/Verrechnungsstellen	5
- Vereine/Verbände	5
- Lebensmittelhandel/Arbeitgeber	3
- Auskunfteien	4
- Adresshandel/Direktmarketing	3
- Sonstige	4

Dabei wurden folgende Mängel am häufigsten festgestellt:

1. Voraussetzungen des § 6b Abs. 1, Abs. 3 - 5 BDSG bei der Videoüberwachung nicht erfüllt (d. h. unzulässige Videoüberwachung, keine oder zu späte Löschung der Daten etc.),
2. Voraussetzungen des § 6b Abs. 1, Abs. 3 - 5 BDSG bei der Videoüberwachung erfüllt, aber die erforderliche Information zur Videoüberwachung fehlte (§ 6b Abs. 2 BDSG),
3. Fehlendes oder inhaltlich unzureichendes Verfahrensverzeichnis (§ 4g Abs. 2 BDSG),
4. Mängel im Bereich der technisch-organisatorischen Maßnahmen (§ 9 BDSG und Anlagen),
5. Unrechtmäßige Verarbeitung (fehlende Rechtsgrundlage/ Einwilligung),
6. Fehlende Vorabkontrolle (§ 4d Abs. 5 und 6 BDSG),
7. Betrieblicher Datenschutzbeauftragter nicht bestellt bzw. mangelnde Fachkunde der zum Datenschutzbeauftragten bestellten Personen (§ 4f BDSG).

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

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

2. Bearbeitung von Anfragen zu datenschutzrechtlichen Problemstellungen und Beratungstätigkeit

2.1 Anfragebearbeitung und datenschutzrechtliche Beratung

Das Regierungspräsidium Darmstadt hatte im Berichtsjahr erneut eine hohe Anzahl von Anfragen und Beratungsersuchen zu bearbeiten. In **337 Fällen** (im Vorjahr: 289 Fälle) erfolgte die Beratung und Information von Unternehmen, Vereinen und Verbänden, Bürgerinnen und Bürgern sowie Arbeitnehmerinnen, Arbeitnehmern und Betriebsräten aktenmäßig. Die direkte telefonische Erledigung von Anfragen sowie die Übersendung von Informationsmaterial und Orientierungshilfen per E-Mail wurden bis auf wenige Ausnahmen nicht statistisch erfasst.

Die statistische Auswertung der 337 Fälle ergab folgende inhaltliche Schwerpunkte:

124 Anfragen zu Auskunfteien und Inkassounternehmen:
Ganz überwiegend Anfragen zur Rechtmäßigkeit der Tätigkeit einer Auskunftei welche schwerpunktmäßig Adressermittlungen durchführt und den Betroffenen die gesetzlich vorgeschriebenen Benachrichtigungen übersendet (95 Anfragen, siehe hierzu Ziffer 7.3); allgemeine Fragen von Betroffenen und der Presse zur datenschutzrechtlichen Zulässigkeit des Datenverarbeitungsverfahrens einer großen Auskunftei, welche schwerpunktmäßig Bonitätsauskünfte über Verbraucher erteilt (22 Fälle), u. a. Fragen zur Berechnung des Scorewerts, zur Erhebung eines Entgelts für die Eigenauskunft und zur Alters- bzw. Identitätsprüfung vor Erteilung einer Eigenauskunft; Anfragen zur Rechtmäßigkeit des Bezugs und der Verarbeitung von Schuldnerverzeichnisdaten durch eine andere Auskunftei und Fragen zu deren Praxis, personenbezogene Wirtschaftsdaten telefonisch mit den Betroffenen zu erörtern; Fragen zu den datenschutzrechtlichen Voraussetzungen für die Gründung einer neuen Auskunftei mit dem Vertragspartnerschwerpunkt beim Internethandel; Beratung von Bürgerinnen und Bürgern (Betroffenen) zur Datenverarbeitung eines Inkassounternehmens, welches Forderungen aus Internetdienstleistungen einzieht; Computermahnanrufe.

39 Anfragen zum Arbeitnehmerdatenschutz:
E-Mail- und Internetnutzung im Unternehmen (Zugriffsrecht des Arbeitgebers, Kontrollen, Vertretungsregelung, Betriebsvereinbarung, Privatnutzung); Maßnahmen der Mitarbeiterüberwachung (Videobeobachtung, GPS-Geräte, Tachografen zur Überwachung der Lenk- und Ruhezeiten von Berufskraftfahrern, Einsatz einer Software, mit deren Hilfe eine Rangfolge der Mitarbeiter entsprechend den Arbeitsergebnissen festlegt wird, Protokollierung von Mitarbeiterdaten, Einsatz einer forensischen Software); Zugriff auf PC mittels Fernsteuerungsprogramm durch Systemadministrator; Erhebung und Speicherung von Arbeitnehmerdaten zum Zweck der Notfallplanung; Datenübermittlung an den Betriebsrat und die Schwerbehindertenvertretung; Zugriffsrechte des Betriebsrats auf Personaldaten; Einführung von Whistleblowing-Hotlines/Abschluss von Betriebsvereinbarungen hierzu; Weitergabe der Teilnehmerliste zur Betriebsversammlung an den Werksschutz; Übermittlung von Personaldaten zum Zweck gesetzlich vorgeschriebener Schulungsmaßnahmen; Verpflichtung der Mitarbeiter auf das Datengeheimnis; E-Learning-Programm zum Thema Datenschutz; Mitarbeiterbefragungen; interne und externe Zustellung von Mitarbeiterpost; Internetrecherche bei Bewerbungsverfahren; Zugangskontrollen auf Baustellen.

28 Anfragen aus dem Gesundheitssektor:
Weitergabe eines augenärztlichen Gutachtens ohne Einwilligung des Betroffenen an die Fahrerlaubnisbehörde; Bestellung eines Datenschutzbeauftragten für eine Privatklinik; Auskunftspflicht eines Arztes gegenüber dem Rechtsanwalt eines Patienten; Übertragung der Rufnummer einer psychotherapeutischen Praxis bei Anruf beim Patienten; Informationsschreiben an einen Patienten zum Ablauf von Vorsorgeuntersuchungen; Weitergabe der Patientendaten durch einen Arzt im Rahmen einer Praxisauflösung bzw. der Bildung einer Gemeinschaftspraxis; Datenübermittlung im Rahmen von Laboruntersuchungen; Übermittlung von Befunden, Röntgenaufnahmen etc. an Unfallversicherungsträger und Berufsgenossenschaften; Datenverarbeitung im Rahmen von organisierten Taxisammelfahrten für Dialysepatienten; Weitergabe von Patientendaten von einem Pflegeheim an ein anderes bei Umzug des Patienten; Speicherdauer von Patientendaten bei Ärzten und

Verrechnungsstellen; Anschluss eines Praxis-PCs an das Internet; Nachweispflicht von Impfungen bei Kindern; Datenverarbeitung bei einer Klink im Rahmen einer Konzernrahmenbetriebsvereinbarung; Datenverarbeitung bei einem Rettungsdienst; Medizinische Forschung (siehe hierzu Ziffer 14.2).

27 Anfragen zu Telemedien und Internet:
Löschung von Anmeldedaten; Betrieb einer sogenannten Personensuchmaschine (siehe hierzu Ziffer 9.3 des 21. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde (Drs. 17/663); Datenspeicherung zwecks Erstellung einer Sperrliste für den Newsletterversand; Aufnahme personenbezogener Daten in zahllose Online-Verzeichnisse; Verwendung biometrischer Daten; Tipps und Informationen zum Umgang mit Link-Spam; Speicherung von IP-Nummern und Setzen von Cookies durch Telemedienanbieter; datenschutzkonforme Erhebung und Speicherung von Daten im WWW; rechtssichere Gestaltung eines Newsletters; korrekte Ausgestaltung der Online-Einwilligung (Double-Opt-In); Aufbau eines sicheren WLAN-Netzwerkes in einem Wohnhaus; datenschutzrechtliche Rahmenbedingungen beim Angebot eines Internet-Forums; Veröffentlichung einer Datenbank mit Ansprechpartnern im Internet; Fragen zum Verhalten der Nutzer von Plattformen für "soziale Netzwerke" im WWW (siehe hierzu Ziffer 9.2); Informationen zum Vorgehen gegen unerwünschte Online-Veröffentlichungen; Gestaltung der Datenschutzerklärung bei einem Internetauftritt, Tipps zum Verhalten beim Erhalt virenverseuchter E-Mails und von unverlangten E-Mails mit vermeintlichen Zugangsdaten; Stellungnahmen gegenüber Bürgerinnen und Bürgern sowie der Presse zu digitalen Straßenansichten und geodatengestützten Diensten (siehe Ziffer 9.1); Hilfestellung für Opfer von Internet-Kostenfallen (siehe hierzu Ziffer 9.2 des 21. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde (Drs. 17/663).

24 Anfragen zum betrieblichen Datenschutzbeauftragten:
Fachliche Voraussetzungen für den betrieblichen Datenschutzbeauftragten; Aus- und Fortbildungsmöglichkeiten für den betrieblichen Datenschutzbeauftragten; Fragen bzgl. der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten; mögliche Interessenkonflikte zwischen der Funktion des internen betrieblichen Datenschutzbeauftragten und anderen Tätigkeiten im Unternehmen (Geldwäschebeauftragter, Betriebsrat, IT-Leiter, Systemadministrator, sonstige IT-Mitarbeiter); Interessenkonflikt bei einem externen Datenschutzbeauftragten, der bei dem vom Unternehmen beauftragten Datenverarbeitungsdienstleister tätig ist; Bestellung einer juristischen Person zum Datenschutzbeauftragten; Einsichtsrecht in das Verfahrensverzeichnis/notwendiger Inhalt von Verfahrensverzeichnissen; Stellung der Datenschutzbeauftragten nach dem Zusammenschluss zweier Unternehmen; erforderlicher Zeitaufwand für die Ausübung der Tätigkeit des betrieblichen Datenschutzbeauftragten; Art und Umfang der Mitarbeiterschulungen.

18 Anfragen zum Datenschutz bei Banken:
Datenweitergabe an Tochter- oder Verbundunternehmen; Einsatz und Verwendung der Verbund-/Allfinanzklausel; Auslagerung von Tätigkeiten im Rahmen des § 11 BDSG; Aufzeichnung von Telefongesprächen; datenschutzrechtliche Aspekte bei der Verschmelzung und Spaltung von Kreditinstituten; Datenweitergabe an ausländische Bank bei Dividendenzahlung von ausländischem Unternehmen; Ausdruck von BIC und IBAN auf dem Kontoauszug des Zahlungsempfängers; Zulässigkeit von Zugriffen eines Softwareunternehmens auf Daten bei Wartungsarbeiten; Zugriff auf das Online-Konto eines Dritten; nach Geldwäschegesetz erforderliche Datenerhebung bei einer Kontoeröffnung.

16 Anfragen zur Datenverarbeitung im Ausland:
Fragen zu den EU-Standardverträgen (welcher Standardvertrag für welchen Übermittlungszweck, Genehmigungspflicht, Anzeigepflicht usw.) und zu Safe Harbor (Reichweite und Bedeutung der Zertifizierung); Übermittlung von Mitarbeiterdaten im Rahmen der Einführung von Personaldatenverarbeitungssystemen; Abgleich von Mitarbeiter- und Bewerberdaten gegenüber Listen, die terrorverdächtige Personen und Organisationen enthalten (Mitarbeiter-Screening); Übermittlung von Kundendaten an eine Versicherungsgesellschaft in Malta, die ihrerseits die Daten an Unternehmen in anderen Staaten weiter übermittelt; Übermittlung von Personalausweis- und Reser-

vierungsdaten von Flugpassagieren an die britischen Zoll- und Sicherheitsbehörden.

12 Anfragen zur Datenverarbeitung durch Vereine und Dachverbände:
Beratung des Deutschen Fußball-Bundes (DFB) hinsichtlich der Anwendung eines Transfervergleichssystems (Transfer Matching System) der Fédération Internationale de Football Association (FIFA); Neufassung der Ticket - AGB des DFB für Heimländerspiele; Datenspeicherung im Rahmen von Leistungstests jugendlicher Nationalspieler bzw. im Rahmen der Sichtung angehender jugendlicher Nationalspieler; Verwaltung von Mitgliederdaten; Bestellung von betrieblichen Datenschutzbeauftragten in Vereinen und Parteien; Auskunftsrecht von Vereinsmitgliedern nach § 34 Abs. 1 BDSG gegenüber ihrem Verein; Erhebung von personenbezogenen Daten der Sportler bei der Teilnahme an Wettkämpfen; Löschpflichten bei personenbezogenen Daten ausgeschiedener Vereinsmitglieder; Herausgabe von Mitgliederlisten im Verein an einzelne Mitglieder; Zulässigkeit der Veröffentlichung der personenbezogenen Daten von Vereinsmitgliedern auf der Homepage des Vereins im Internet.

12 Anfragen zur Videoüberwachung
Fragen zur Zulässigkeit der Videobeobachtung von privaten Grundstücken, von Spielplätzen und von Fahrstühlen in Wohnanlagen; Videobeobachtung eines Flussabschnittes zur Kanuzählung für eine Diplomarbeit; Videoüberwachung in einem Museumsrestaurant, in einer Spielhalle und in Taxen (zur Einrichtung eines Alarmsystems mittels Videoaufzeichnung bei Notfall).

4 Anfragen zur Werbewirtschaft
Reaktion auf unzulässige unerwünschte Telefonwerbung; Nutzung fremder Kunden- und Adressdaten durch Dritte; Auskünfte zur geplanten Gesetzesänderung zum Werbewiderspruch; Durchsetzung der Löschung personenbezogener Daten von einer Verteilerliste.

4 Anfragen aus dem Bereich Miete und Wohnen
Übermittlung von Mieterdaten durch Versorgungs- und Entsorgungsunternehmen an den Vermieter; Herausgabe von Kontoauszügen der Wohnungseigentümer durch die Hausverwaltung an den Verwaltungsbeirat zur Überprüfung der Endabrechnung.

3 Anfragen zur Markt- und Meinungsforschung
Zulässigkeit der telefonischen Befragung von ehemaligen Patienten eines Krankenhauses sowie der Verarbeitung und Nutzung der Patientendaten zu Zwecken der Marktforschung, Vorlage von Interviewerausweisen; datenschutzgerechte Gestaltung von Fragebögen eines Sozialforschungsinstitutes.

2 Anfragen zur Versicherungsbranche
Überprüfung der Einwilligungserklärung eines Versicherungsunternehmens; Verarbeitung der Daten von Mitgliedern eines Verbands im Rahmen einer Gruppenversicherung.

24 Anfragen aus unterschiedlichen Wirtschafts- und Lebensbereichen
Aufzeichnung mobiler Sprachkommunikation; Verarbeitung von Daten zu nicht vertragsgemäßem Verhalten im Telekommunikationsbereich; Datenübergabe nach dem Aufkauf eines Unternehmens; Datenverarbeitung von Schülerdaten durch eine Privatschule; Bereitstellung des Internetzugangs in einem Berufsschulinternat; Organisation eines Fanclubs; Sperrung einer "Sedcard" (Bewerbungsunterlage für Fotomodelle); Gesetzliche Aufbewahrungsfristen; Weitergabe von Kundendaten; Konzept zu Erstellung von Sicherungskopien.

2.2 Öffentlichkeitsarbeit

Vertreterinnen und Vertreter der Aufsichtsbehörde haben auch im Jahr 2008 im Rahmen von Informationsveranstaltungen diverser Veranstalter wieder Fragen zum Datenschutz beantwortet und Vorträge gehalten.

Sowohl an der Frühjahrs- als auch der Herbsttagung des Erfahrungsaustauschkreises Hessen der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. nahm die Aufsichtsbehörde teil, berichtete über die Aufsichtstätigkeit sowie die Beschlüsse des Düsseldorfer Kreises (siehe Ziffer 6) und beantwortete Fragen der anwesenden betrieblichen Datenschutzbeauftragten.

Auch bei Veranstaltungen anderer Erfahrungsaustauschkreise betrieblicher Datenschutzbeauftragter in Hessen war die Aufsichtsbehörde vertreten. Sie nahm außerdem an einem Workshop des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. zur Schaffung von Berufsregeln für betriebliche Datenschutzbeauftragte teil.

Dem Wunsch des Landesverbands der Hospitz-Vereine und des Landesverbands des Deutschen Roten Kreuzes, durch Vorträge über den Datenschutz zu informieren, konnte jeweils entsprochen werden.

Ferner hat ein Vertreter der Aufsichtsbehörde im Rahmen der Abschlussveranstaltung der Projektwoche eines Gymnasiums zu "Sozialen Netzwerken im WWW" an einer Podiumsdiskussion mit Lehrern, Eltern und Schülern sowie Internet-Experten teilgenommen (siehe hierzu Ziffer 9.2).

Schon seit mehreren Jahren besteht ein regelmäßiger Kontakt mit der Hochschule Darmstadt. Studenten des Studiengangs "Informationswissenschaft" besuchen jeweils im Sommersemester die Aufsichtsbehörde, um sich über deren Tätigkeit und aktuelle Themen aus der Aufsichtspraxis zu informieren. Im Berichtsjahr absolvierte auch wieder ein Student der Hochschule ein Praktikum bei der Aufsichtsbehörde.

Beim Girls Day am 25. April 2008 wirkte die Aufsichtsbehörde mit und erläuterte interessierten Mädchen ihre Arbeit anhand bestimmter Themen, zu denen die Mädchen aufgrund ihrer eigenen Lebenserfahrung einen Bezug haben (zum Beispiel Gefahren der Internetnutzung, Internet-Kostenfallen, Selbstschutz, Mobilfunkgebühren und Tätigkeit von Auskunfteien).

Das Angebot an Informationsmaterial, das die Datenschutzaufsichtsbehörde zu unterschiedlichsten Fragestellungen des Datenschutzrechts u. a. auch auf den WWW-Seiten des Regierungspräsidiums Darmstadt bereithält, wurde wieder gut angenommen.

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

3.1 Genehmigungsverfahren nach § 4c Abs. 2 BDSG

Eine internationale Unternehmensgruppe hatte einen komplexen Vertrag zwischen den Mitgliedsunternehmen geschlossen, der als Grundlage für Datenübermittlungen innerhalb der Gruppe dienen soll. Mit dem Vertrag sollen insbesondere die speziellen datenschutzrechtlichen Anforderungen beim Datentransfer in Staaten außerhalb der Europäischen Union und der Mitgliedstaaten der Europäischen Union erfüllt werden (siehe bereits Ziffer 3 des 21. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde (Drucks. 17/663).

Das in Hessen ansässige Unternehmen dieser Gruppe stellte nach eingehender Beratung durch die Aufsichtsbehörde einen Genehmigungsantrag nach § 4c Abs. 2 BDSG, der nach gewissen Modifikationen nun positiv beschieden werden konnte.

Bei dem Vertrag handelte es sich um einen Mehrparteienvertrag, das heißt, sämtliche europäischen und außereuropäischen Konzernunternehmen unterzeichneten den Vertrag. Die Besonderheit des Vertrags besteht darin, dass er zum einen Regelungen für den Fall enthält, dass der jeweilige Datenimporteur als eigenständige verantwortliche Stelle (Controller) fungiert. Die diesbezüglichen Vertragsbestandteile waren an die hierfür vorgesehenen Controller-Controller-Standardverträge der EU-Kommission vom Juni 2001 und Dezember 2004 angelehnt. Zum anderen enthielt der Vertrag Regelungen für den Fall, dass der Datenimporteur als Datenverarbeitungsdienstleister (Processor) fungiert. Die diesbezüglichen Vertragsbestandteile waren an den hierfür vorgesehenen Controller-Processor-Standardvertrag der EU-Kommission vom Dezember 2001 angelehnt. Im Vertrag war jedoch weder konkret genannt, welche Unternehmen überhaupt Datenimporteure sind, noch war deren Rolle (Controller oder Processor) konkret bestimmt.

Das Unternehmen hatte zunächst die Vorstellung, dass die konkrete Benennung der Datenimporteure in der Genehmigung offen bleiben und die Genehmigung somit im Voraus auch für die Datenübermittlung an künftig hinzukommende Vertragsunterzeichner erteilt werden könne. Ebenso wenig müsse benannt werden, welche Rolle ein Datenimporteur einnimmt.

Diese und weitere grundsätzliche Fragen wurden in der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises erörtert, auch im Hinblick auf einen ähnlichen Fall in einem anderen Bundesland. Hierbei wurden auch die Erörterungen auf europäischer Ebene im Zusammenhang mit den Vorschlägen von Wirtschaftsverbänden für einen alternativen Controller-Processor-Standardvertrag (siehe hierzu auch Ziffer 11) berücksichtigt.

Zwischen den Aufsichtsbehörden bestand Einigkeit, dass eine Genehmigung nur erteilt werden kann, wenn die Datenimporteure und deren Rolle konkret benannt werden. Daraus folgt, dass beim Hinzukommen weiterer Konzernunternehmen als Datenimporteure hierfür eine zusätzliche Genehmigung beantragt werden muss. Selbstverständlich bleiben bereits erteilte Genehmigungen unberührt.

Im konkreten Fall fungieren alle Datenimporteure, welche Daten von dem deutschen Unternehmen erhalten, derzeit als Controller. Daher wurde dies im Genehmigungsantrag und in der Genehmigung so festgelegt. Ferner wurde ein spezielles Verfahren definiert, nach dem bei Bedarf später anerkannt werden kann, dass ein Datenimporteur als Datenverarbeitungsdienstleister fungiert.

In der Arbeitsgruppe Internationaler Datenverkehr verständigten sich die Aufsichtsbehörden auch darüber, dass hinreichend bestimmt sein muss, welche Daten vom antragstellenden Datenexporteur übermittelt werden. Im konkreten Fall waren in dem Anhang zum Vertrag die Übermittlungen der unterschiedlichsten Daten zu den jeweils unterschiedlichen Zwecken dargestellt. Es war aber nicht spezifiziert, welche Daten welcher Datenexporteur konkret übermittelt. Das deutsche Unternehmen übermittelt jedoch tatsächlich nur einen Teil der Daten. Die Übermittlung einiger Daten wäre nach deutschem Datenschutzrecht wohl auch unzulässig gewesen (Anforderungen 1. Stufe). Wenngleich es von der Intention des Mehrparteienvertrags her verständlich ist, dass die maximal zwischen den Unternehmen der Gruppe vorgesehenen Übermittlungen zusammengefasst dargestellt werden sollten, kann eine Genehmigung doch nur für solche Übermittlungen erteilt werden, die der Datenexporteur in absehbarer Zeit wahrscheinlich vornehmen wird und gegen deren Übermittlung keine offensichtlichen Bedenken im Hinblick auf die Anforderungen der 1. Stufe bestehen. Das deutsche Unternehmen hat daher dem Genehmigungsantrag eine entsprechend eingeschränkte Anlage beigefügt.

Eine weitere grundsätzliche Frage war, inwieweit die technisch- organisatorischen Maßnahmen beschrieben werden müssen. Der Standardvertrag vom Dezember 2001 (für Übermittlungen an Datenverarbeitungsdienstleister) sieht vor, dass diese Maßnahmen in einer Anlage dargestellt werden. Die Arbeitsgruppe Internationaler Datenverkehr teilt die Auffassung der europäischen Aufsichtsbehörden, dass auch hier eine hinreichende Bestimmtheit erforderlich ist. In dem Mehrparteienvertrag war nur sehr abstrakt festgelegt, dass technisch-organisatorische Maßnahmen zu treffen sind. Es wurde jedoch auf eine Datensicherheitsrichtlinie Bezug genommen, die in der gesamten Unternehmensgruppe gelten und Bestandteil des Vertrags sein sollte. Folglich war es für das Genehmigungsverfahren erforderlich, dass entweder diese Datensicherheitsrichtlinie dem Antrag beigefügt oder zumindest die wesentlichen Inhalte in einer Anlage verbindlich dargestellt würden. Angesichts des sehr großen Umfangs und Detaillierungsgrades der Datenschutzrichtlinie entschied sich das Unternehmen für das Letztere.

3.2 Abstimmungsverfahren betreffend verbindliche Unternehmensregelungen zum Drittstaatentransfer

Statt durch Verwendung der EU-Standardverträge oder den Abschluss individueller - genehmigungsbedürftiger - Verträge können die besonderen datenschutzrechtlichen Voraussetzungen für den Datentransfer in Drittstaaten ohne angemessenes Datenschutzniveau nach § 4c Abs. 2 BDSG auch durch verbindliche unternehmensinterne Datenschutzregelungen (Binding Corpora-

te Rules - BCR) erfüllt werden. Entscheidet sich ein Konzern, solche Reglungen zu schaffen, um konzernweit für ein angemessenes Datenschutzniveau zu sorgen, so erfolgt bei der Prüfung dieser Regelungen eine europaweite Koordination zwischen den Aufsichtsbehörden. Wie im Arbeitspapier (Working Paper - WP) 107 der Artikel 29 Datenschutzgruppe der EU-Mitgliedsstaaten festgelegt, hat der Konzern zunächst eine Aufsichtsbehörde in Europa als federführende Stelle vorzuschlagen. Entsprechend den im WP 107 vorgegebenen Kriterien, wurde bisher in den meisten Fällen die britische Aufsichtsbehörde (Information Commissioner - ICO) als federführende Stelle vorgeschlagen.

Sämtliche Arbeitspapiere der Artikel 29-Gruppe sind im Internet abrufbar unter http://ec.europa.eu/justice_home/fsj/privacy/.

Im Berichtsjahr wurde das Regierungspräsidium Darmstadt in fünf Fällen an diesen Koodinierungsverfahren beteiligt und zunächst befragt, ob Bedenken gegen die Federführung durch den ICO (in vier Fällen) bzw. durch die französische Aufsichtsbehörde (in einem Fall) bestehen, was verneint wurde.

In einigen Koordinierungsverfahren, die im Berichtsjahr bzw. im Vorjahr begonnen hatten, waren die Prüfungen durch den ICO so weit gediehen, dass die Erörterungen mit dem jeweiligen Konzern abgeschlossen waren und dieser einen entsprechend überarbeiteten Entwurf ("Consolidated Draft") vorgelegt hatte. Hierzu wurden dann die anderen europäischen Aufsichtsbehörden um Stellungnahme gebeten, u.a. in drei Fällen das Regierungspräsidium Darmstadt als allein oder federführend innerhalb Deutschlands zuständige Aufsichtsbehörde.

Bei den Prüfungen stellte das Regierungspräsidium Darmstadt fest, dass die BCR höchst unterschiedlich waren. Schon vom Umfang und der Struktur her gab es eine enorme Bandbreite. Es gab BCR, die nur wenige Seiten umfassten und aus einem einzigen Dokument bestanden, während andere BCR sehr kompliziert aufgebaut waren ("Intra Group Agreement" sowie "Policy" nebst zahlreicher Anhänge mit unterschiedlicher Bindungswirkung) und insgesamt mehr als einhundert Seiten umfassten. Dementsprechend waren auch Regelungstiefe und Inhalte sehr unterschiedlich.

Wenngleich gewisse Unterschiede selbstverständlich sind, da BCR auf die Struktur und Datenverarbeitung der jeweiligen Unternehmensgruppe zugeschnitten sind und Ausdruck deren Datenschutzpolitik sein können und sollen, warfen die festgestellten gravierenden Unterschiede doch die grundsätzliche Frage auf, welche Mindestanforderungen BCR erfüllen müssen. Diese Anforderungen wurden im WP 74 und im WP 108 der Artikel 29-Gruppe definiert, aber nicht präzise genug. Daher sah sich das Regierungspräsidium Darmstadt - wie andere beteiligte europäische Aufsichtsbehörden auch - gezwungen, nicht nur eine Plausibilitätsprüfung, sondern eine genauere inhaltliche Prüfung vorzunehmen, damit einheitliche Maßstäbe gewährleistet sind.

Beispielsweise hinterfragte das Regierungspräsidium Darmstadt, warum bestimmte Anforderungen nicht erfüllt wurden, obwohl diese in einem früheren (dem einzigen bis dato abgeschlossenen) Koordinierungsverfahren auf europäischer Ebene gestellt und in jenem Fall auch erfüllt worden waren.

Diese Prüfung war äußerst aufwändig. Abgesehen davon, dass die BCR in Englisch vorgelegt und die Stellungnahme ebenso in Englisch abzugeben war, waren vor allem die Regelungsinhalte zu den einzelnen Anforderungen des WP 108 zum Teil an ganz unterschiedlichen Stellen in den Gesamtregelwerken verteilt, sodass erst nach Zusammensetzung der "Puzzleteile" beurteilt werden konnte, ob in der Gesamtschau die Anforderungen des WP 74 und des WP 108 erfüllt waren. Zugleich zeigte sich, dass die Anforderungen des WP 108 (und erst Recht des WP 74) zu abstrakt waren. Die Artikel 29-Gruppe erkannte dies ebenfalls und verabschiedete im Juni 2008 die neuen Arbeitspapiere WP 153, WP 154 und WP 155, in welche die zwischen den Aufsichtsbehörden ausgetauschten Stellungnahmen und Prüferfahrungen eingeflossen waren.

Das Arbeitspapier WP 153 enthält eine Übersicht, in der aufgeführt ist, was in den BCR nach Maßgabe der Arbeitspapiere WP 74 und WP 108 geregelt werden muss. Es ist genau angegeben, welche Bestimmungen in die BCR

aufzunehmen und welche Angaben das Antragsformular für die Genehmigung der BCR enthalten muss (WP 133).

Das Arbeitspapier WP 154 enthält einen Rahmen bzw. einen Vorschlag, wie eine verbindliche Unternehmensregelung strukturiert wird und wie sie inhaltlich (mit allen notwendigen Bestandteilen entsprechend WP 74 und WP 108) aussehen könnte.

Im Arbeitspapier WP 155 sind eine Reihe weiterer Probleme betreffend BCR in Form von Antworten auf häufig gestellte Fragen ("Frequently Asked Questions" - FAQ) behandelt.

Fortan legten das Regierungspräsidium Darmstadt und die anderen europäischen Aufsichtsbehörden selbstverständlich diese Arbeitspapiere ihren Prüfungen zugrunde, obwohl diese bei Erstellung der konsolidierten Entwürfe der BCR noch nicht vorhanden waren, und tauschten sich herüber aus.

Insgesamt ergaben sich folgende wesentliche Erkenntnisse:

Das europäische Abstimmungsverfahren nach WP 107 ist noch immer sehr langwierig und bindet in ganz Europa erhebliche personelle Kapazitäten der Aufsichtsbehörden. Für die Aufsichtsbehörden ist dies unbefriedigend, aber selbstverständlich auch für die Unternehmen. Beispielsweise sah sich eine Unternehmensgruppe veranlasst, die beteiligten europäischen Aufsichtsbehörden nacheinander zu besuchen, um jeweils bilateral deren Bedenken und Fragen zu erörtern.

Der von der Wirtschaft vorgetragene Wunsch, dass die von einer nach den Kriterien des WP 107 bestimmten Aufsichtsbehörde vorgenommene Bewertung der BCR auch von den anderen europäischen Aufsichtsbehörden anerkannt wird, ist daher verständlich.

Die deutschen Aufsichtsbehörden haben sich deshalb im Berichtsjahr der "Mutual Recognition Declaration" angeschlossen. Dies ist eine Absichtserklärung zur gegenseitigen Anerkennung der Bewertung von BCR.

Allerdings hatten die Prüferfahrungen gerade gezeigt, dass das bisherige Koordinationsverfahren vor allem deshalb so mühsam ist, weil nach wie vor Unklarheiten bzgl. der Anforderungen an BCR bestehen und weil die Herangehensweise bzw. Prüftiefe der Aufsichtsbehörden z. T. unterschiedlich ist. Durch die neuen Arbeitspapiere ist hier ein großer Fortschritt erzielt worden, allerdings zeigte sich, dass weiter an einer Harmonisierung der Prüfmaßstäbe und der Prüfpraxis gearbeitet werden muss. Dies ist auch im Interesse der Wirtschaft, denn für diese ist es bedeutsam, dass die Bewertungen berechenbar, gleichmäßig und somit gerecht erfolgen.

Das Regierungspräsidium Darmstadt sprach sich deshalb - wie andere deutsche Aufsichtsbehörden auch - dafür aus, dass die Vereinbarung der gegenseitigen Anerkennung nur gerechtfertigt ist, wenn parallel an der weiteren Präzisierung bzw. Vereinheitlichung der Prüfmaßstäbe gearbeitet wird.

Die BCR-Arbeitsgruppe der Artikel 29 Gruppe sah dies ebenso und hat mittlerweile drei Überarbeitungen und Ergänzungen der FAQs des WP 155 vorgenommen, bei dem die weiteren Erfahrungen aus den konkreten Fällen eingeflossen sind. Weitere Sitzungen sind geplant. Von deutscher Seite soll jeweils diejenige Aufsichtsbehörde teilnehmen, in deren Zuständigkeit die zu erörternden BCR fallen.

Künftig soll in einer Auflistung aufgezeigt werden, durch welche Reglungen in den BCR die Anforderungen der Arbeitspapiere erfüllt sind. Dies wird die Prüfungen der Aufsichtsbehörden erheblich erleichtern.
Die "Mutual Recognition Declaration" soll nach ein bis zwei Jahren evaluiert werden.

Im Jahr 2008 wurde also der Weg zu einer Vereinfachung und Beschleunigung der Anerkennung von BCR - bei gleichzeitiger Gewähr für gleichmäßige Entscheidungen - eingeschlagen.

4. Register der meldepflichtigen Verfahren nach § 4d BDSG

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

Am Ende des Berichtsjahres waren 116 Verfahren von 99 verantwortlichen Stellen im Melderegister eingetragen. Nur sechs verantwortliche Stellen haben mehr als ein Verfahren gemeldet. Davon werden in 65 gemeldeten Verfahren geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung gespeichert (Adresshändler, Handels- und Wirtschaftsauskunfteien, meldepflichtig nach § 4d Abs. 4 Nr. 1 BDSG). Die weiteren 51 der eingetragenen Verfahren dienen dem Zwecke der anonymisierten Übermittlung (Markt- und Meinungsforschung, meldepflichtig nach § 4d Abs. 4 Nr. 2 BDSG).

5. Ordnungswidrigkeitenverfahren

Von drei noch offenen Verfahren aus 2006 wurden zwei im Berichtsjahr 2008 beendet. Eines wurde wegen eines Verfahrensfehlers eingestellt. Das andere Verfahren endete mit der Zahlung eines reduzierten Bußgelds im Rahmen eines gerichtlichen Vergleichs. In diesem Verfahren wurden mehrere Verstöße (Erhebung und Verarbeitung von Daten ohne rechtliche Grundlage, Nichtbestellung eines betrieblichen Datenschutzbeauftragten und Nichterteilen von Auskünften) mit einer Geldbuße in Höhe von 14.000 € geahndet. Ein Verfahren aus dem vorherigen Berichtszeitraum ist noch beim Amtsgericht anhängig. In diesem, bereits im 21. Tätigkeitsbericht dargestellten Verfahren, erfolgen auf Veranlassung der Staatsanwaltschaft weitere Ermittlungen durch die Aufsichtsbehörde.

Von den fünf noch offenen Verfahren aus 2007 wurden zwei mit der Zahlung des Bußgelds beendet, drei sind noch anhängig.

Im Berichtsjahr wurden vom Regierungspräsidium Darmstadt siebzehn Verstöße nach dem Ordnungswidrigkeitengesetz (OWIG) mit einem Bußgeldbescheid geahndet. Vier Verfahren befinden sich noch im Stadium der Anhörung, für zwei Verfahren ist ein Gerichtstermin für 2009 avisiert.

Übersicht 2008

Verstoß	Grund	Rechtskraft/Bußgeldhöhe
§ 43 Abs. 1 Nr. 1	Verstoß gegen die Meldepflicht	Noch anhängig
§ 43 Abs. 1 Nr. 2	Nichtbestellung eines Datenschutzbeauftragten	Rechtskräftig Bußgeld 2000 €
§ 43 Abs. 1 Nr. 2	Nichtbestellung eines Datenschutzbeauftragten	Rechtskräftig Bußgeld 10.000€
§ 43 Abs. 1 Nr. 10	Nichterteilung von Auskünften	Noch anhängig
§ 43 Abs. 1 Nr. 10	Nichterteilung von Auskünften	Noch anhängig
§ 43 Abs. 1 Nr. 10	Nichterteilung von Auskünften	Noch anhängig
§ 43 Abs. 1 Nr. 10	Nichterteilung von Auskünften	Rechtskräftig Bußgeld 1000 €
§ 43 Abs. 1 Nr. 10	Nichterteilung von Auskünften	Noch anhängig
§ 43 Abs. 1 Nr. 10	Nichterteilung von Auskünften	Noch anhängig
§ 43 Abs. 1 Nr. 10	Nichterteilung von Auskünften	Noch anhängig
§ 43 Abs. 1 Nr. 10	Nichterteilung von Auskünften	Noch anhängig
§ 43 Abs. 2 Nr. 1	Unzulässige Übermittlung von Daten	Rechtskräftig Bußgeld 100 €
§ 43 Abs. 2 Nr. 1	Unbefugte Verarbeitung personenbezogener Daten	Noch anhängig
§ 43 Abs. 2 Nr. 1	Unbefugte Verarbeitung personenbezogener Daten	Bußgeld vom Amtsgericht auf 200 € reduziert
§ 43 Abs. 2 Nr. 1	Unbefugte Verarbeitung personenbezogener Daten	Rechtskräftig Bußgeld 500 €
§ 43 Abs. 2 Nr. 3	Unbefugte Beschaffung von Daten	Rechtskräftig Bußgeld 700 €
§ 43 Abs. 2 Nr. 3	Unbefugte Beschaffung von Daten	Rechtskräftig Bußgeld 2000 €

Wie sich aus der Übersicht ersehen lässt, beruhen die meisten der eingeleiteten Ordnungswidrigkeitenverfahren auf Verstößen gegen § 38 Abs. 3 BDSG, bei denen die verantwortlichen Stellen der Aufsichtsbehörde die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte nicht, nicht vollständig oder nicht unverzüglich erteilt hatten. In diesen Fällen ist die Einleitung

eines Ordnungswidrigkeitenverfahrens geboten, um für die Zukunft ein gesetzeskonformes Verhalten zu erreichen.

Ein Schwerpunkt der Aufsichtsbehörde für den nicht öffentlichen Bereich war die Kontrolle, ob beim Vorliegen der gesetzlichen Voraussetzungen ein betrieblicher Datenschutzbeauftragter bestellt wurde. Diese Überprüfung führte zu mehreren Ordnungswidrigkeitenverfahren und wird auch 2009 ein Arbeitsschwerpunkt sein, da die vom Gesetz vorgeschriebene Bestellung eines betrieblichen Datenschutzbeauftragten offensichtlich in vielen Bereichen nicht stattgefunden hat.

6. Teilnahme an Arbeitsgruppen

Das Hessische Ministerium des Innern und für Sport hatte im Jahr 2008 turnusgemäß den Vorsitz des "Düsseldorfer Kreises", das bundesweite Abstimmungsgremium der obersten Datenschutzaufsichtsbehörden der Bundesländer, übernommen und zu den Sitzungen im Frühjahr und Herbst nach Wiesbaden eingeladen.

Zu folgenden Themen wurden Beschlüsse gefasst:

- "Internet-Portale zur Bewertung von Einzelpersonen"
- "Datenschutzkonforme Gestaltung sozialer Netzwerke" (siehe hierzu Ziffer 9.2)
- "Datenschutzrechtliche Bewertung von digitalen Straßenansichten, insbesondere im Internet" (siehe hierzu Ziffer 9.1)
- "Keine fortlaufenden Bonitätsauskünfte an den Versandhandel" (siehe hierzu Ziffer 7.2 des 21. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde, Drucks. 17/663)
- "Novellierung des Bundesdatenschutzgesetzes in den Bereichen Adresshandel, Werbung und Datenschutzaudit"

Diese und sämtliche anderen, seit November 2006 vom Düsseldorfer Kreis gefassten Beschlüsse wurden auf der Website des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit veröffentlicht (http://www.bfdi.bund.de, Pfad: "Datenschutz/Entschließungen/Düsseldorfer Kreis").

Die in den Beschlüssen behandelten Themen sind jedoch nur ein kleiner Ausschnitt dessen, was Gegenstand der Beratungen war. Natürlich haben sich die Aufsichtsbehörden des Düsseldorfer Kreises auch mit den im Jahr 2008 in bisher unbekanntem Maße aufgetretenen Verstößen gegen das Bundesdatenschutzgesetz beschäftigt. Es galt, zunächst die Aufsichtstätigkeit abzustimmen und zu koordinieren, soweit es sich um Verstöße gegen bundesweit tätige Unternehmen handelte (siehe hierzu Ziffer 12.1).

Auch das Regierungspräsidium Darmstadt war wieder an der Arbeit des Düsseldorfer Kreises und den von diesem gebildeten Arbeitsgruppen beteiligt und nahm an dessen Sitzungen sowie an denen der meisten Arbeitsgruppen teil (siehe hierzu Ziffer 6 des 20. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde, Drucks. 16/7646). In Vertretung für das Hessische Ministerium des Innern und für Sport übernahm das Regierungspräsidium Darmstadt auch den Vorsitz in der Frühjahrssitzung der Arbeitsgruppe Auskunfteien.

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

Ausgesuchte Probleme und Einzelfälle

7. Auskunfteien

7.1 Mängel bei der Verarbeitung von Bonitätsdaten durch Vertragspartner

Ein Betroffener beschwerte sich darüber, dass sein Telekommunikationsanbieter gleich zweimal fehlerhafte Negativdaten zu seiner Person bei einer

großen Verbraucherauskunftei im Aufsichtsbezirk eingemeldet habe. Diese Falschmeldungen hätten wiederum zu negativen Auswirkungen auf andere Kreditverhältnisse mit anderen Kreditgebern geführt, welche als Vertragspartner der Verbraucherauskunftei durch Nachmeldungen Kenntnis von den fehlerhaften Negativdaten erhalten hätten.

Der Telekommunikationsanbieter hatte die Fehler bereits eingestanden, gleichwohl schaltete die Aufsichtsbehörde, wie in diesen Fällen üblich, auch den hierfür zuständigen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zwecks Prüfung etwaiger Organisationsmängel bei dem Telekommunikationsanbieter ein.

Die Prüfung der Aufsichtsbehörde bei der Auskunftei ergab, dass die Verbraucherauskunftei die Daten, nachdem der Betroffene sich zeitnah bei ihr beschwert hatte, unverzüglich geprüft und die Falschmeldungen umgehend gelöscht hatte. Darüber hinaus waren alle weiteren Kreditgeber des Betroffenen, welche die Falschmeldungen nach § 35 Abs. 7 BDSG im Nachmeldeverfahren erhalten hatten, mehrfach elektronisch und per Fax über den Fehler und die bereits erfolgte Korrektur informiert worden.

Gleichwohl sperrte ein Kreditkartenunternehmen die Kundenkreditkarte des Betroffenen noch nachträglich und begründete dies gegenüber dem Betroffenen mit dem von der Verbraucherauskunftei gemeldeten Negativmerkmal. Bedauerlicherweise war die Aufklärung der konkreten Zusammenhänge für die Kartensperre beim Kreditkartenunternehmen erst möglich, nachdem ein Bußgeld wegen Nichtbeauskunftung bzw. nicht richtiger und nicht vollständiger Beauskunftung der Aufsichtsbehörde in Aussicht gestellt wurde.

Hintergrund der Kartensperre war zunächst, dass eine solche von dem Datenverarbeitungssystem des Kreditkartenunternehmens automatisch veranlasst wurde, als die Negativmeldung der Verbraucherauskunftei zu dem Kunden einging. Die unverzügliche Korrekturmeldung wurde in diesem Prozess jedoch weder automatisiert noch manuell berücksichtigt.

Auf die Nachforschungen der Aufsichtsbehörde hin stellte sich heraus, dass die Software, mit der die Auskunftei-Meldungen verarbeitet wurden, insgesamt drei Wochen und gerade in der Zeit nach der Negativnachmeldung zu dem Betroffenen nicht ordnungsgemäß funktioniert hatte, was die IT-Abteilung des Kreditkartenunternehmens jedoch erst nach etwa zwei Wochen feststellte. In dem gesamten Zeitraum wurden die von der Verbraucherauskunftei automatisiert bereit gestellten Nachmeldungen von dem Kreditkartenunternehmen nicht abgerufen. Es erfolgte jedoch auch keine Rückmeldung vom Kreditkartenunternehmen an die Verbraucherauskunftei bezüglich des technischen Problems.

Da die Verbraucherauskunftei aber den Nichtabruf der Nachmeldungen in ihrem Datenverarbeitungssystem registrierte, wurde entsprechend ihrem System sogleich automatisiert organisiert, dass die Nachmeldungen dem Kreditkartenunternehmen auf dem Postweg zugestellt wurden. Doch auch diese Nachmeldungen in Papierform wurden offensichtlich von dem Kreditkartenunternehmen nicht berücksichtigt.

Aufgrund der Beschwerde des Betroffenen hatte das Kreditkartenunternehmen bei der Verbraucherauskunftei zwar eine Anfrage zum Datensatz des Kunden gestartet, die Anfrage jedoch nicht weiter verfolgt, nachdem zwei Versuche innerhalb des intern gesetzten Zeitfensters nicht geglückt waren. Schließlich behauptete ein Mitarbeiter des Kreditunternehmens fälschlich gegenüber dem Betroffenen, dass die Verbraucherauskunftei für die lange Dauer der Kartensperre verantwortlich gewesen sei.

Es entstand der Eindruck, dass bei dem Kreditkartenunternehmen der ordnungsgemäßen Verarbeitung von Bonitätsinformationen nicht die erforderliche Aufmerksamkeit gewidmet wurde. Diese technischen und organisatorischen Mängel im Umgang mit Bonitätsauskünften wurden beanstandet und sind Ausgangspunkt dafür, dass das Kreditkartenunternehmen intensiver von der Aufsichtsbehörde kontrolliert wird.

7.2 Bonitätsprüfung bei der Anbahnung von Kreditgeschäften

7.2.1 "Kreditanfrage"/"Konditionenanfrage" und kein Ende

Die Aufsichtsbehörde musste sich im Berichtszeitraum erneut mit den Anfragemerkmalen "Kreditanfrage" und "Konditionenanfrage" befassen, die eine große Verbraucherauskunftei eingeführt hatte. Deren Unterscheidung gelingt bei den Kreditinstituten nach wie vor nicht durchgängig (siehe dazu schon Ziffer 7.3 des 21. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde, Drucks. 17/663, mit weiteren Verweisen auf entsprechende vorhergehende Berichte).

Die Auskunftei hatte die beiden Merkmale in ihre Allgemeinen Geschäftsbedingungen (AGB) aufgenommen und die Vertragspartner im Berichtsjahr ausdrücklich darauf hingewiesen, dass das Merkmal "Kreditanfrage" nur bei Vorliegen eines zivilrechtlichen Kreditantrags verwandt werden dürfe. Auch die AGB wurden entsprechend präzisiert. Damit wies die Auskunftei gegenüber der Aufsichtsbehörde nach, dass sie die erforderlichen Informationen zum Einsatz der beiden Merkmale an ihre Vertragspartner weiter gegeben hatte.

Aufgrund von Beschwerden Betroffener wurde jedoch auch in diesem Berichtszeitraum ersichtlich, dass nicht wenige Kreditinstitute das falsche Merkmal, nämlich "Kreditanfrage" statt "Konditionenanfrage" für eine Anfrage verwendeten, wenn der Betroffene lediglich die Konditionen für einen Kredit erfragen wollte. Dies wurde jeweils beanstandet. Insbesondere gab es wieder Fälle von Online-Kreditwünschen Betroffener, bei denen sich die Bank darauf berief, dass die Interessenten einen sogenannten "Kreditantrag" ausgefüllt hätten, was die Benutzung des Merkmals "Kreditanfrage" rechtfertige. Ist bei Krediten der Zinssatz jedoch nicht von vornherein festgelegt, konkretisiert die Bank selbst den Zinssatz erst, wenn sie dem Kunden auf dessen Kreditwunsch hin eine Ausfertigung des Kreditvertrags zur Unterschrift übermittelt. In diesen Fällen darf bei dem Kreditersuchen des Betroffenen durch Ausfüllen des Online-"Kreditantrags" nur mit einer "Konditionenanfrage" gearbeitet werden.

Die betreffenden Banken sicherten zu, dies künftig zu beachten.

7.2.2 Unzureichende Identifizierung Betroffener vor Bonitätsanfragen bei Online-Kreditgeschäften

Im Zusammenhang mit der Prüfung der Online-Kreditabläufe fiel der Aufsichtsbehörde auf, dass Kreditinstitute die Kreditinteressierten vor der Bonitätsanfrage bei der Verbraucherauskunftei nicht ausreichend identifizierten. In diesen Fällen war nicht sicher gestellt, dass tatsächlich nur der wahre Betroffene die Angaben zum Kreditantrag übermittelt hatte. Es besteht daher die Gefahr, dass sich jemand unter falschem Namen für einen Kredit interessiert und damit unter Umständen Informationen über die Bonität einer anderen Person erhält. Beispielsweise ermöglicht die Ablehnung eines bestimmten Kredits ggf. einen Rückschluss auf die Bonität des Betroffenen. Ferner besteht die Gefahr, dass sich bei einer Verwendung des Merkmals "Kreditanfrage" durch das Kreditinstitut der Bonitätsscore des Betroffenen verschlechtert (siehe hierzu obige Ausführung und die Darstellungen in früheren Tätigkeitsberichten).

Die Problematik wurde von der Aufsichtsbehörde gegenüber den Kreditinstituten und gegenüber der Auskunftei beanstandet. Sie wurde auch zwischen den Aufsichtsbehörden im Bundesgebiet und den Vertretern der Auskunftei und der Kreditbranche erörtert.

Das Post-Ident-Verfahren wäre für die Fälle der Online-Kreditbeantragung eine sichere Identifizierungsmöglichkeit. Es wird jedoch von den Unternehmen der Kreditbranche nicht gewünscht, weil sie befürchten, dass die Kunden dieses Verfahren nicht akzeptieren werden. Daher stellte die Aufsichtsbehörde klar, dass die Kreditbranche insoweit in der Pflicht ist, eine alternative Lösung zu entwickeln.

7.3 Zahlreiche Beschwerden aufgrund Benachrichtigung durch Auskunftei

Im Vorjahr wurde über eine Auskunftei berichtet, die sich im Wesentlichen auf Adressermittlungen spezialisiert hat (siehe Ziffer 7.7 des 21. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde, Drucks. 16/8377). Entgegen den dort geäußerten Erwartungen der Aufsichtsbehörde war im Berichtsjahr kein signifikanter Rückgang der Anfragen und Beschwerden bezüglich dieser Auskunftei zu verzeichnen.

Die im vergangenen Jahr von dem Unternehmen angekündigte Überarbeitung des Standard-Benachrichtigungsschreibens ist aufgrund unternehmensinterner Umstrukturierungsmaßnahmen nicht erfolgt. Dies ist zwar unbefriedigend, aber die aktuelle Formulierung der Benachrichtigung ist rechtlich durchaus korrekt. Ob die Eingaben Betroffener darauf zurück zu führen sind, dass sie das Benachrichtigungsschreiben nicht verstanden haben, oder ob eine Vielzahl von Bürgern, aufgeschreckt durch die bekannten Datenschutzskandale des Jahres, nur besonders sensibilisiert auf die Schreiben reagiert hat, mag dahingestellt bleiben. Jedenfalls konnte in allen vorgetragenen Fällen "Entwarnung" gegeben werden. Der Aufsichtsbehörde wurde insoweit kein Fall von unberechtigter Datenverarbeitung bekannt.

Es bleibt also für die Zukunft abzuwarten, ob eine verbesserte Information der Betroffenen zu einem Rückgang der Anfragen und Beschwerden führen wird.

8. Banken

8.1 Bonitätsprüfung bei Guthabenkonto

Zum Start auf dem deutschen Privatkundenmarkt präsentierte die Niederlassung einer ausländischen Bank interessante Konditionen für ein Tagesgeldkonto. Für diese Anlage interessierte sich auch der Beschwerdeführer und informierte sich über diese Anlage. Hierbei stellte er fest, dass die Allgemeinen Geschäftsbedingungen des Kreditinstituts eine ausführliche Klausel enthielten, wonach die Bank zum Zwecke der Bonitätsprüfung Daten über die Geschäftsbeziehung an eine große Auskunftei übermitteln und auch einholen würde. Irritiert wandte sich der Interessent an die Aufsichtsbehörde.

Die Beschaffung von Daten über die Bonität einer Person ist nur erforderlich, wenn die Bank ein kreditorisches Risiko eingeht. Nur dann liegt ein berechtigtes Interesse für die Einholung einer Auskunft vor.

Auf Nachfrage erklärte die Bank die Auskunftei-Klausel in ihren Vertragsunterlagen mit der ursprünglichen Absicht, auch ein Kontokorrentkonto anbieten zu wollen. Hiervon habe man dann Abstand genommen und sich auf Guthabenkonten konzentriert. Leider sei versäumt worden, die Kontounterlagen zu ändern. Auskunftei-Anfragen hatte die Bank nicht veranlasst, insoweit war eine Datenschutzverletzung nicht erfolgt. Zeitnah berichtigte das Kreditinstitut seine Vertragsunterlagen und entfernte den Abschnitt zur Bonitätsprüfung.

8.2 Bankdaten in Werbeschreiben

Einige Bankkunden, die ordnungsgemäß, ohne Zahlungsstörungen ihren alten Konsumentenkredit zurückgeführt hatten, gerieten in den Focus der Marketingabteilung einer Bank.

Teilweise wiederholt erhielten mehrere Kunden das Angebot für einen persönlichen Kredit als Dank für die gute Zusammenarbeit. Betont wurde in dem Anschreiben die Zuverlässigkeit des Kreditnehmers, die eine unbürokratische Kreditgewährung ermöglicht. Dem Brief beigelegt war auch in mehrfacher Ausfertigung der Darlehensvertrag, der neben Adressdaten und den Angaben zur Darlehenshöhe auch die Bankverbindung des Kunden enthielt, über die der alte Ratenkredit abgewickelt wurde. Die Beschwerdeführer waren irritiert und wandten sich an die Aufsichtsbehörde.

Die Bank begründete den Abdruck der Bankverbindungsdaten in den Kreditformularen mit einem Service gegenüber den Bankkunden. Dieses wurde

von der Aufsichtsbehörde beanstandet. Der Empfänger von Werbepost rechnet nicht damit, dass diese sensitive Daten wie die Bankverbindung enthält und wirft diese oft ungeöffnet weg. Es besteht die Gefahr des Missbrauchs der Kontodaten. Infolge der Beanstandung dieser Praxis änderte die Bank den Bearbeitungsprozess und wird künftig keine Kontodaten in den Darlehensangeboten mehr verwenden.

9. Telemedien, Internet

9.1 Digitale Straßenansichten im Internet

Vor allem den Anbietern von Telemedien im Internet bietet die technische Entwicklung immer mehr faszinierende Möglichkeiten. Gleichzeitig bringt es enorme Gefahren für Persönlichkeitsrechte betroffener Bürgerinnen und Bürger mit sich, dass Unternehmen mit geradezu gigantischen Speicherkapazitäten heute auf schnellen Datenleitungen Nutzer weltweit mit einer Fülle von Informationen versorgen können. Dies zeigte sich im Berichtsjahr insbesondere an dem Projekt "Street-View" des amerikanischen Internet-Marktführers Google.

Obwohl bereits von einigen Unternehmen und auch Kommunen in letzter Zeit Seiten mit digitalisierten Straßenansichten z.B. aus Marketinggründen oder zur Tourismusförderung in das WWW eingestellt werden, erregte erst Googles "Street-View" die Aufmerksamkeit der Bevölkerung und der Presse.

Es handelt sich bei "Street View" um eine Ergänzung des bereits bestehenden Google-Dienstes "Maps", mit dem schon seit Jahren weltweit Landkarten und Satellitenaufnahmen mit einer überraschend guten Auflösung frei zugänglich im WWW aufgerufen werden können. "Street View" erlaubt es dem Nutzer zusätzlich zur Luftbildansicht einen Straßenzug aus der Perspektive eines Autofahrers zu betrachten. Jeder kann sozusagen aus dem Luftbild einer Stadt in eine wahlfreie Straße "eintauchen" und dann wie ein Autofahrer nach vorne, hinten, links oder rechts "sehen".

Bisher war diese Funktion für das Gebiet von Deutschland in "Maps" allerdings noch nicht aktivierbar. Für einige Länder der Erde wie zum Beispiel für die USA, Großbritannien und Frankreich wurde "Street-View" bereits in die Luftbildfunktion von "Maps" integriert. Da das Unternehmen das Angebot ausbauen möchte, sind Googles Kamerawagen zurzeit in Nordamerika, Europa, Asien und Australien unterwegs und lichten dabei systematisch die Straßenzüge ganzer Städte ab.

Im Berichtsjahr gingen nun bei der Datenschutzaufsichtsbehörde zahlreiche Anfragen verunsicherter Bürgerinnen und Bürger ein, die Fahrzeuge mit einem großen auffälligen Stativaufbau mit mehreren Kameras durch die Straßen von Frankfurt am Main hatten fahren sehen und sich besorgt erkundigten, wer hier zu welchem Zweck Foto- oder Videoaufnahmen der Straßen Frankfurts anfertigt und ob dies zulässig sei. Einige Journalisten waren bereits besser informiert und kurz darauf war es auch der Presse zu entnehmen, dass Google beabsichtigte, die Funktion "Street-View" auch für Deutschland anzubieten. Das Unternehmen habe gerade damit begonnen, die Straßen einiger deutscher Großstädte systematisch abzufahren.

Aus datenschutzrechtlicher Sicht ist es sicherlich nicht "per se" unzulässig, Fotografien von Häuserzeilen, die an öffentlichen Straßen liegen und daher für jedermann ohne Probleme ohnehin sichtbar sind, zur späteren Veröffentlichung anzufertigen. Allerdings können auch hier schutzwürdige Interessen der jeweiligen Eigentümer und Bewohner tangiert sein. Dies gilt in besonderem Maße für dabei zufällig aufgenommene erkennbare Personen und personenbeziehbare Kfz-Kennzeichen. Hier können Betroffene in der Regel ohne großen Aufwand identifiziert werden. Die Gefahr einer Verletzung von Persönlichkeitsrechten bei der Veröffentlichung im WWW ist daher in diesen Fällen besonders groß. Die Information darüber, wer sich wann an einer bestimmten Stelle aufgehalten hat, ist eben in der Regel nicht öffentlich zugänglich, sondern gehört vielmehr zur Privatsphäre der jeweils Betroffenen, die ein gegenüber dem berechtigten Interesse von Google an der Bereitstellung umfänglicher Informationen offensichtlich überwiegendes schutzwürdiges Interesse daran haben, dass diese Angaben zu ihrer Person oder ihrem Kfz nicht im WWW verbreitet werden.

Zuständige Datenschutzaufsichtsbehörde für die Datenerhebung und Datenverwendung durch Google ist der Hamburgische Datenschutzbeauftragte, da die dort ansässige Google Germany GmbH als Inlandsvertreter von Google im Sinne des § 1 Abs. 5 BDSG anzusehen ist. Da von "Street-View" aber mehrere Bundesländer betroffen waren und die Datenschutzaufsichtsbehörden aller Bundesländer mit Fragen zu dem Vorhaben konfrontiert wurden, hat sich der Düsseldorfer Kreis mit den damit zusammenhängenden datenschutzrechtlichen Fragestellungen befasst (siehe bereits Ziffer 6). Das Hessische Ministerium des Inneren und für Sport übermittelte der Google Inc. den folgenden Beschluss als gemeinsame Position der deutschen Datenschutzaufsichtsbehörden für den nicht öffentlichen Bereich:

"**Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet**

Bei digital erfassten Fotos von Gebäude- und Grundstücksansichten, die über Geokoordinaten eindeutig lokalisiert und damit einer Gebäudeadresse und dem Gebäudeeigentümer sowie den Bewohnern zugeordnet werden können, handelt es sich in der Regel um personenbezogene Daten, deren Erhebung und Verarbeitung nach dem Bundesdatenschutzgesetz zu beurteilen ist. Die Erhebung, Speicherung und Bereitstellung zum Abruf ist nur zulässig, wenn nicht schutzwürdige Interessen der Betroffenen überwiegen. Bei der Beurteilung schutzwürdiger Interessen ist von Bedeutung, für welche Zwecke die Bilddaten verwendet werden können und an wen diese übermittelt bzw. wie diese veröffentlicht werden.

Die obersten Aufsichtsbehörden sind sich einig, dass die Veröffentlichung von georeferenziert und systematisch bereit gestellten Bilddaten unzulässig ist, wenn hierauf Gesichter, Kraftfahrzeugkennzeichen oder Hausnummern erkennbar sind.

Den betroffenen Bewohnern und Grundstückeigentümern ist zudem die Möglichkeit einzuräumen, der Veröffentlichung der sie betreffenden Bilder zu widersprechen und dadurch die Bereitstellung der Klarbilder zu unterbinden. Keine schutzwürdigen Interessen bestehen, wenn die Darstellung der Gebäude und Grundstücke so verschleiert bzw. abstrakt erfolgt, dass keine individuellen Eigenschaften mehr erkennbar sind.

Um die Möglichkeit zum Widerspruch schon vor der Erhebung zu eröffnen, sollte die geplante Datenerhebung mit einem Hinweis auf die Widerspruchsmöglichkeit rechtzeitig vorher bekannt gegeben werden. Die Widerspruchsmöglichkeit muss selbstverständlich auch noch nach der Veröffentlichung bestehen."

Der Beschluss bezieht sich ausdrücklich nicht "Google Street View" sondern ist allgemein gefasst, weil die darin bezeichneten Anforderungen selbstverständlich für alle Anbieter solcher Straßenansichten gelten.

Bei Redaktionsschluss dieses Berichts lag bereits eine erste Reaktion der Google Inc. auf die letztlich auf Transparenz und Wahrung der Rechte von Betroffenen gerichteten Forderungen der Datenschutzaufsichtsbehörden vor. Das Unternehmen sichert darin die Unkenntlichmachung ("Verpixelung") von Gesichtern und Kfz-Kennzeichnen vor der Veröffentlichung zu, wie dies bereit bei den Aufnahmen in anderen Ländern geschehen ist, und kündigte an, die beste am Markt verfügbare Technik hierfür einzusetzen. Weiterhin sei geplant, es jedem Betroffenen sozusagen "auf Mausklick" ohne viel Aufwand zu ermöglichen, unerwünschte Aufnahmen auch von Häuserfassaden aus "Street View" wieder entfernen zu lassen und damit seine schutzwürdigen Belange zu berücksichtigen. Den Aufsichtsbehörden wurde auch Informationsmaterial über die Umsetzung der Widerspruchsmöglichkeit zur Veröffentlichung auf deren Homepages angeboten.

Dass Google damit auf die deutschen Datenschützer zugeht, ist ohne Zweifel anerkennenswert. Ob die Google-Technik aber wirklich zur automatischen Unkenntlichmachung im notwendigen Umfang und mit erforderlicher Qualität in der Lage ist, wird sich zeigen. Angesichts der Erfahrungen aus anderen Ländern, in denen "Street View" schon länger verfügbar ist, muss allerdings damit gerechnet werden, dass sich in Einzelfällen immer noch datenschutzrechtliche Probleme ergeben werden.

Es bleibt abzuwarten, ob Google den darüber hinausgehenden Forderungen der Datenschutzaufsichtsbehörden, zum Beispiel nach der frühzeitigen Bekanntgabe der geplanten Datenerhebungen, nachkommen wird. Als zum Redaktionsschluss die ersten Links auf Bilder der deutschen Google-Kamera-Flotte (schwarze Kleinwagen mit sehr hohem Dachaufbau und großen Google-Aufklebern) im WWW veröffentlicht wurden, hatte das Unternehmen die beginnenden Aufnahmen dem Düsseldorfer Kreis zwar angekündigt. Fragen des Regierungspräsidiums Darmstadt nach Zeitspannen und konkreten Orten geplanter Aufnahmen in Hessen wurden mit Verweis auf die Abhängigkeit von der jeweils herrschenden Witterung und die flexible und selbständige Arbeitsorganisation der Google-Fahrer allerdings nicht beantwortet. Sicher war lediglich, dass nur dicht besiedelte Gebiete befahren werden und dass Frankfurt am Main davon nicht mehr betroffen sein wird, da die Straßen der Stadt bereits im letzten Jahr weitgehend aufgenommen wurden.

Das Regierungspräsidium Darmstadt hat sich daraufhin dafür eingesetzt, dass das Unternehmen beispielsweise auf einer Internetseite bekannt gibt, welche Städte in welchen Zeiträumen aufgenommen werden und ab wann diese Aufnahmen im WWW abrufbar sein werden. Eine Reaktion von Google stand zu Redaktionsschluss noch aus.

9.2 Datenschutz in sozialen Online-Netzwerken

Plattformen für sog. "Soziale Netzwerke" im Internet, also Seiten im WWW, auf denen sich Gleichgesinnte kennenlernen, treffen, chatten, online austauschen und hierfür auch eigene Inhalte bis zum ausführlichen Persönlichkeitsprofil einstellen können, sind in den letzten Jahren wie Pilze aus dem Boden geschossen. Ob Schüler, Studenten, Senioren, Fachexperten oder Anhänger nahezu jeden Hobbys, für alle findet sich im WWW mittlerweile eine passende virtuelle Gemeinschaft. Fast die Hälfte aller Internet-Nutzer hat inzwischen auch einen aktiven Zugang zu solchen Plattformen. Welche Bedeutung diesen virtuellen Treffpunkten neben dem Medium E-Mail und dem Instant Messaging in Zukunft zukommen kann, ist insbesondere daran erkennbar, dass die Anschlussquote bei den unter Zwanzigjährigen Anfang 2009 schon bei nahezu 95 v.H. lag (vgl. www.heise.de/newsticker/meldung/132240). Da alle großen deutschen Plattformen inzwischen mehrere Millionen Mitglieder haben, kann man dabei durchaus von einem Massenphänomen sprechen.

Die mit diesem Trend zusammenhängenden datenschutzrechtlichen Probleme sind so vielfältig wie die Angebote und ihre Nutzer: Immer mehr junge Menschen offenbaren dort zunehmend Details aus ihrem Privatleben oder stellen gar sensible Inhalte oder Fotos über Dritte - oftmals nicht einmal in böser Absicht sondern aus mangelnder Sensibilität - öffentlich zugänglich ins Netz. Fast zwei Drittel der unter Dreißigjährigen veröffentlichen nach einer Forsa-Umfrage Bilder oder Texte über sich in solchen virtuellen "social online communities".

Gerade Kindern und Jugendlichen fehlt in diesem Zusammenhang offensichtlich das Gefühl dafür, dass die preisgegebenen Informationen oft nicht nur wenigen Freunden, sondern jedermann weltweit, zur Verfügung stehen. Zudem können Daten, einmal im WWW veröffentlicht, leicht kopiert, verfälscht und in jeder Hinsicht zweckentfremdet verwendet werden. Viele übersehen auch, dass das Netz nichts "vergisst" und dass Informationen nach ihrer weltweiten Veröffentlichung sich leicht verselbständigen und nie mehr eingefangen werden können. Auch vielen Erwachsenen ist nicht bewusst, dass die veröffentlichten Informationen über das eigene Privatleben für künftige Arbeit- oder Kreditgeber sehr aufschlussreich sein können. Zudem können die Anbieter solcher Plattformen aufgrund dieser Informationen sehr leicht Interessenprofile bilden und individuell zugeschnittene Werbung bei den Nutzern platzieren oder die Daten für andere Zwecke verwenden. Dass die Daten der Mitglieder das wichtigste Kapital der anbietenden Unternehmen sind, zeigte sich u. a. auch daran, dass nach Presseberichten zum Teil Daten auch nach der Löschung der Mitgliedschaft noch bei einem Anbieter verfügbar waren, also entgegen dem ersten Anschein von dem Unternehmen doch keine komplette Datenlöschung bei dem Austritt eines Mitglieds durchgeführt wurde.

Zu dem bemerkenswert leichtsinnigen Umgang der Betroffenen mit den eigenen Daten und auch den Daten anderer Personen gesellen sich neben den Gefahren für das Persönlichkeitsrecht durch das kommerzielle Verwertungsinteresse der Anbieter zusätzlich noch die Risiken durch unzulängliche Sicherheitsmaßnahmen. Beispielsweise wurden einige Plattformen für "social networks" im Berichtsjahr Opfer von Hacker-Attacken, Phishing-Betrügern und Identitätsdieben. Mehrfach soll es Tätern mit einfachen Manipulationen gelungen sein, Bilder sowie Daten über politische Orientierung und Familienverhältnisse herunterzuladen, die eigentlich nur einer geschlossenen Benutzergruppe zugänglich sein sollten. Nach Presseberichten konnten in Einzelfällen auch Kennungen und Passwörter von Nutzern entwendet werden.

Die Datenschutzaufsichtsbehörde beim Regierungspräsidium Darmstadt hat sich, wie fast alle anderen Datenschutzaufsichtsbehörden Deutschlands auch, aufgrund der explosionsartigen Entwicklung der sozialen Online-Netzwerke mehrfach mit damit zusammenhängenden datenschutzrechtlichen Fragestellungen befasst, hat in vielen Fällen nachfragende Anwender, Eltern und Schüler beraten, der Presse regelmäßig Rede und Antwort gestanden und auch an einer Podiumsdiskussion zu diesem Thema mit Lehrern, Eltern und Internet-Experten teilgenommen (vgl. Ziffer 2.2).

Im Mittelpunkt standen vor allem die Bemühungen, die Nutzerinnen und Nutzer solcher Netzwerke sensibler dafür zu machen, dass es im Internet keine echte Privatheit gibt und dass die Betroffenen mit ihren Daten vorsichtiger und sparsamer umgehen sollten. Gleichzeitig müssen auch die Anbieter solcher Portale dazu angehalten werden, die datenschutzrechtlichen Grundsätze, zum Beispiel den Grundsatz der Datensparsamkeit, das Transparenzgebot und die Achtung des Selbstbestimmungsrechts der Betroffenen, zu beachten. Dass hier noch erheblicher Verbesserungsbedarf existiert, machte z. B. eine Studie des Fraunhofer-Instituts vom Sommer 2008 deutlich, die erhebliche Datenschutzlücken in "sozialen Netzwerken" diagnostizierte und bei allen sieben großen deutschen Anbietern solcher "social communities" große Lücken in den Bereichen Zugriffskontrolle und deren Steuerungsmöglichkeit, Standardkonfiguration sowie Verschlüsselungsmöglichkeiten feststellte.

Der Düsseldorfer Kreis (siehe bereits Ziffer 6) hat unter Vorsitz des Hessischen Ministeriums des Innern und für Sport dazu folgenden Beschluss auf seiner Sitzung im April 2008 in Wiesbaden gefasst:

"**Datenschutzkonforme Gestaltung sozialer Netzwerke**

Der datenschutzgerechten Gestaltung sozialer Netzwerke im Internet kommt eine zentrale Bedeutung zu. Die Aufsichtsbehörden rufen in diesem Zusammenhang in Erinnerung, dass Anbieter in Deutschland zur Einhaltung des Regulierungsrahmens zum Datenschutz verpflichtet sind. Insbesondere sind folgende rechtliche Rahmenbedingungen einzuhalten:

Anbieter sozialer Netzwerke müssen ihre Nutzer umfassend gemäß den gesetzlichen Vorschriften über die Verarbeitung ihrer personenbezogenen Daten und ihre Wahl- und Gestaltungsmöglichkeiten unterrichten. Das betrifft auch Risiken für die Privatsphäre, die mit der Veröffentlichung von Daten in Nutzerprofilen verbunden sind. Darüber hinaus haben die Anbieter ihre Nutzer aufzuklären, wie diese mit personenbezogenen Daten Dritter zu verfahren haben.

Die Aufsichtsbehörden weisen darauf hin, dass nach den Bestimmungen des Telemediengesetzes (TMG) eine Verwendung von personenbezogenen Nutzungsdaten für Werbezwecke nur zulässig ist, soweit die Betroffenen wirksam darin eingewilligt haben. Bei Werbemaßnahmen aufgrund von Profildaten müssen die Betroffenen nach den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) mindestens eine Widerspruchsmöglichkeit haben. Die Aufsichtsbehörden empfehlen, dass die Anbieter die Nutzer selbst darüber entscheiden lassen, ob - und wenn ja, welche - Profil- oder Nutzungsdaten zur zielgerichteten Werbung durch den Anbieter genutzt werden.

Die Aufsichtsbehörden erinnern weiterhin daran, dass eine Speicherung von personenbezogenen Nutzungsdaten über das Ende der Verbindung hinaus ohne Einwilligung der Nutzer nur gestattet ist, soweit die Daten zu Abrechnungszwecken gegenüber dem Nutzer erforderlich sind.

Für eine vorauseilende Speicherung von Daten über die Nutzung sozialer Netzwerke (wie auch anderer Internet-Dienste) für eventuelle zukünftige Strafverfolgung besteht keine Rechtsgrundlage. Sie wird insbesondere auch nicht durch die Regelungen zur Vorratsdatenspeicherung vorgeschrieben.

Schließlich weisen die Aufsichtsbehörden darauf hin, dass das TMG die Anbieter dazu verpflichtet, das Handeln in sozialen Netzwerken anonym oder unter Pseudonym zu ermöglichen. Dies gilt unabhängig von der Frage, ob ein Nutzer sich gegenüber dem Anbieter des sozialen Netzwerks mit seinen Echtdaten identifizieren muss.

Die Anbieter sind verpflichtet, die erforderlichen technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Sie müssen insbesondere einen systematischen oder massenhaften Export oder Download von Profildaten aus dem sozialen Netzwerk verhindern.

Bei der datenschutzfreundlichen Gestaltung von sozialen Netzwerken kommt den Standardeinstellungen - z. B. für die Verfügbarkeit von Profildaten für Dritte - eine zentrale Bedeutung zu. Die Aufsichtsbehörden fordern die Anbieter sozialer Netzwerke auf, datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch die die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen müssen besonders restriktiv gefasst werden, wenn sich das Portal an Kinder richtet. Der Zugriff durch Suchmaschinen darf jedenfalls nur vorgesehen werden, soweit der Nutzer ausdrücklich eingewilligt hat.

Der Nutzer muss die Möglichkeit erhalten, sein Profil auf einfache Weise selbst zu löschen. Schließlich sollten die Anbieter sozialer Netzwerkdienste die Einführung von Verfallsdaten oder zumindest automatische Sperrungen erwägen, die von den Nutzern selbst festgelegt werden können."

Die größten deutschen Unternehmen, die im WWW als Anbieter von Plattformen für soziale Netzwerke auftreten, haben Anfang 2009 als erste Reaktion auf die vielfach negative Presseberichterstattung im Zusammenhang mit sozialen Online-Netzen und auf den Druck von Jugend-, Daten- und Verbraucherschützern hin eine gemeinsame Selbstverpflichtungserklärung unterschrieben, die den Jugend-, Daten- und Verbraucherschutz auf ihren Seiten im Sinne ihrer Nutzerinnen und Nutzer stärken soll und deren Inhalt den wesentlichen Forderungen der Datenschutzaufsichtsbehörden aus dem o.a. Beschluss des Düsseldorfer Kreises weitgehend entgegenkommt.

9.3 Online-Gewinnspiele und Adresshandel

Zahlreiche Beschwerden gingen gegen ein Adresshandelsunternehmen ein, das zur Adressgewinnung Online-Gewinnspiele betreibt. Die Beschwerdeführer gaben an, dass das Unternehmen Online-Einwilligungen zur E-Mail und Telefonwerbung erschleiche und die so gewonnenen Adressen an Dritte zur werblichen Nutzung übermittle.

Die Datenschutzaufsichtsbehörde schaute sich daraufhin einige dieser Gewinnspiele im WWW an und überprüfte, wie sich das Unternehmen die E-Mail-Adressen und Telefonnummern beschafft.

Dies geschieht, indem der Betroffene auf der Online-Erhebungsmaske zunächst seine Daten für die Teilnahme am Gewinnspiel einträgt. Dann drängt ein blinkender Weiter-Button zum Abschluss des Vorgangs. Unterhalb des Buttons folgt ein Fließtext, der zunächst Informationen zum Gewinnspiel enthält und anschließend auf die beabsichtigte werbliche Nutzung der Daten hinweist. In manchen Gewinnspielen ist dieser Text auch dem Weiter-Button vorangestellt.

Nach Ansicht des Unternehmens hat der Betroffene durch Betätigen des Weiter-Buttons bereits seine wirksame Einwilligung erteilt, da davon auszugehen sei, dass er den Fließtext gelesen habe.

Die Aufsichtsbehörde hat diese Praxis beanstandet und gefordert, die gesetzlichen Bestimmungen der §§ 12 und 13 Telemediengesetz (TMG) einzuhalten.

Nach § 12 Abs. 2 TMG darf der Dienstanbieter für die Bereitstellung von Telemedien erhobene personenbezogene Daten für andere Zwecke nur verwenden, wenn der Nutzer eingewilligt hat. Diese Einwilligung kann nach § 13 Abs.2 TMG elektronisch erklärt werden, wenn der Dienstanbieter sicherstellt, dass der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat und die Einwilligung protokolliert wird.

Erforderlich ist also, dass der Betroffene objektiv einen Einwilligungstatbestand erfüllt und subjektiv mit Handlungswillen, Erklärungsbewusstsein und Geschäftswillen im Hinblick auf die Verarbeitung konkret bezeichneter Daten handelt (Heckmann in juris PK-Internetrecht, Kapitel 1, Abschnitt 13, Rn 25 ff).

Die Arbeitsgruppe Telemedien und Telekommunikation des Düsseldorfer Kreises fordert aus diesen Gründen ein nicht vorbelegtes Kästchen und eine Bestätigungsschaltfläche für die eindeutige und bewusste elektronisch erteilte Einwilligung im Sinne des § 13 Abs. 2 Nr. 1 TMG.

Diese Forderung wird bestätigt durch das sog. Ebay-Urteil des Oberlandesgerichts Brandenburg vom 11. Januar 2006 (7 U 52/05), wonach der Dienstanbieter sicherzustellen hat, dass die Einwilligung durch eine eindeutige und bewusste Handlung des Nutzers erfolgt:

"*Dem ist genügt, wenn ein durchschnittlich verständiger Nutzer erkennen kann und muss, dass er rechtsverbindlich einer Verarbeitung seiner persönlichen Daten zustimmt. Das wiederum ist stets dann anzunehmen, wenn die Einwilligungserklärung durch eine bestätigende Wiederholung des Übermittlungsbefehls bei gleichzeitiger zumindest auszugsweiser Darstellung der Einwilligungserklärung auf dem Bildschirm erteilt wird. (...) Die Einwilligungserklärung wird bestätigend wiederholt, indem der Nutzer zunächst ein Kontrollkästchen mit dem Text (...) und sodann nochmals ein Schaltfeld mit dem Text ‚Ich akzeptiere und willige ein' aktivieren muss.*"

Diese Mindestanforderungen wurden dem Unternehmen als unverzichtbar nach § 13 Abs. 2 Nr. 1 TMG mitgeteilt.

Um außerdem sicherzustellen, dass die E-Mail-Adresse dem Einwilligenden gehört und nicht von einem unbefugten Dritten missbräuchlich angegeben wurde, eignet sich das Double-Opt-In-Verfahren. Hier wird erst durch die Bestätigung einer Begrüßungsnachricht durch den E-Mail-Empfänger, etwa durch Zurücksenden der E-Mail oder durch Anklicken eines in der Begrüßungsnachricht enthaltenen individualisierten Links, der E-Mail-Empfang aktiviert. Reagiert der Empfänger nicht, wirkt das faktisch wie eine Ablehnung (vgl. z. B. AG Berlin Mitte, Urteil vom 11. Juni 2008 - 21 C 43/08).

Zudem kann durch das Double-Opt-In die Protokollierung der Einwilligung zur werblichen Nutzung der E-Mail-Adresse nach § 13 Abs. 2 Nr. 2 TMG einfach gewährleistet werden (vgl. auch die Empfehlungen und Richtlinien zum E-Mail-Marketing der einschlägigen Branchenverbände eco e. V., DMMV e. V., DDV e. V. und BDMV), weil diese immer im E-Mail-Zusammenhang unter Benutzung genau der E-Mail-Adresse, um deren Authentifizierung und spätere Nutzung bzw. Übermittlung es geht, erfolgt. Ein Web-Server-Protokoll, in dem lediglich eine IP-Nummer, ein Zeitstempel und einige technische Daten des Nutzers bei der Dateneingabe in das WWW-Erhebungsformular aufgezeichnet werden, kann diese gesetzlich vorgegebenen Anforderungen an die Protokollierung einer Online-Einwilligung nicht erfüllen. Aus diesen Daten kann systembedingt nicht hervorgehen, ob es sich bei dem Surfer, der eine E-Mail-Adresse zur Teilnahme am Online-Gewinnspiel angegeben hat, auch wirklich um den Inhaber der angegeben E-Mail-Adresse handelt.

Abgesehen von dem Double-Opt-In-Verfahren als solchem ist es maßgeblich, den Handlungswillen des Betroffenen zu dokumentieren. Hier kommt es auf den Text der Einwilligung (verständlich und schlüssig formuliert) und auf den Text der Bestätigungsmail (nochmaliger Hinweis auf die beabsichtigte werbliche Nutzung) an.

Die Datenschutzaufsichtsbehörde ermittelte im oben genannten Fall, dass das Unternehmen das Double-Opt-In-Verfahren zwar anwendet, die Bestätigungs-E-Mail der Gewinnspiel-Teilnehmer aber nicht zwingend abwartet,

sondern die personenbezogenen Daten auch ohne diese direkt an Geschäftspartner zu Werbezwecken übermittelt. In den meisten Beschwerdefällen konnte das Unternehmen als vermeintlichen "Nachweis der Einwilligung" daher nur ein Webserver-Protokoll vorlegen. Dies zeigte dann lediglich, dass irgendein Nutzer zu einer bestimmten Zeit mit einer bestimmten IP-Nummer die E-Mail-Adresse des Beschwerdeführers zur Teilnahme an einem Gewinnspiel in die Erhebungsmaske eingetragen hatte. Dieses Protokoll wurde von der Aufsichtsbehörde nicht als Nachweis der Einwilligung anerkannt, da hier weder nachweisbar ist, dass der Adressinhaber und der Nutzer des Erhebungsformulars identisch sind, noch daraus der Erklärungswille in die werbliche Nutzung des personenbezogenen Datums hervorgeht.

Dem Dienstanbieter wurde mitgeteilt, dass in jedem Einzelfall, in welchem kein belastbarer Nachweis der Einwilligung vorgelegt werden kann, von einer unbefugten Verarbeitung personenbezogener Daten auszugehen ist und die Einleitung eines Bußgeldverfahrens nach § 43 Abs. 2 Nr. 1 BDSG geprüft wird.
Bei Redaktionsschluss war die Frist, innerhalb derer sich der Dienstanbieter äußern sollte, ob er seine Datenerhebungspraxis künftig datenschutzgerecht umgestaltet, noch nicht abgelaufen.

9.4 Branchenverzeichnisse im Internet

Häufig mussten Beschwerdeführer feststellen, dass Ihre Daten (Namen, Adresse, Branche, manchmal Telefonnummer und E-Mail-Adresse) in einem von einem Frankfurter Unternehmen geführten Branchenverzeichnis im Internet zu finden waren. Sie sahen ihre Persönlichkeitsrechte verletzt, da sie von dem Eintrag nichts wussten, geschweige denn ihre Einwilligung im Sinne des § 4a Abs. 1 BDSG dazu gegeben hatten. Die Daten stammten aus öffentlich zugänglichen Quellen, wie zum Beispiel einem Online-Telefonbuch, den Gelben Seiten im Internet oder einem weiteren Verzeichnis, dem sie die Daten aufgrund einer früheren selbständigen Tätigkeit häufig sogar selbst mitgeteilt hatten oder deren Veröffentlichung sie zumindest zugestimmt hatten.

Die Nutzung bereits veröffentlichter Daten ist in diesem Fall nach § 28 Abs. 1 Nr. 3 BDSG bzw. § 29 Abs. 1 Nr. 1 a) BDSG - je nachdem, wo der vorrangige Geschäftszweck der Verzeichnisses anzusiedeln ist - zulässig, solange die schutzwürdigen Interessen des Betroffenen nicht offensichtlich überwiegen. Eine Einwilligung des Betroffenen ist dafür regelmäßig nicht erforderlich. Dementsprechend setzt der Betreiber des Verzeichnisses ständig Webcrawler ein, welche die übrigen Verzeichnisse und andere öffentlich zugängliche Quellen nach personenbezogenen Daten durchsuchen und die Funde mit dem eigenen Datenbestand abgleichen. Soweit die Daten im gleichen Kontext wiedergegeben werden, ist die Verletzung eines offensichtlich schutzwürdigen Interesses nicht zu erwarten und an der Vorgehensweise nichts auszusetzen.

Falls die Daten falsch wiedergegeben werden oder veraltet sind, besteht nach § 35 Abs. 1 bzw. Abs. 2 BDSG ein Anspruch auf Berichtigung bzw. Löschung. Dem kommt das Unternehmen nach. Mittlerweile wird auf Ersuchen der Aufsichtsbehörde auch die Herkunft der Daten gespeichert, um dem zur Wahrung der Rechte auf Berichtigung und Löschung unverzichtbaren Auskunftsanspruch nach §§ 6, 34 BDSG genügen zu können.

9.5 Schuldnerlisten im Internet

In mehreren Fällen schilderten Beschwerdeführer, dass die über Internetsuchmaschinen erzielten Suchergebnisse zu ihrem Namen erkenne ließen, dass sie in Insolvenz geraten waren. Mit Insolvenzverwaltung beschäftigte Anwaltsbüros hatten Listen der bearbeiteten Fälle im Internet veröffentlicht, um den jeweiligen Insolvenzverwaltern die Arbeit zu erleichtern und Gläubigern die Möglichkeit zu bieten, sich anzumelden. Sie beriefen sich dabei auf eigene Geschäftszwecke im Sinne des § 28 BDSG und die Tatsache, dass die Schuldnerdaten im Rahmen der gerichtlichen Insolvenzbekanntmachungen ohnehin im Internet zu finden seien und damit auch für andere Zwecke an einen Dritten weitergegeben werden können.

In der Tat werden die Schuldnerdaten nach § 9 Abs. 1 Insolvenzordnung (InsO) auf einer Website des Justizministeriums Nordrhein-Westfalen im Internet amt-

lich bekanntgegeben. Das Land Hessen beteiligt sich seit dem 1. Dezember 2003 an diesem Verfahren. Die Rahmenbedingungen sind nach § 9 Abs. 2 InsO durch die Verordnung zur öffentlichen Bekanntmachung von Insolvenzverfahren im Internet vom 12. Februar 2002 geregelt. Ein Suchlauf ohne Kenntnis des Verfahrens auf der Seite "www.insolvenzbekanntmachungen.de" führt zunächst einmal nur zu Grunddaten (Name, Gericht und Aktenzeichen). Anschließend sind beim Anklicken des Links die Einzelheiten des Verfahrens für jedermann aufrufbar, allerdings höchstens 2 Wochen lang. Danach muss bereits zur Durchführung des Suchlaufs der Sitz des Insolvenzgerichts und zusätzlich Familienname, Wohnsitz oder Aktenzeichen des Insolvenzverfahrens genannt werden. Die Liste ist für Suchmaschinen nicht auffindbar und der jeweilige Datensatz wird spätestens sechs Monate nach der Aufhebung oder der Rechtskraft der Einstellung des Insolvenzverfahrens gelöscht.

Werden die Schuldnerlisten nun durch die Anwaltsbüros offen zugänglich ins Internet gestellt, ist hierauf nicht § 28, sondern § 29 BDSG anzuwenden, da die Daten unabhängig von den jeweiligen Geschäftsabläufen für einen unbestimmten Empfängerkreis abrufbar sind. Die Bereitstellung von allgemein zugänglichen Daten ist nach § 29 Abs. 1 Nr. 2 BDSG möglich, solange keine offensichtlich schutzwürdigen Interessen des Betroffenen entgegenstehen. Diese Voraussetzung ist nur dann erfüllt, wenn die Veröffentlichungen der Anwaltsbüros auch die in der Verordnung zu öffentlichen Bekanntmachungen von Insolvenzverfahren im Internet genannten Bedingungen erfüllen. Andernfalls werden die durch die Regelungen für amtliche Insolvenzbekanntmachungen im Internet gesetzten Einschränkungen unterlaufen. Durch die einfachen und zeitlich unbegrenzten Auswertungsmöglichkeiten im Internet wird das Ziel, dem Schuldner nach Abschluss des Insolvenzverfahrens einen Neustart zu ermöglichen, unmöglich gemacht. Zu diesem Urteil kommt auch der Hessische Datenschutzbeauftragte in seinem 37. Tätigkeitsbericht (Drucks. 18/106 Ziffer 4.1.2.1).

Die Übermittlung an Dritte darf nach § 29 Abs. 2 Nr. 1 a) und Nr. 2 BDSG nur erfolgen, soweit diese ein berechtigtes Interesse glaubhaft darlegen und keine schutzwürdigen Interessen des Betroffenen dagegen sprechen (zur Problematik der Anwendung der BDSG-Vorschriften auf Internet-Angebote, insbesondere der Abgrenzung zwischen § 28 und § 29 BDSG siehe Ziffer 9.3 des 21. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde, Drucks. 17/663).

Werden die Daten in einer Weise zur Übermittlung bereitgehalten, dass sie von Suchmaschinen nicht recherchiert werden können, reduzieren sich die potentiellen Übermittlungen auf den Personenkreis, der die Website des Insolvenzverwalters gezielt aufsucht. Während der ersten zwei Wochen genügt dies den Anforderungen und die schutzwürdigen Interessen der Betroffenen treten demgegenüber zurück. Nach Ablauf der ersten zwei Wochen muss durch Angabe bereits bekannter Einzelheiten ein berechtigtes Interesse nachgewiesen werden, das die schutzwürdigen Interessen der Betroffenen überwiegt.

Die von der Aufsichtsbehörde angeschriebenen verantwortlichen Stellen haben umgehend durch technische Maßnahmen ("Robots.txt") den Zugriff durch Suchmaschinen unterbunden. Ein Anwaltsbüro hat darüber hinaus den gesamten Bereich durch ein nur für die Gläubiger erhältliches Passwort geschützt, was die in der Verordnung zur öffentlichen Bekanntmachung von Insolvenzverfahren im Internet vorgesehenen Beschränkungen sogar noch übertrifft; eine weitere verantwortliche Stelle ist noch mit der Umstellung beschäftigt.

9.6 Überraschende Funde im Internet: Die unbeabsichtigte Veröffentlichung personenbezogener Daten im WWW

Der Gebrauch von Internetsuchmaschinen ist für alle Surfer eine Selbstverständlichkeit. Zum einen natürlich, um sich in der Vielfalt der Online-Angebote überhaupt orientieren zu können. Zum andern sucht fast ein Drittel aller Internet-Nutzer regelmäßig im WWW nach dem eigenen Namen (sog. "Ego-Googlen", vgl. auch Ziffer 9.5 dieses Berichts), teilweise sogar in hierauf spezialisierten Namenssuchmaschinen (siehe hierzu Ziffer 9.3 des 21. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde,

Drucks. 17/663). Dass die Ergebnisse solcher Namenssuchen für große Überraschungen sorgen können, mussten einige Betroffene feststellen, die sich daraufhin mit der Bitte an die Datenschutzaufsichtsbehörde wandten, bei den jeweiligen Host- und Content-Providern für eine umgehende Löschung ihrer Daten zu sorgen:

Ein Bürger fand seinen Namen beispielsweise zusammen mit seiner E-Mail-Adresse und den Daten seines Arbeitgebers auf einer umfangreichen Liste, die auf den WWW-Seiten eines Dienstleisters aus dem Bankbereich angeboten wurde. Wie sich herausstellte, handelte es sich um die Daten der Besucher eines Messestands, die sich dort vor mehr als zwei Jahren für einen speziellen Newsletter angemeldet hatten. Auf Hinweis der Datenschutzaufsichtsbehörde wurden die Daten von dem Telemedien-Anbieter umgehend entfernt. Als Grund für die kurzzeitige Veröffentlichung der eigentlich als internes Backup vorgesehenen Liste stellte sich die Fehlbedienung des Content-Management-Systems bei einem Dienstleistungsunternehmen heraus. Da der Anbieter zusätzlich einen Eilantrag bei der Internet-Suchmaschine Google zur Löschung der Inhalte aus dem Google-Cache stellte, war die Auflistung kurz darauf auch aus der Google-Trefferliste verschwunden. Die Veröffentlichung der Daten wurde beanstandet. Der Dienstleister nahm den Vorfall zum Anlass, sein WWW-Angebot intensiv nach weiteren möglichen unbeabsichtigten Veröffentlichungen zu durchsuchen.

In einem weiteren Fall erhielt die Datenschutzaufsichtsbehörde folgenden Hinweis über eine anonyme E-Mail-Adresse: Auf dem Server eines hessischen Host-Providers, der als Anbieter fremder Inhalte nach § 10 TMG hauptsächlich für Privatpersonen kostenlos Speicherplatz und eine individuelle WWW-Adresse für eine eigene Homepage anbietet, war es möglich, listenartig in alle dort angelegten Verzeichnisse dieser Homepage-Kunden Einblick zu erhalten. Dabei waren nicht nur die Verzeichnisse mit den Dateien der Homepage-Inhalte abrufbar, sondern man konnte mit wenig Aufwand auch die Konfigurationsdateien und die Access-Logfiles der Betroffenen auslesen. Auch dieser Provider reagierte noch am selben Tag auf die entsprechende Nachfrage der Datenschutzaufsichtsbehörde. Der sehr engagierte betriebliche Datenschutzbeauftragte des Unternehmens sorgte für die umgehende Beseitigung der Lücke in dem Webserver, auf dem das Angebot gehostet wurde. Die unbeschränkte Zugriffsmöglichkeit auf die Daten der Homepage-Kunden wurde hierdurch unterbunden. Als Grund für den mangelhaften Zugriffsschutz stellte sich ein ungewöhnlicher Konfigurationsfehler bei dem betroffenen Webserver heraus, der von den bereits implementierten Prüfmechanismen nicht gefunden wurde. Der betriebliche Datenschutzbeauftragte veranlasste daraufhin, dass die vorhandenen Aktualisierungs- und Prüfmechanismen der Homepage-Webserver verbessert wurden, um solche Konfigurationsabweichungen künftig sofort erkennen zu können. Festgehalten werden muss, dass auch dieser Vorfall nur bemerkt wurde, weil ein betroffener Bürger bei der Internetrecherche mittels Suchmaschine nach seinem Namen auf die unbeabsichtigte Veröffentlichung aufmerksam wurde.

Ein weiterer Homepage-Kunde wandte sich an die Datenschutzaufsichtsbehörde, weil er mit Hilfe einer Internetsuchmaschine festgestellt hatte, dass unter der Adresse seiner alten Homepage noch Daten und Unterlagen öffentlich angeboten wurden, obwohl er seinen Vertrag bei dem Provider schon seit einigen Jahren gekündigt habe. Er gab an, heute auch keine Kennung und kein Passwort mehr für den Account zu besitzen. Da der Kundenservice des Unternehmens auf seine Fragen, Hinweise und Löschungsbitten nicht reagierte, bat er die Datenschutzaufsichtsbehörde um Rat, wie weiter vorzugehen sei. Auch dieser Anbieter reagierte sofort auf die Beanstandung durch die Datenschutzaufsichtsbehörde und löschte die mittlerweile unerwünschten Inhalte des Petenten von der Homepage. Das Unternehmen teilte allerdings auch mit, dass die kostenlose Homepage unabhängig von dem gekündigten Vertrag gewesen sei und weiter Bestand hatte. Allerdings sei das Passwort für die Homepage schon vor Jahren gesperrt worden, da der Betroffene sein Passwort damals selbst mehrfach falsch angegeben habe. Der Betroffene habe sich für seine Homepage wohl einfach nicht mehr interessiert und er habe sich nicht mehr darum gekümmert, zum Beispiel habe er kein neues Passwort beantragt. Weshalb der Kundenservice des Unternehmens die Nachfragen des Ex-Kunden ignoriert hatte, nachdem dieser durch eine Suche im Internet wieder an die alte Homepage erinnert wurde, konnte nicht aufgeklärt werden.

9.7 Versand von Massen-E-Mails an offen gelegte Adresslisten

Auch im Berichtsjahr 2008 gab es erneut Beschwerden bezüglich der Versendung von Massen-E-Mails an offen gelegte Adresslisten.

Im Tätigkeitsbericht für 2006 (siehe hierzu unter Ziffer 12.2 des 20. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde, Drucks. 16/7647) war über diese Problematik bereits berichtet worden.

Ein bundesweit tätiger Verein startete eine Werbeaktion zur Förderung benachteiligter Kinder durch die Übersendung einer E-Mail mit 900 offenen Empfänger-Adressen. Ein Arzt gab unzulässigerweise E-Mail-Adressen seiner Patienten preis, indem er Informationen zur Eröffnung einer Gemeinschaftspraxis an ca. 750 Patienten aus Deutschland und dem europäischen Ausland im offen gelegten "An"-Feld übersandte. Letzterer Fall ist besonders hervorzuheben, da hier das Vertrauensverhältnis Arzt-Patient empfindlich gestört wurde. Auch waren 3.000 Empfänger im offenen "An"- bzw. "Cc"-Feld einer E-Mail zu lesen, die ein hessisches Unternehmen an seine Kunden versandte - da kann bei einem Ausdruck das Papier knapp werden. Aber es gibt noch weit größere Probleme.

Datenschutzrechtlich ist der Versand einer Massen-E-Mail mit offen gelegter Adressatenliste unzulässig. Es handelt sich bei jeder einzelnen Übermittlung einer E-Mail-Adresse um die Übermittlung personenbezogener Daten, die jeweils nicht erforderlich war und ohne Rechtsgrundlage erfolgte. Damit kann nach § 43 Abs. 2 Nr. 1 BDSG der Tatbestand einer Ordnungswidrigkeit erfüllt sein, wenn sich darunter E-Mail-Adressen befinden, die nicht öffentlich zugänglich sind.

Die Datenschutzaufsichtsbehörde teilte den Verursachern jeweils mit, dass diese Art des Versands sich nur für geschlossene Benutzergruppen von überschaubarer Größe oder für vergleichbare Adressatengruppen eignet, bei denen die Erforderlichkeit für die Übermittlung der Daten an alle anderen besteht und keine schutzwürdigen Interessen entgegenstehen.

Der Versand einer E-Mail an einen großen Empfängerkreis außerhalb solcher Benutzergruppen hat stets in der Weise zu erfolgen, dass die E-Mail-Adressen den jeweils anderen Empfängern der Massenmail unbekannt bleiben. Hierzu muss der Versender die Adressaten in das "Bcc"-Feld eintragen, die E-Mail-Adressen bleiben für den Empfänger unsichtbar. In das "An"-Feld wird eine eigene E-Mail-Adresse eingetragen.

Neben der datenschutzrechtlichen Problematik kommt hier der Aspekt der Datensicherheit hinzu. Einige Schadprogramme verschicken sich selbständig an jede E-Mail-Adresse, die sie auf dem befallenen PC finden. Sie können Funktionen beeinträchtigen, vertrauliche Daten ausspionieren oder Spam versenden. Wird das oben empfohlene Verfahren angewendet, können höchstens zwei E-Mail-Adressen betroffen sein. Ganz anders sieht dies im Fall einer Massen-E-Mail mit offenem Adressatenkreis aus.

Hinzu kommt, dass durch die Versendung mittels einer offen gelegten Adressliste die erhaltenen E-Mail-Adressen von den Empfängern für unverlangte Werbe-E-Mails genutzt werden können ("Spamming"). Dies kann durch die hohe Zahl der Posteingänge bis zur Funktionsunfähigkeit eines E-Mail-Accounts führen. Bei einer E-Mail mit offen gelegter Adressliste haftet der Versender zudem zivilrechtlich als Mitstörer auch für den Missbrauch der E-Mail-Adressen der Empfänger der Werbe-Mail durch andere Empfänger.

Nach Ansicht des OLG Düsseldorf (Urteil vom 24. Mai 2006 - Az: I 15 U 45/06) "*greift die Einwilligung stets nur für einen ordnungsgemäßen, Datenschutz und Sicherheit der E-Mail-Adresse wahrenden Versand…Werden beim Versand die Empfängeradressen durch Verwendung der Cc-Funktion …bekannt, greift die Einwilligung nicht mehr.*"

Das Vertrauen der Betroffenen (Kunden, Patienten, Mitglieder) in die verantwortliche Stelle wird durch das Versenden von Massen-E-Mails rasch und wirkungsvoll gestört. Wird bereits mit den E-Mail-Adressen derart sorglos umgegangen, liegt auch ein liederlicher Umgang mit anderen Daten nahe. Eine weitere unerwünschte Folge ist, dass Konkurrenten Einblick in

Kundenkontakte erhalten können. Ferner entlarvt sich der Versender als Laie im Umgang mit neuen Kommunikationsformen, was sowohl peinlich als auch unseriös sein kann.

In allen geschilderten Fällen wurden die Verursacher auf ihr datenschutzrechtlich unzulässiges Handeln hingewiesen und Beanstandungen ausgesprochen. Die verantwortlichen Stellen entschuldigten den Versand regelmäßig als Versehen und Ergebnis menschlicher Fehler.

Im Rahmen der Bearbeitung der Massen-E-Mail, die durch ein Unternehmen versandt worden war, äußerte sich der Geschäftsführer nicht zu den Fragen der Aufsichtsbehörde. Es wurde daher ein inzwischen rechtskräftiges Bußgeld in Höhe von 2.000,00 € wegen mangelnder Auskunftserteilung nach § 43 Abs. 1 Nr. 10 BDSG verhängt, ein weiteres Verfahren ist noch gerichtsanhängig.

Die Bearbeitung der beiden anderen geschilderten Fälle ist noch nicht abgeschlossen, die verantwortlichen Stellen müssen jedoch mit der Einleitung von Ordnungswidrigkeitenverfahren nach § 43 Abs. 2 Nr. 1 BDSG rechnen.

10. Werbewirtschaft, Adresshandel, Direktmarketing Missachtung unabdingbarer Rechte von Betroffenen in der Werbebranche

Wie schon in den vergangenen Jahren hatte sich die Aufsichtsbehörde auch im Berichtsjahr 2008 wieder mit zahlreichen Beschwerden im Bereich Werbewirtschaft, Adresshandel und Direktmarketing zu befassen. Grund hierfür war die Missachtung unabdingbarer Rechte Betroffener nach § 6 BDSG. Auskunftsbegehren nach § 34 Abs. 1 BDSG wurden ignoriert, Werbewidersprüche nach § 28 Abs. 4 BDSG nicht beachtet, Daten wurden gelöscht, mit der Folge, dass eine Auskunftserteilung nach § 34 Abs. 1 BDSG insbesondere auch über die Adressherkunft nicht mehr möglich war.

Eine deutliche Zunahme der Beschwerden war im Bereich des Telefon- und E-Mail-Marketing zu verzeichnen. Das Hauptproblem war hier die fehlende Einwilligung der Betroffenen in die werbliche Ansprache.

Zwar räumt das BDSG den Betroffenen eine Vielzahl von Rechten ein, doch sind ihre Möglichkeiten, diese gegenüber den Unternehmen durchzusetzen, begrenzt bzw. mühsam und nur über den zivilen Rechtsweg erreichbar. Erhält der Betroffene keine Antwort auf sein Auskunftsbegehren, kann er auch seine Folgerechte auf Sperrung, Löschung und Werbewiderspruch nicht wahrnehmen. Die Missachtung des Anspruchs auf Auskunft nach § 34 Abs. 1 BDSG erfüllt derzeit keinen Ordnungswidrigkeitentatbestand.

Vor der Einleitung eines zivilrechtlichen Verfahrens wenden sich die Betroffenen daher in der Regel an die Datenschutzaufsichtsbehörde. Durch deren Beteiligung erfahren sie, auf welchen Wegen ihre Adresse in den gewerblichen Adresshandel gelangte und die Zusendung unerwünschter Werbung kann wirksam unterbunden werden.

Wird die Auskunft an die Aufsichtsbehörde nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt, verfügt diese mit § 43 Abs. 1 Nr. 10 BDSG über ein wirksames Mittel, sich im Sinne der Betroffenen durchzusetzen. Die Bußgeldandrohung führte in den allermeisten Fällen zur gewünschten Auskunft. Wurde diese nicht erteilt, wurden Bußgeldverfahren eingeleitet.

Erfreulicherweise beabsichtigt die Bundesregierung, die Rechte der Betroffenen zu stärken, indem künftig bereits die Missachtung der Auskunftsrechte gegenüber den Betroffenen mit einem Bußgeld sanktionierbar sein soll (siehe Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes vom 8. August 2008, Bundesrats-Drs. 548/08).

11. Aspekte internationaler Datenverarbeitung Reaktion der Wirtschaft auf den Beschluss des Düsseldorfer Kreises vom April 2007

Der Düsseldorfer Kreis hatte in seiner Sitzung vom 19./20. April 2007 zwei Dokumente anerkannt und beschlossen, die zuvor in der Arbeitsgruppe In-

ternationaler Datenverkehr erarbeitet worden waren. Es handelt sich um ein Positionspapier zu einigen Fragestellungen des internationalen Datenverkehrs und um eine Handreichung zur rechtlichen Bewertung von Fallgruppen zur internationalen Auftragsdatenverarbeitung. Der Beschluss einschließlich dieser Papiere ist im Internet unter anderem abrufbar unter: "www.rp-darmstadt.hessen.de" (Pfad: "Sicherheit und Ordnung/Datenschutz/Auslandsdatentransfer").

Bereits im 20. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde, Drucks. 16/6929, wurden unter Ziffer 9 die in diesen Dokumenten behandelten Rechtsfragen und deren Bewertung dargestellt, da sich diese hauptsächlich im Rahmen der Beratungstätigkeit des Regierungspräsidiums Darmstadt ergeben hatten. Der in diesem Bericht noch enthaltene Vorbehalt, dass der - damals noch nicht gefasste - Beschluss des Düsseldorfer Kreises maßgeblich sei, ist zwischenzeitlich obsolet, da der Beschluss die Ergebnisse der Arbeitsgruppe Internationaler Datenverkehr uneingeschränkt bestätigte.

Ein Jahr danach, im April 2008, hat der BITKOM gegenüber dem Leiter der Arbeitsgruppe Internationaler Datenverkehr, dem Berliner Beauftragten für Datenschutz und Informationsfreiheit, ein "Echo" zu dem Beschluss des Düsseldorfer Kreises abgegeben. Der BITKOM ist ein Interessenverband der IT-, Telekommunikations- und Neue-Medien-Branche. Die von den Mitgliedsunternehmen gesammelten praktischen Erfahrungen und die Erörterungen im Verband sind in dem "Echo" dargestellt.

Für die Aufsichtsbehörden war es sehr interessant und hilfreich, diese Resonanz zu erhalten. Daher hat sich die Arbeitsgruppe Internationaler Datenverkehr in ihrer Herbstsitzung 2008 sehr eingehend damit befasst, wobei das Regierungspräsidium Darmstadt umfangreiche Vorarbeiten leistete. Die in der Arbeitsgruppe erarbeitete Stellungnahme wurde sodann im gesamten Düsseldorfer Kreis abgestimmt und im Januar 2009 vom Vorsitzenden des Düsseldorfer Kreises an den BITKOM gesandt. Diese Stellungnahme ist derzeit nicht zur Veröffentlichung vorgesehen. Einige Kernpunkte sollen jedoch im Folgenden dargestellt werden, da sie von allgemeinem Interesse sein dürften.

Der BITKOM bemängelte grundsätzlich, dass in der Handreichung zu Fallgruppen der internationalen Auftragsdatenverarbeitung "*wichtige datenschutzrechtliche Instrumente wie das Safe Harbour-Abkommen und Binding Corporate Rules oder vertragliche Gestaltungsmöglichkeiten*" nicht einbezogen worden sind.

Hierzu stellte der Düsseldorfer Kreis klar, dass in der Handreichung ganz bewusst nur einige Fallgestaltungen dargestellt wurden. Keinesfalls erhebt die Handreichung den Anspruch, dass alle denkbaren Fallgestaltungen behandelt werden sollten. Demzufolge wurden auch nicht alle denkbaren Varianten von Lösungsmöglichkeiten behandelt. Beispielsweise wurde die Betrachtung der Fallgruppen A und B bewusst auf die Darstellung von Lösungsmöglichkeiten beim Einsatz der Standardvertragsklauseln beschränkt. In den Fallgruppen C und D wurde zwar zusätzlich bzw. alternativ vom Vorhandensein individueller Verträge ausgegangen, dies war jedoch für die betrachtete Problematik und die zu findende Lösung unerheblich. In allen Fällen wurden Varianten, bei denen der Datenimporteur Safe-Harbor-zertifiziert ist oder BCRs bestehen, bewusst ausgeklammert.

Die Aussage in dem Beschluss des Düsseldorfer Kreises, dass in der Handreichung die "wichtigsten" Fallkonstellationen dargestellt seien, ist also insoweit zu relativieren, als sich die Fallkonstellationen bzw. die dargestellten Lösungsmöglichkeiten im wesentlichen auf die Fälle beschränken, bei denen die EU-Standardverträge eingesetzt werden sollen.

Der Düsseldorfer Kreis beabsichtigt derzeit nicht, die Handreichung zu ergänzen. Dies heißt jedoch nicht, dass sich die Arbeitsgruppe künftig nicht auch mit weiteren Fallgestaltungen befassen wird. Beispielsweise sollen einige zusätzliche Fallgestaltungen, die auch in den vom BITKOM genannten Praxisfällen relevant sind und zu denen zum Teil konkrete Beratungsanfragen beim Regierungspräsidium Darmstadt vorliegen, in der nächsten Sitzung der Arbeitsgruppe behandelt werden.

Bezüglich der Fallgruppe A der Handreichung hielt der BITKOM die dargestellte Lösung der Aufsichtsbehörden (Abschluss eines Standardvertrags zwischen dem Auftraggeber und dem Unterauftragnehmer im Drittstaat bzw. dessen Beitritt zum Standardvertrag zwischen Auftraggeber und Auftragnehmer in Deutschland/der EU) für nicht hinreichend praktikabel und interessengerecht. Der BITKOM favorisierte statt dessen die Lösung, dass der Datenverarbeitungsdienstleister in eigenem Namen einen Vertrag mit dem Unterauftragnehmer schließt.

Hierzu stellte der Düsseldorfer Kreis - in Anknüpfung an die obigen Ausführungen - klar, dass der Düsseldorfer Kreis nur Lösungen für eine Unterbeauftragung im Drittstaat gesucht hat, die auf der Basis der Standardverträge zu realisieren sind, also Lösungen, die keiner Genehmigungserteilung nach § 4c Abs. 2 BDSG bedürfen. Dabei war von vornherein klar, dass es ideale Lösungen auf der Grundlage des Controller-Processor-Standardvertrags vom Dezember 2001 nicht geben kann, denn dieser Standardvertrag geht nur von einem zweiseitigen Rechtsverhältnis zwischen Auftragnehmer und Auftraggeber aus. Gestufte Rechtbeziehungen wie bei der Unterbeauftragung sind in diesem Standardvertrag nicht geregelt.

Auf europäischer Ebene gibt es Diskussionen über einen alternativen Controller-Processor Standardvertrag, der von Wirtschaftsverbänden/-vertretern erarbeitet wurde. Dieser Entwurf sieht eine spezielle Klausel für Unterauftragsverhältnisse vor. Die deutschen Aufsichtsbehörden haben es grundsätzlich begrüßt, dass eine solche Klausel geschaffen wird. Die Diskussionen über die Ausgestaltung dieser Klausel und über diesen alternativen Entwurf waren aber im Berichtsjahr insgesamt noch nicht abgeschlossen.

Solange ein alternativer Standardvertrag mit einer entsprechenden Regelung nicht in Kraft getreten ist, kann der Vorschlag des BITKOM jedenfalls nicht als "genehmigungsfreie Standardvertragslösung" akzeptiert werden. Der Düsseldorfer Kreis regte an, dass der BITKOM seine Lösung näher ausarbeitet. Falls vom BITKOM gewünscht, könnte im Düsseldorfer Kreis dann eine grundsätzliche Bewertung erfolgen, ob die Texte als Grundlage einer Genehmigung nach § 4c Abs. 2 BDSG geeignet sind. Ferner empfahl der Düsseldorfer Kreis dem BITKOM, sich über die europäischen Wirtschaftsverbände in die Erörterungen auf europäischer Ebene zu einem alternativen Controller-Processor Standardvertrag einzubringen. Bezüglich der Kritik des BITKOM an der in der Handreichung dargestellten Lösung zur Fallgruppe B gilt entsprechendes.

Ein weiterer Kritikpunkt des BITKOM bezog sich auf die Aussagen unter Nummer II.2 und II.3 des Positionspapiers, worin der Düsseldorfer Kreis darauf hinweist, dass Wertungswidersprüche zwischen den Anforderungen der sog. "Ersten Stufe" und den Reglungen in den EU-Standardverträgen vermieden werden müssen. (Näheres siehe Ziffer 9.2 des 20. Berichts der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde, Drs. 16/6929.). Demzufolge hatte der Düsseldorfer Kreis insbesondere Vorbehalte gegen die Verwendung des alternativen Standardvertrags vom Dezember 2004 beim Drittstaatentransfer von Arbeitnehmerdaten geäußert.

Der Düsseldorfer Kreis erläuterte gegenüber dem BITKOM, dass Art. 2 Satz 2 des Standardvertrags vom Juni 2001, der ausdrücklich davon ausgeht, dass nationale Bestimmungen unberührt bleiben, gerade nicht durch die Entscheidung der Kommission zu dem alternativen Standardvertrag geändert wurde (s. Art 1 der Entscheidung von 2004). Wenngleich nicht jedes Zurückbleiben des Schutzes im Zielland durch erhöhte Anforderungen auf der 1. Stufe und entsprechende Regelungen kompensiert werden muss, so kann andererseits nicht jedes Zurückbleiben akzeptiert werden. Gerade im Arbeitnehmerbereich kann es nicht ohne weiteres hingenommen werden, dass sich der Arbeitgeber den Anforderungen des BDSG und des deutschen Arbeitsrechts durch Verlagerung der Datenverarbeitung ins Drittland entzieht und diese nationalen Anforderungen damit unterlaufen werden.

Der Düsseldorfer Kreis stellte klar, dass er die Verwendung des alternativen Standardvertrags nicht schlichtweg ablehnt, vielmehr wurde in Position II.2 darauf hingewiesen, dass dieser Vertrag "evtl. ergänzungsbedürftig" sei.

Ferner wurden für die relevanten Probleme konkrete Lösungsmöglichkeiten aufgezeigt, damit die Standardverträge vom Juni 2001 und Dezember 2004 verwendet, aber gleichzeitig Wertungswidersprüche vermieden werden können:

a) Problem: Die o. g. Standardverträge sehen bei Werbung nur ein Widerspruchsrecht (opt out) vor, nach dem BDSG hingegen ist bei Arbeitnehmerdaten grundsätzlich eine Einwilligung erforderlich.
Lösung: Wenn in der Anlage zum Standardvertrag als Zweck der Übermittlung die Werbung nicht aufgeführt ist, darf der Importeur die Daten nicht für Werbezecke nutzen oder weiterübermitteln. Dann wäre das Problem also obsolet. Wenn der Importeur jedoch die Daten auch für Werbezwecke nutzen und verarbeiten können soll, muss dieser Zweck in der Anlage aufgeführt werden und der Arbeitgeber muss vor der Übermittlung die Einwilligung der Arbeitnehmer hierfür einholen.

b) Problem: Der alternative Standardvertrag 2004 sieht in Klausel I.d vor, dass vereinbart werden kann, dass der Importeur die Auskunftserteilung übernimmt. Schutzwürdige Belange der Arbeitnehmer erfordern es aber grundsätzlich, dass er sich an den Exporteur wenden kann (zu den Differenzierungen und entsprechenden Ausnahmen wird auf die Ausführungen im Arbeitsbericht der ad-hoc-AG zum konzerninternen Datentransfer, abrufbar unter "www.rp-darmstadt.hessen.de" (Pfad: "Sicherheit und Ordnung/Datenschutz/Arbeitnehmerdatenschutz"), verwiesen).
Lösung: In einer Fußnote zur Klausel I.d ist kenntlich zu machen, dass von dieser Option kein Gebrauch gemacht wird; alternativ eine Garantieerklärung (siehe unter c).

c) Problem: Der alternative Standardvertrag 2004 sieht vor, dass u. U. nur der Importeur haftet. Schutzwürdige Belange der Arbeitnehmer erfordern es aber grundsätzlich, dass er sich an den Exporteur wenden kann.
Lösung: Garantieerklärung des Exporteurs (vgl. Schmidl, DuD 4/2008, Seite 258 f). Nach Auffassung der Aufsichtsbehörden könnte diese Garantieerklärung auch in einer Betriebsvereinbarung enthalten sein. Insoweit wäre eine "Unterwerfungs-Erklärung" des Importeurs unter die Betriebsvereinbarung nicht erforderlich, denn es ist Sache des Exporteurs, ob und inwieweit er den Arbeitnehmern zusätzliche Garantien gibt, sodass er selbst für die Rechte der Betroffenen einsteht.

Im Übrigen bestand sehr weitgehend Übereinstimmung mit dem BITKOM. Zum Teil gab es vermeintliche Gegensätze, die jedoch durch Erläuterungen und Klarstellungen seitens des Düsseldorfer Kreises aufgelöst werden konnten. Für die Aufsichtsbehörden war es sehr hilfreich, zu erfahren, inwieweit es Missverständnisse geben kann. Die gewonnen Erfahrungen werden in der Beratungspraxis Berücksichtigung finden.

In Bezug auf das Positionspapier wies der Düsseldorfer Kreis darauf hin, dass dieses nicht aus sich heraus umfassend verständlich ist. Es ist aufgrund einer Sondersitzung der Arbeitsgruppe Internationaler Datenverkehr vom Juni 2007 entstanden, in der einige Vertreter der Wirtschaft Gelegenheit hatten, ihre Auffassungen und Erfahrungen darzulegen. Es muss daher im Zusammenhang mit dem Sitzungsverlauf gesehen werden. Im Übrigen sind auch nicht alle denkbaren Fragen erschöpfend behandelt.

Unter Ziffer 9 des 20. Tätigkeitsberichts (a.a.O.) sind einige Erläuterungen hierzu enthalten, für weitere Fragen sollten sich Unternehmen an die für sie zuständige Aufsichtsbehörde wenden. Hierauf hat das Regierungspräsidium Darmstadt bei der Veröffentlichung des Positionspapiers auf seiner Website bereits hingewiesen.

12. Arbeitnehmerdatenschutz

12.1 Mitarbeiterüberwachung in Lebensmittelmärkten

Im Berichtsjahr wurden die Aufsichtsbehörden im Bundesgebiet mit mehreren Fällen der Mitarbeiterüberwachung in Lebensmittelmärkten konfrontiert, die bei weitem die Grenze des rechtlich Zulässigen überschritten.

Auslöser für umfangreiche datenschutzrechtliche Überprüfungen war der Bericht eines Nachrichtenmagazins, demzufolge die Mitarbeiter in den Filia-

len eines großen Lebensmitteldiscounters einer systematischen Bespitzelung durch den Einsatz von Videokameras, Detekteien und anderen Sicherheitsunternehmen ausgesetzt waren. Der Artikel enthielt Auszüge aus Einsatzprotokollen, in denen unter anderem Informationen aus dem Privatleben, zum Beispiel über Beziehungsprobleme oder finanzielle Schwierigkeiten sowie über das Verhalten der Mitarbeiter bei der Arbeit und im Umgang miteinander berichtet wurde.

Auftraggeber der Detekteien waren die rechtlich selbständigen Vertriebsgesellschaften des Lebensmitteldiscounters, die sich auf zwölf Bundesländer verteilen. Daher leiteten die für die Unternehmenssitze zuständigen zwölf Aufsichtsbehörden gegen die jeweiligen Vertriebsgesellschaften datenschutzrechtliche Überprüfungsverfahren ein, deren Koordination die Aufsichtsbehörde in Baden-Württemberg (Innenministerium) übernahm.

Nach den Feststellungen der Aufsichtsbehörden enthielten etwa die Hälfte der noch vorhandenen Einsatzprotokolle unzulässige Inhalte. Die damit verbundenen datenschutzrechtlichen Verstöße wurden vielfach als schwerwiegend bewertet. Auch für die Videobeobachtung der Mitarbeiter fehlte in vielen Fällen die Rechtsgrundlage.

Alle Vertriebsgesellschaften waren darüber hinaus ihrer nach § 4f BDSG bestehenden Verpflichtung, einen betrieblichen Datenschutzbeauftragten zu bestellen, nicht nachgekommen.

Gegen die Vertriebsgesellschaften wurden Bußgelder in einer Gesamthöhe von rd. 1,5 Mio. € festgesetzt. Die gegen die einzelnen Gesellschaften verhängten Geldbußen bewegten sich dabei zwischen 10.000 und 310.000 €. Geahndet wurde von allen Aufsichtsbehörden die Nichtbestellung eines Datenschutzbeauftragten mit jeweils 10.000 €. Geldbußen wegen unzulässiger Mitarbeiterüberwachung wurden dann festgesetzt, wenn Verstöße anhand von Einsatzprotokollen der beauftragten Detekteien nachweisbar waren.

In Hessen ist eine Vertriebsgesellschaft ansässig, gegen die ein Bußgeld wegen Verstoßes gegen die Pflicht, einen betrieblichen Datenschutzbeauftragten zu bestellen, in Höhe von 10.000 € verhängt wurde. Weitere Bußgelder wurden nicht erhoben, denn bei der hessischen Vertriebsgesellschaft waren, ebenso wie bei einigen Gesellschaften in anderen Bundesländern, sämtliche Einsatzberichte von Detekteien bzw. Sicherheitsunternehmen bei Beginn der datenschutzrechtlichen Überprüfung bereits vernichtet. Es konnte somit nicht mehr festgestellt werden, ob im Rahmen der Detektivüberwachung Berichte mit unzulässigen Inhalten angefertigt und von der Vertriebsgesellschaft entgegengenommen, gelesen und aufbewahrt wurden.

Wie weiteren Medienberichten zu entnehmen war, konnten derartige Praktiken der Mitarbeiterüberwachung nicht nur in diesem einen Unternehmen beobachtet werden. Vielmehr scheinen sie in der Lebensmittelbranche teilweise an der Tagesordnung zu sein. Die Datenschutzaufsichtsbehörden haben daher vereinbart, auch die anderen in ihrem jeweiligen Zuständigkeitsbereich ansässigen Lebensmittelhändler - insbesondere die in den Presseartikeln genannten - einer Überprüfung zu unterziehen.

Zwei große Lebensmittelunternehmen haben in Hessen ihren Sitz. Gegen beide hat die Aufsichtsbehörde ein datenschutzrechtliches Überprüfungsverfahren eingeleitet. Während die Überprüfung bei einem Unternehmen noch andauert, konnte das Verfahren gegen das andere Unternehmen eingestellt werden. In diesem Fall wurde kein Verstoß festgestellt. Das Unternehmen hatte zwar ebenfalls eine Detektei zur Aufdeckung von Ladendiebstählen und Inventurverlusten beauftragt, die Geschäftsbeziehung nach einer Testphase jedoch beendet, da die Vorgehensweise der Detektive und deren Einsatzberichte, die Informationen über die Mitarbeiter enthielten, nicht dem Auftrag entsprachen.

12.2 Videoüberwachung am Arbeitsplatz

In Folge der Medienberichte, die sich mit der Mitarbeiterüberwachung - u.a. mittels Einsatz von Videokameras - in Lebensmittelmärkten befassten, wurden auch aus anderen Branchen eine Reihe von Anfragen und Beschwerden über Videobeobachtung am Arbeitsplatz an die Aufsichtsbehörde herangetragen.

In einem Metall verarbeitenden Betrieb wurde beispielsweise das Betriebsgelände und die Werkshallen durch Videokameras überwacht. Die Notwendigkeit der Maßnahme wurde seitens der Betriebsleitung damit begründet, dass es in der Vergangenheit Diebstähle in großem Ausmaß, Manipulationen bei der Stückaufschreibung etc. gegeben habe. Diebstähle hätte man wegen nicht ausreichender Beweise gegen bestimmte Personen bisher nicht zur Anzeige gebracht. Von der Videoüberwachung verspreche man sich sowohl eine abschreckende Wirkung als auch eine Handhabe zur Beweisführung bei weiteren Vorkommnissen.

Aus datenschutzrechtlicher Sicht wurde zwar grundsätzlich das berechtigte Interesse der Firmenleitung an der Videobeobachtung anerkannt, allerdings nicht in dem vorhandenen Ausmaß. Soweit sich im Blickfeld der Kameras keine Arbeitsplätze befanden und Mitarbeiter nur dann aufgenommen wurden, wenn sie die Hallen, die Flure etc., auf die die Kameras gerichtet waren, durchquerten oder sich dort kurzfristig aufhielten, bestanden gegen die Videoüberwachung keine Bedenken.

Wie die Vertreter der Aufsichtsbehörde allerdings anlässlich einer Begehung des Betriebsgeländes feststellen konnten, waren drei Kameras direkt auf Arbeitsplätze gerichtet, sodass die dort beschäftigten Arbeitnehmer permanent von der jeweiligen Kamera erfasst wurden. Ein berechtigtes Interesse an der Beobachtung dieser Arbeitsplätze, zum Beispiel wegen eines konkreten Diebstahlverdachts gegen die dort tätigen Mitarbeiter, wurde seitens des Arbeitgebers nicht geltend gemacht, damit war die Erforderlichkeit dieser Maßnahme auszuschließen. Vielmehr überwogen hier die schutzwürdigen Interessen der betroffenen Beschäftigten. Auch wenn sich diese Mitarbeiter nicht ständig an ihrem Arbeitsplatz aufhielten, war die Videobeobachtung in diesen Fällen doch als eine ständige und damit unzulässige Überwachungsmaßnahme zu bewerten. Eine solche dauerhafte Kontrolle erzeugt bei Arbeitnehmern einen Überwachungsdruck, der mit dem grundgesetzlich garantierten Schutz ihrer Persönlichkeitsrechte nicht zu vereinbaren ist. Die Betriebsleitung wurde aufgefordert, diese Kameras entweder zu entfernen oder so auszurichten, dass Arbeitsplätze von ihnen nicht mehr erfasst werden. Der Aufforderung wurde Folge geleistet.

12.3 Weitergabe von Personaldaten im Rahmen einer geplanten teilweisen Betriebsveräußerung

In einem international tätigen Transportunternehmen sollte wegen einer geschäftlichen Neuausrichtung die Schließung mehrerer Niederlassungen und möglichst deren Veräußerung erfolgen. Im Rahmen einer sogenannten "Due-Dilligence-Prüfung" wurde den potentiellen Kaufinteressenten Einblick in die Firmenunterlagen gewährt. Diese Unterlagen wurden in einem eigens zu diesem Zweck eingerichteten Datenraum bereitgestellt.

Die Kaufinteressenten konnten nicht nur die Finanzdaten der zum Verkauf stehenden Niederlassungen einsehen, sondern auch sämtliche Personaldaten aller betroffenen Mitarbeiter der jeweiligen Niederlassung. Es wurde nämlich versäumt, den Kaufinteressenten die Mitarbeiterdaten nur in anonymisierter Form zur Einsichtnahme zur Verfügung zu stellen.

Der Datenschutzbeauftragte wurde in das Projekt nicht einbezogen und war über den Umfang der zur Einsichtnahme bereit gestellten Mitarbeiterdaten nicht informiert.

Mit der Veräußerung der Niederlassungen nach Abschluss des Due-Dilligence-Verfahrens wurden den Käufern alle Personaldaten übermittelt, ohne das Ende der den Mitarbeitern nach § 613a BGB zustehenden Widerspruchsfrist abzuwarten.

Da die Übermittlung von Arbeitnehmerdaten im Vorfeld von Unternehmensveräußerungen im Rahmen der Due-Dilligence-Prüfung nicht der Zweckbestimmung der mit den Mitarbeitern bestehenden Vertragsbeziehungen zugeordnet werden kann, muss der Betriebsinhaber für die Übermittlung der Daten diesbezügliche "berechtigte Interessen" (§ 28 Abs. 1 Nr. 2 BDSG) geltend machen. Diese sind in der Regel dann anzuerkennen, wenn sich ohne eine Weitergabe der Daten eine Veräußerung des Betriebs nicht realisieren ließe. Abzuwägen ist dieses Interesse des Arbeitgebers mit den

entgegenstehenden Interessen der Mitarbeiter daran, dass keine Offenlegung ihrer Daten gegenüber Dritten erfolgt.

Beispielsweise wird ein Unternehmen kaum zu veräußern sein, ohne dass der potentielle Erwerber Informationen über das leitende Management und ggf. besonders relevante Experten des Unternehmens erhält. In diesen Fällen können dem potentiellen Erwerber die ihn interessierenden Informationen gegeben werden. Dagegen sollen Angaben über die sonstigen Mitarbeiter keine Rückschlüsse auf bestimmte Personen zulassen und sind daher aggregiert oder in anonymisierter Form zu übermitteln. Die Mitteilung anonymisierter und aggregierter Daten werden den Informationsinteressen des potentiellen Erwerbers in der Regel in ausreichender Maße gerecht.

Mit der Veräußerung eines Betriebs oder Betriebsteils kommt es zum gesetzlichen Arbeitgeberwechsel. Nach § 613a Abs. 5 BGB sind die Arbeitnehmer über den Betriebsübergang und die sich daraus ergebenden rechtlichen, wirtschaftlichen und sozialen Folgen sowie die insoweit beabsichtigten Maßnahmen zu informieren. Die Arbeitnehmer können dann innerhalb eines Monats dem Übergang ihres Arbeitsverhältnisses widersprechen (§ 613a Abs. 6 BGB). Eine Übermittlung der Arbeitnehmerdaten darf erst dann erfolgen, wenn der Arbeitnehmer der Fortsetzung des Arbeitsverhältnisses mit dem neuen Arbeitgeber nicht innerhalb der gesetzten Frist widersprochen hat.

Das Unternehmen hat in zweifacher Hinsicht in unzulässiger Weise personenbezogene Daten übermittelt, nämlich mit der den Kaufinteressenten gewährten Einsichtnahme in Personaldaten aller betroffenen Arbeitnehmer sowie mit der vorzeitigen Übermittlung der Mitarbeiterdaten an die Käufer der Niederlassungen vor Ablauf der Widerspruchsfrist. Von der Festsetzung einer Geldbuße wurde in Anbetracht der Tatsache, dass der für die unzulässige Datenübermittlung verantwortliche Geschäftsführer zum Zeitpunkt der Prüfung bereits nicht mehr in dem Unternehmen beschäftigt war, abgesehen. Die festgestellten datenschutzrechtlichen Verstöße wurden aber von der Aufsichtsbehörde ausdrücklich beanstandet. Gegenüber der neuen Geschäftsführung wurde die Erwartung ausgesprochen, dass sich derartige Verstöße nicht wiederholen werden.

12.4 Datendiebstahl bei einer Jobvermittlung

Eine international tätige Online-Jobvermittlung setzte die Aufsichtsbehörde darüber in Kenntnis, dass bei einem Angriff auf ihre Datenbank sowohl Informationen über Kunden (Arbeitgeber) als auch über Arbeitsuchende kopiert wurden. Betroffen waren u. a. bestimmte Kontakt- und Benutzerkontodaten einschließlich Nutzer-IDs und Passwörter, Namen, E-Mail-Adressen, Telefonnummern etc., aber keine Lebensläufe der Bewerber.

Es war bereits das zweite Mal innerhalb von zwei Jahren, dass das Unternehmen Ziel eines illegalen Zugriffs auf seine Datenbank wurde. Das Unternehmen ging davon aus, dass die gestohlenen Daten für Betrugsversuche im Rahmen von "Phishing" oder "Spoofing" genutzt werden sollten.

Das Unternehmen reagierte auf den Datenangriff umgehend mit einer breit angelegten Informationskampagne. Auf seinen Internetseiten wurde ein Sicherheitshinweis geschaltet, um Kunden und Bewerber zu warnen und dem Missbrauch der gestohlenen Daten vorzubeugen. Die Betroffenen wurden - zunächst mit einem Online-Brief, später beim Einloggen in ihren Account durch das System - aufgefordert, ihre Passwörter zu ändern.
Anders als bei dem ersten Datendiebstahl hatte sich das Unternehmen diesmal gegen eine direkte Benachrichtigung seiner Nutzer per E-Mail entschieden, um die Möglichkeit, dass diese abgefangen und als "Phishing-E-Mails" verwendet werden, von vornherein auszuschließen.

Das Unternehmen arbeitet zur Aufklärung des Vorfalls mit den Strafverfolgungsbehörden zusammen. Die Ermittlungen sind noch nicht abgeschlossen.

Die Aufsichtsbehörde begrüßt die offensive Informationspolitik des Unternehmens. Was das Unternehmen hier freiwillig getan hat, soll nach dem Gesetzentwurf der Bundesregierung (vgl. Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften vom 2. Januar 2009, Bundesrats-Drucks. 4/09) künftig vorgeschrieben werden, soweit besonders sensible personenbezogene Daten be-

troffen sind, nämlich die Benachrichtigung der Aufsichtsbehörde und der Betroffenen.

12.5 Hacker-Angriff auf Bewerber-Datenbank

Von der Redaktion eines Fernseh-Wirtschaftsmagazins erhielt ein in Hessen ansässiges Wirtschaftsprüfungs- und Beratungsunternehmen Hinweise über einen Hacker-Angriff auf eine Servicedatenbank für Arbeitsuchende und einen damit verbundenen Datendiebstahl in großem Umfang. Diese bei einem externen Serviceprovider (Auftragsdatenverarbeiter) betriebene Datenbank diente interessierten Nutzern zur vereinfachten Erstellung ihrer Bewerbung bei dem Unternehmen. Das Unternehmen erstattete aufgrund des Hinweises umgehend Strafanzeige gegen Unbekannt. Auch die Aufsichtsbehörde für den Datenschutz wurde über die Vorfälle informiert.

Nach Recherchen des Wirtschaftsmagazins wurden die Daten, bestehend aus E-Mail-Adressen und Passwörtern, auf einem Internetserver in der Volksrepublik China veröffentlicht. Vor Ausstrahlung der Sendung informierte die Redaktion die potenziell Geschädigten über den Sachverhalt und empfahl ihnen, ihre Zugangsdaten umgehend zu ändern.

Die Datendiebe spekulierten anscheinend darauf, dass zahlreiche Internet-Nutzer bei verschiedenen Diensten die gleiche Kombination aus E-Mail-Adresse und Passwort verwenden. In solchen Fällen wäre eine unabsehbare Weiternutzung der Daten möglich. Hier zeigt sich wieder einmal, wie wichtig die Verwendung unterschiedlicher Passwörter bei der Nutzung verschiedener Online-Dienste ist.

Ein direkter Zugriff auf die Bewerberdaten bei dem Unternehmen selbst war mit den im Netz befindlichen Informationen nicht möglich, da man sich dort nur mit Hilfe von Benutzernamen anmelden konnte, die sich nicht bei den gestohlenen Daten befanden.

Gemeinsam mit der Polizei leitete die Aufsichtsbehörde Überprüfungen bei dem Unternehmen sowie dem Dienstleister ein. Die Bewerberdatenbank wurde umgehend vom Netz genommen und war von außen nicht mehr zugänglich. Eine Löschung der Daten erfolgte, nachdem der Stand der Ermittlungen dies zuließ und soweit dies mit den Belangen der Betroffenen vereinbar war. All dies geschah in Abstimmung mit den Strafermittlungsbehörden und der Aufsichtsbehörde. Die Betroffenen wurden von dem Unternehmen entsprechend benachrichtigt.

Einige Betroffene behaupteten, das Unternehmen sei aufgrund unzureichender Datensicherheitsmaßnehmen für den Datendiebstahl mitverantwortlich und erstatteten Strafanzeige gegen das Unternehmen. Ferner richteten sie entsprechende Beschwerden an die Aufsichtsbehörde.

Die Ermittlungen der Strafverfolgungsbehörden haben Vorrang. Diese baten die Aufsichtsbehörde daher, von weiteren eigenen Ermittlungen abzusehen. Bei Redaktionsschluss lag noch keine Mitteilung über den Abschluss der strafrechtlichen Ermittlungen vor.

13. Videoüberwachung und Web-Cams

13.1 Übertragung von Videobildern aus einer Bäckerei mittels Web-Cam ins Internet

Anlässlich des 125-jährigen Firmenjubiläums hat eine Bäckerei ihren Internetauftritt neu gestalten lassen und ist dabei der Anregung des Webdesigners gefolgt, eine Web-Cam im Laden zu installieren. Damit sollte den Kunden das Angebot gemacht werden, online einen Blick in das Ladengeschäft zu werfen, um sehen zu können, was genau in diesem Moment im Laden passiert.

Auf den telefonischen Hinweis einer Kundin hin und der damit verbundenen Frage, ob dies denn zulässig sei, prüfte die Aufsichtsbehörde den Fall und stellte fest, dass über die Web-Cam im Internet fast die gesamte Ladentheke mit den entsprechenden Waren, den Verkäuferinnen und den davorstehenden Kunden zu sehen war. Die Personen - Mitarbeiter sowie Kunden - waren

eindeutig identifizierbar. Ein Schild, das auf die Web-Cam hinweist, war nicht angebracht.

Web-Cams, die Bilder ins Internet übertragen, sind datenschutzrechtlich nur dann unbedenklich, wenn eine Identifizierbarkeit der abgebildeten Personen ausgeschlossen ist oder die Einwilligung der Betroffenen vorliegt. Da im vorliegenden Fall alle Personen erkennbar waren, hätten von allen Betroffenen Einwilligungen zu der Veröffentlichung im Internet vorliegen müssen. Dies ergibt sich aus der gebotenen Abwägung nach § 6b Abs. 1 Nr. 3 BDSG und im Hinblick auf § 22 Kunsturhebergesetz (Recht am eigenen Bild), wonach Bildnisse in der Regel nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden dürfen. Dabei gibt es nur eng begrenzte Ausnahmen, die im § 23 dieses Gesetzes geregelt sind. Diese Ausnahmen sind hier nicht einschlägig.

Nachdem die Aufsichtsbehörde den Geschäftsinhaber über die Rechtslage informiert und sein Vorgehen als datenschutzrechtlichen Verstoß beanstandet hatte, war dieser sofort bereit, die Übertragung der Bilder aus seinem Ladengeschäft ins Internet abzustellen und die Web-Cam in angemessener Frist abzubauen.

Etwas irritiert zeigte sich der Unternehmer, dass der Webdesigner ihm bei der Gestaltung der Homepage die Web-Cam vorgeschlagen hatte, ohne offenbar über die rechtliche Zulässigkeit informiert gewesen zu sein. Hier scheinen auch Fachfirmen die datenschutzrechtlichen Voraussetzungen nicht genau zu kennen oder diese aus vordergründigen Geschäftsinteressen zu ignorieren.

13.2 Videobeobachtung im Dusch- und Saunabereich einer ausschließlich von Männern besuchten Sauna

Ein Beschwerdeführer wies darauf hin, dass er sich erheblich in seinem Persönlichkeitsrecht beeinträchtigt sehe, wenn in einer "Gay-Sauna" im Duschbereich gefilmt werde, und bat um Klärung, ob Videobeobachtung in diesem Bereich zulässig ist.

Auf Nachfrage der Aufsichtsbehörde begründete der Betreiber der "Gay-Sauna" die Videobeobachtung im Sauna- und Duschbereich damit, dass diese der Kontrolle diene und zwar zum einen, ob alle Türen (Sauna/Dampfband) geschlossen seien und zum anderen, ob die Duschen nach Benutzung abgestellt werden (Energieeinsparung). Darüber hinaus soll Unfällen vorgebeugt werden und ein schnelles Eingreifen bei Übelkeit und Stürzen der älteren Besucher sichergestellt werden. Im Übrigen würden keine Bilddaten gespeichert, sondern lediglich in Echtzeit übertragen, es erfolge also reines Monitoring. Der videobeobachtete Bereich sei durch Piktogramme entsprechend gekennzeichnet.

Die Aufsichtsbehörde stellte fest, dass im vorliegenden Fall die Videobeobachtung des öffentlich zugänglichen Raums mit optisch-elektronischen Einrichtungen nach § 6b Abs. 1 Nr. 2 und 3 BDSG nicht erforderlich ist und darüber hinaus die schutzwürdigen Interessen der Betroffenen in jedem Fall überwiegen.

Die Begründungen hinsichtlich der Erforderlichkeit der Videoüberwachung durch den Betreiber sind nicht überzeugend. Das Schließen der Saunatüren muss nicht per Video überwacht werden, da in der Regel die Besucher einer Sauna oder des Dampfbads selbst ein starkes Interesse daran haben, dass die Saunatüren beim Hinein- und Hinausgehen sofort wieder geschlossen werden. Eine Kontrolle erfolgt insoweit bereits durch die übrigen Gäste, die dafür sorgen, dass "Fehlverhalten" - wie das offen stehen lassen der Tür - unterbleibt. Um Energie zu sparen, kann die Wasserzufuhr zu den Duschen über eine Zeitschaltuhr laufen, sodass die Laufzeit einer Dusche immer auf einen kurzen Zeitraum beschränkt ist und bei längerem Duschbedarf immer wieder neu eingeschaltet werden muss.

In den seltensten Fällen wird sich in der Sauna nur ein Besucher aufhalten, dem bei gesundheitlichen Problemen nur Hilfe geleistet werden kann, weil man über eine Videoanlage beobachtet. Zum überwiegenden Teil der Öffnungszeiten halten sich sicher mehrere Besucher in der Sauna auf, die not-

falls Hilfe holen oder leisten können. Außerdem könnten auch über ein zu installierendes "Notfallklingelsystem" Hilfeleistungen angefordert werden.

Daher beanstandete die Aufsichtsbehörde die Videobeobachtung. Der Saunabetreiber baute daraufhin die Videokamera umgehend ab.

14. Gesundheit

14.1 Arztgeheimnis und Datenschutz in ärztlichen Kooperationsformen, insbesondere in medizinischen Versorgungszentren und Bereitschaftsdienstzentralen

14.1.1 Die Bedeutung des § 203 Strafgesetzbuch (StGB) und das Verhältnis zum Datenschutzrecht

Die Patientendaten in einer Arztpraxis unterliegen als besondere Arten personenbezogener Daten nach § 3 Abs. 9 BDSG einem erhöhten Schutz nach den Vorschriften des BDSG. Darüber hinaus unterliegen sie dem besonderen Schutz des § 203 StGB, also der ärztlichen Schweigepflicht. Die ärztliche Schweigepflicht gilt dabei auch für Ärzte untereinander, also prinzipiell auch innerhalb eines medizinischen Versorgungszentrums oder einer Bereitschaftsdienstzentrale.

14.1.2 Gemeinschaftspraxen und Praxisgemeinschaften

Gemeinschaftspraxen und Praxisgemeinschaften sind rechtlich unterschiedliche ärztliche Kooperationsformen.

Bei einer Praxisgemeinschaft teilen sich die beteiligten Ärzte nur die Räumlichkeiten und die Einrichtung der Praxis. Sie bilden jedoch keine Abrechnungsgemeinschaft. Der Behandlungsvertrag wird jeweils zwischen dem Patienten und dem einzelnen Arzt geschlossen. Es handelt sich also praktisch um mehrere rechtlich selbständige Arztpraxen, die in gemeinsamen Räumlichkeiten betrieben werden. Jeder Arzt hat somit einen eigenen Patientenstamm, auf den der andere keinen Zugriff hat und haben darf.

Bei einer Gemeinschaftspraxis handelt es sich um einen wirtschaftlichen und organisatorischen Zusammenschluss zweier oder mehrerer Ärzte, der inzwischen auch ortsübergreifend (überörtliche Gemeinschaftspraxis) möglich ist. Im Gegensatz zur Praxisgemeinschaft werden also nicht notwendigerweise gemeinsamen Räumlichkeiten genutzt. Wesentlicher Unterschied zur Praxisgemeinschaft ist, dass der Patient grundsätzlich mit allen Ärzten gemeinschaftlich einen Behandlungsvertrag schließt. Meist haben die Ärzte daher einen gemeinsamen Patientenstamm, der, sofern sie zuvor in Einzelpraxen tätig waren, durch eine Zusammenführung der beiden Patientenstämme der Einzelpraxen gebildet worden sein kann. Dabei ist in einer Gemeinschaftspraxis darauf zu achten, dass der Arzt auf die Behandlungsdaten eines Praxiskollegen aus der Zeit vor Gründung der Gemeinschaftspraxis nur im Einverständnis mit dem jeweiligen Patienten zugreifen darf. Auch der gegenseitige Zugriff auf die aktuellen Patientendaten bedarf jedoch einer Rechtfertigung. Diese kann sich aus einer mutmaßlichen Einwilligung der Patienten ergeben. Je nach Art und Größe der Gemeinschaftspraxis kann es Zweifelsfragen geben. Da die grundsätzlichen Rechtsfragen die gleichen sind wie bei den Medizinischen Versorgungszentren (MVZ) wird auf die folgenden Ausführungen verwiesen.

14.1.3 Vertiefte Betrachtung der Medizinischen Versorgungszentren (MVZ)

14.1.3.1 Was ist ein MVZ?

Seit dem 1. Januar 2004 können Ärzte auch in einer fachübergreifenden, ärztlich geleiteten Einrichtung in Form eines medizinischen Versorgungszentrums (MVZ) tätig werden. Die Rechtsgrundlage hierzu bildet § 95 Sozialgesetzbuch 5. Buch (SGB V). Ärzte können dort entweder als Inhaber oder als Angestellte tätig sein. Gesellschafter eines MVZ können nur zugelassene Leistungserbringer nach dem SGB V sein, was auch Krankenhäuser und Heilmittelerbringer einschließt. In einem MVZ arbeiten Ärzte, welche in der Regel unterschiedlichen Fachrichtungen angehören, mit dem Ziel einer umfassenden Patientenversorgung "unter einem Dach" zusammen. Der Behand-

lungsvertrag wird immer mit dem MVZ und nicht mit dem einzelnen Arzt abgeschlossen. Für die Patienten ist das MVZ grundsätzlich mit einer Gemeinschaftspraxis vergleichbar.

Es gibt zum Teil sehr kleine MVZ, mitunter aber auch solche mit einer Vielzahl von Ärzten, sogar mit über einhundert Ärzten. Zum Teil sind die MVZ an eine Klinik angebunden. Das Ziel dieser Zusammenarbeit ist eine umfassende Versorgung des Patienten. Der Zahl der MVZ im Bundesgebiet ist in den letzten Jahren stark ansteigend.

14.1.3.2 Überprüfung von MVZ in Hessen

Um festzustellen, wie die MVZ in Hessen arbeiten, und wie insbesondere der Zugriff auf die Patientendaten geregelt ist, wurden zusammen mit dem Hessischen Datenschutzbeauftragten (HDSB) im Jahr 2008 verschiedene MVZ überprüft. Die gemeinsame Überprüfung wurde vorgenommen, da für den öffentlich rechtlichen Bereich die Zuständigkeit des HDSB gegeben ist und sich die MVZ zum Teil in öffentlicher Trägerschaft und/oder in Kooperation und Datenaustausch mit öffentlichen Krankenhäusern befinden. Es wird auf die Ausführungen unter Ziffer 4.7.4 des 37. Tätigkeitsberichts des Hessischen Datenschutzbeauftragten - Drs. 18/106 - verwiesen.

14.1.3.2.1 Datenübermittlungen zwischen MVZ und Kliniken

Bei den Prüfungen wurden zwei unterschiedliche Konstellationen vorgefunden. Teilweise handelte das MVZ autonom, wie eine übliche Arztpraxis. Es war also klar zwischen Klinik und MVZ unterschieden worden; die Übermittlung der Patientendaten erfolgte im Einzelfall im jeweils erforderlichen Umfang, soweit dies für die Mitbehandlung durch die andere Stelle erforderlich war.

Teilweise kooperierte das MVZ so eng mit der Klinik, dass eine pauschale Übermittlung der Daten von Patienten des MVZ an das Klinikum erfolgte, auch von Personen, die nicht im Klinikum mitbehandelt wurden. Auch umgekehrt bestand die Möglichkeit der Kenntnisnahme der Daten von Patienten des Klinikums, ohne dass diese auch im MVZ behandelt wurden.

Da es sich bei Klinik und MVZ um zwei rechtlich selbständige Stellen handelt, bedürfen Datenübermittlungen zwischen den beiden Stellen einer Rechtsgrundlage. In der Regel kommt als Rechtsgrundlage hierfür nur die Einwilligung der Patienten in Betracht. Soweit Daten übermittelt wurden, die zur Mitbehandlung durch die andere Stelle nicht erforderlich waren, also bei der zweitgenannten Konstellation, war teilweise zuvor eine Einwilligung der Patienten eingeholt worden. Der Wortlaut der Einwilligungserklärung bezog sich jedoch auf die Behandlungsdaten, die zur weiteren Mitbehandlung erforderlich sind, und konnte daher keine Rechtsgrundlage sein für die Übermittlung der Daten von Personen, die gar nicht Patienten der anderen Stelle waren. Im Übrigen bestehen Bedenken gegen eine pauschale Einwilligungserklärung bezüglich aller künftigen Behandlungsfälle. Eine solche Einwilligung kann nicht als informierte Einwilligung im Sinn von § 4a Abs. 1 und 3 BDSG sowie § 12 Hessisches Krankenhausgesetz (HKHG) i. V. m. § 7 Abs. 2 Hessisches Datenschutzgesetz (HDSG) bewertet werden. Als nicht zulässig wurde es auch angesehen, dass eine pauschale Einwilligung in die Übermittlung nicht erforderlicher Daten als Voraussetzung einer Behandlung im MVZ - außer in Notfällen - angesehen wurde.

Bei der erstgenannten Konstellation war insoweit kein Problem ersichtlich, denn bei einer Vor- und Nachbehandlung des Patienten wird das Vorliegen dessen mutmaßlichen Einverständnisses in die Datenübermittlung regelmäßig anzunehmen sein, wenn sich der Patient tatsächlich in die Weiterbehandlung begibt.

Eine schriftliche Einwilligung ist für die Übersendung des Befundes an Mitbehandler in der Regel nicht zwingend erforderlich. Allerdings kann es von Vorteil sein, wenn die vorgesehenen Datenübermittlungen auf diese Weise klar vereinbart werden. Wie bereits ausgeführt, muss sich die Einwilligung jedoch auf den konkreten Behandlungsfall beziehen.

14.1.3.2.2 Zugriffsausgestaltung innerhalb der MVZ

Bei den überprüften MVZ wurden hinsichtlich der Zugriffsberechtigungen nur teilweise verschiedene Rollen, wie zum Beispiel Administrator, Arzt, Arztgehilfin etc., unterschieden. Die Ärzte hatten gemeinsame Zugriffsmöglichkeiten auf alle Patientendaten. Bei einem MVZ waren lediglich die Behandlungsdaten der dort tätigen Psychologin nicht im Computersystem gespeichert, sondern existierten nur in Papierform und wurden ausschließlich in verschlossenen Behältern im Behandlungszimmer der Psychologin aufbewahrt.

Der gemeinsame Zugriff auf Patientendaten ist bei MVZ trotz des Abschlusses des Behandlungsvertrags mit dem MVZ selbst und nicht mit dem einzelnen Arzt kritisch zu sehen. Es ist nicht nachvollziehbar, zu welchem Zweck zum Beispiel ein Orthopäde die gesamten Behandlungsdaten eines Augenarztes einsehen können sollte. Je höher die Anzahl der Ärzte und Fachrichtungen in einem MVZ ist, desto wichtiger ist die Frage der Differenzierung der Zugriffsrechte.

In den überprüften MVZ wird teilweise von den Patienten eine Einwilligung in die Kenntnisnahme ihrer Daten durch alle Ärzte des MVZ eingeholt. Eine Behandlung wird dann in der Regel - außer in Notfällen - abgelehnt, wenn der Patient die Einwilligungserklärung nicht unterschreibt. Offensichtlich wird hier zumindest erkannt, dass ein Zugriff aller Ärztinnen und Ärzte keineswegs selbstverständlich ist. Das Einholen einer Einwilligung in nicht erforderliche Zugriffsmöglichkeiten ist jedoch nicht im Interesse des Patienten und zudem rechtlich problematisch. Zum Teil waren die Einwilligungen so formuliert, dass sie sich nur auf Zugriffe bezogen, die für die Behandlung erforderlich sind. Hier kann bei den Patienten der irrtümliche Eindruck entstehen, dass der Zugriff auch entsprechend technisch begrenzt ist, was jedoch tatsächlich nicht der Fall ist.

Die "Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung" der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (www.bundesärztekammer.de) sehen vor, dass jeder Benutzer nur Zugriff auf die seinem Tätigkeitsfeld entsprechenden Datenbestände und Programme hat. Es ist laut dieser Empfehlung zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems berechtigten Personen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Zu diesem Zweck sollten die berechtigten Personen über Zugriffskontrollmechanismen, zum Beispiel persönliche Passwörter, legitimiert werden. Diese Empfehlungen finden zwar auf MVZ nicht unmittelbar Anwendung, gleichwohl sind Maßnahmen zum Zugriffsschutz auch bei MVZ von Bedeutung.

Insgesamt vertritt die Aufsichtsbehörde in Übereinstimmung mit dem Hessischen Datenschutzbeauftragten folgende Auffassung:

Die ärztliche Schweigepflicht und die Vorgaben des BDSG bzw. des HDSG zu den technischen Datensicherheitsmaßnahmen finden auch innerhalb von Kooperationspraxen und MVZ Anwendung. Die Vorstellung bzw. Erwartung eines Patienten, der sich in eine Kooperationspraxis oder in ein MVZ begibt, ist sicherlich unterschiedlich. In jedem Fall wird es auch Patienten geben, die gezielt zu einem Arzt in Behandlung gehen und - gerade auch in großen Kooperationspraxen bzw. MVZ und/oder bei bestimmten Erkrankungen erwarten, dass nicht alle Ärzte ihre persönlichen medizinischen Daten zur Kenntnis nehmen können. Wenn in bestimmten Konstellationen von einer mutmaßlichen Einwilligung des Patienten in die Datenweitergabe innerhalb der Kooperationspraxis oder des MVZ ausgegangen wird, muss dem Patienten zumindest ein Widerspruchsrecht gegen eine allgemeine Kenntnisnahme seiner Daten innerhalb der Kooperationspraxis bzw. des MVZ eingeräumt werden. Jedenfalls bei großen Kooperationspraxen und MVZ bestehen aber erhebliche Zweifel, ob hier noch von einer mutmaßlichen Einwilligung des Patienten in eine allgemeine Kenntnisnahme der Daten durch alle Ärzte ausgegangen werden kann.
Zwingend erforderlich ist mehr Transparenz für den Patienten, welche Stelle seine Daten verarbeitet, zum Beispiel Klinik oder MVZ, und in welchem Umfang und für welchen Zweck seine Daten innerhalb der Kooperationspraxis oder dem MVZ anderen Ärzten, die ihm nicht als Behandler bekannt sind, zur Kenntnis gelangen können.

Wie für jede andere Daten verarbeitende Stelle auch, besteht für Kooperationspraxen und MVZ die Notwendigkeit der Differenzierung nach Rollen und Umfang der Zugriffsberechtigung (Ärzte, Arztgehilfe, Aufnahme, Administrator etc.). Dies ergibt sich bereits aus § 9 BDSG bzw. § 10 HDSG und ist ein wesentlicher Bestandteil der Revisionsfähigkeit der Datenverarbeitung. Als solche sind diese Maßnahmen auch unter Haftungsaspekten unerlässlich.
Für die Umsetzung der o.a. Anforderungen (Revisionssicherheit, Widerspruchsrecht des Patienten) kommen grundsätzlich verschiedene technische Maßnahmen in Betracht. Unstreitig müssen ändernde Zugriffe nachvollziehbar sein. Soweit es sich um Zugriffe handelt, bei denen in Papierdokumenten eine Unterschrift des Arztes zwingend erforderlich ist, kann diese nur durch eine qualifizierte elektronische Signatur ersetzt werden; dies muss beachtet werden, wenn elektronische Dokumente die rechtlich verbindliche Behandlungsdokumentation darstellen.

Wenn der Widerspruch eines Patienten gegen eine Einsichtnahme bestimmter Ärzte in seine Patientendaten technisch zwingend umgesetzt werden soll, dürfen diese Ärzte nicht auf die Daten zugreifen können. Die Möglichkeit eines allgemeinen lesenden Zugriffs durch diese Ärzte wäre in diesem Fall nicht akzeptabel. Wenn demgegenüber der Widerspruch eines Patienten gegen eine Einsichtnahme nur durch Protokollierung lesender Zugriffe, Durchsicht der Protokolle und bei Bedarf Aufklärung des Sachverhalts soweit wie möglich gewährleistet werden soll, können Ärzte technisch auf die Daten dieses Patienten zugreifen und ein unberechtigter Zugriff kann nur durch nachträgliche Kontrollen festgestellt und evtl. sanktioniert werden.

Zur zweiten Alternative ist noch folgendes anzumerken: Generell gilt, dass Protokolle auch bezüglich auffälliger Ereignisse kontrolliert werden müssen. Um die Protokolle überschaubar zu halten, könnte darauf verzichtet werden, lesende Zugriffe durch die den Patienten behandelnden Ärzte aufzuzeichnen. Sobald ein nicht als Behandler geführter Arzt zugreift, wäre ein lesender Zugriff zu protokollieren.

Im Rahmen der Prüfungen wurde seitens der MVZ vorgetragen, dass die bei den MVZ eingesetzte Praxissoftware entsprechende praktikable, datenschutzgerechte Lösungen nicht unterstütze oder überhaupt nicht ermögliche. Diese Software sei von der Kassenärztlichen Bundesvereinigung zertifiziert, aber nur im Hinblick auf die Abrechnungsschnittstelle zur Kassenärztlichen Vereinigung (KV). Da die Ausgestaltung der Software den rechtlichen Anforderungen folgen muss und nicht umgekehrt, muss die datenschutzrechtliche Problematik vor Anschaffung einer Software bedacht werden.

14.1.4 Bereitschaftsdienstzentralen

Aufgrund einer Beratungsanfrage der KV Hessen wurde eine ärztliche Bereitschaftsdienstzentrale (BDZ) näher betrachtet. Ziel war die exemplarische Prüfung der Fragen des Zugriffschutzes etc.

Die KV Hessen ist Trägerin der Bereitschaftsdienstzentrale. Die Ärzte bilden eine Gesellschaft bürgerlichen Rechts. Hinsichtlich der Abrechnung mit der KV ist die Zentrale mit einer Praxisgemeinschaft vergleichbar, da jeder Arzt einzeln abrechnet. Von der inneren Organisation her ist die Bereitschaftsdienstzentrale laut KV aber eher mit einer Gemeinschaftspraxis zu vergleichen (vgl. Ziffer 14.1.2 dieses Berichts).

Datenschutzrechtlich besonders problematisch bei diesen Zentralen kann es sein, wenn zum Beispiel eine Apotheke oder eine physiotherapeutische Praxis der BDZ angeschlossen ist. Dies war jedoch bei der aufgesuchten Zentrale nicht der Fall. Bei dieser sind ca. 60 Ärzte der unterschiedlichen Fachrichtungen tätig, wobei diese in der Regel noch in ihrer eigenen Praxis arbeiten und oft auch noch in anderen Notdienstzentralen beschäftigt sind.

Jeder Arzt kann alle Patientendaten im Datenverarbeitungssystem sehen. Es ist nur ein gemeinsames Passwort vergeben und es erfolgt keine Protokollierung. Grundsätzlich bestehen somit die gleichen Probleme wie oben dargestellt. Allerdings wurde nachvollziehbar dargelegt, dass aufgrund der besonderen Arbeitsbedingungen technische Zugriffsdifferenzierungen nicht angemessen und realisierbar erscheinen. Eine Information der Patienten vor der Behandlung ist jedoch erforderlich. Ein entsprechendes Hinweisschild am

Eingangsbereich war vorhanden, eine Präzisierung der Information wird noch abzustimmen sein.

Gerade bei den BDZ wurde auch verständlich, dass möglichst einfach handhabbare technische Lösungen erforderlich sind. Auch hier wurde auf Defizite der vorhanden KV-zertifizierten Software verwiesen.

14.1.5. Weiteres Vorgehen

Zur weiteren Konkretisierung der künftigen Verfahrensweisen sind gemeinsame Besprechungen mit der Landesärztekammer und der KV vorgesehen. Die KV Hessen hatte der Aufsichtsbehörde bereits Mitte 2008 mitgeteilt, dass sie beabsichtige, das Thema Datenschutz in das Qualitätsmanagement zu integrieren und bei Prüfungen entsprechend zu kontrollieren. Hierfür soll den Ärzten praktische Hilfestellung gegeben werden. Die Aufsichtsbehörde ist gerne bereit, die KV bei diesem sehr zu begrüßenden Vorhaben zu unterstützen. Die Ergebnisse der geplanten Besprechungen sollten in einen Leitfaden einfließen. Auch die Software-Problematik sollte vertieft werden.

14.2 Medizinische Forschung

Das Regierungspräsidium Darmstadt wurde in den vergangenen Jahren immer wieder um Beratung zur datenschutzgerechten Gestaltung von Forschungsvorhaben gebeten. U. a zur Einrichtung einer Knochenmarkspenderdatei, zum bundesweiten Projekt Mammographie-Screening, zu einem Suchtbekämpfungsprojekt, zu einer Studie zum Wachstum und zur Ausbreitung von Brustkrebs, im Rahmen eines Pilotprojekts zur Surveillance (Überwachung) von Influenza-Erkrankungen, zur Beobachtung der kognitiven Leistungsfähigkeit bei Multipler Sklerose und zu einem Biopsieprojekt bei Morbus Parkinson.

14.2.1 Die Funktion von Ethikkommissionen bei der Überprüfung von Forschungsprojekten

Ethikkommissionen erstellen schriftliche Voten für oder gegen beantragte Forschungsvorhaben. Diese Verfahren sind in Deutschland zum Beispiel für jede der klinischen Prüfungen, wie sie für die Zulassung von Arzneimitteln durchgeführt werden müssen, gesetzlich vorgeschrieben.

Ethikkommissionen gehen hauptsächlich auf die revidierte Deklaration von Helsinki des Weltärztebundes von 1975 zurück. Das übergreifende Ziel der Ethikkommissionen ist die Beurteilung von Forschungsvorhaben, die an Lebewesen durchgeführt werden, aus ethischer, rechtlicher und sozialer Sicht, sowie der Schutz des Individuums vor den Folgen der (klinischen) Forschung am Lebewesen. In der Regel sind Mediziner und Naturwissenschaftler Mitglieder eine Ethikkommission, die Aufnahme von Juristen und Theologen ist bei Besetzung einer Ethikkommission jedoch Pflicht.

Die gesetzliche Grundlage von Ethikkommissionen sind in Deutschland im Wesentlichen das Arzneimittelgesetz (§ 40 Abs. 1 AMG) und das Medizinproduktegesetz (§ 20 Abs. 7 MPG). Zudem sieht das Stammzellgesetz (StZG) für den Import embryonaler Stammzellen ebenfalls eine Prüfung und Bewertung durch eine eigens dafür gebildete Ethikkommission vor (§§ 8, 9 StZG). Die konkrete Bildung der Kommissionen richtet sich nach dem jeweiligen Recht des Bundeslands, ebenso ihr Verfahren. Träger von Forschungsvorhaben holen zum Teil auch dann eine Empfehlung der Ethikkommission ein, wenn deren Beteiligung nicht zwingend vorgeschrieben ist.

Im Rahmen ihrer Stellungnahme empfehlen Ethikkommissionen immer häufiger, eine Stellungnahme der Datenschutzaufsichtsbehörde einzuholen, so auch im nachfolgend geschilderten Fall.

14.2.2 Langzeitstudie bei Brustkrebserkrankungen

Im Jahr 2008 wurde eine vertiefte Prüfung einer Langzeitstudie bei Brustkrebserkrankungen vorgenommen.

Die anfragende Forschungseinrichtung - eine private Stelle - hat bereits verschiedene Grundstudien zum Thema Brustkrebs durchgeführt und führt

sie auch noch durch. Das Unternehmen arbeitet mit einer Vielzahl von Kliniken und Ärzten, welche als Prüfzentren bezeichnet werden, zusammen.

Mit einer Langzeitstudie möchte die Brustkrebsstudiengruppe nun feststellen, ob und in welchem Umfang es zu Rückfällen und zu Todesfällen nach Abschluss der Behandlung kommt. Dabei besteht die Problematik, dass die Patientinnen nach erfolgter Heilung oftmals den Kontakt zu dem Prüfzentrum, in welchem ihre Behandlung durchgeführt wurde, abbrechen und die Nachbehandlung bei ihrem Haus- bzw. Facharzt vornehmen lassen. Das heißt, die Prüfzentren selbst verfügen nicht über die für die Langzeitbeobachtung erforderlichen Daten. Daher sieht das Forschungskonzept vor, dass diese Gesundheitsdaten durch eine Befragung der Patientinnen erhoben werden. Ursprünglich sollte dies in der Weise erfolgen, dass die Prüfzentren, in welchen die Krebsbehandlung erfolgte, den Patientinnen Fragebögen zuschicken, in denen Auskunft zu ihrem derzeitigen Gesundheitszustand eingeholt wird. Schließlich wurde die Aufgabe der Zusendung dieser Fragebögen jedoch auf einen Datentreuhänder übertragen, welcher die Adressdaten verwaltet. Im Rahmen dieser Direktbefragung wird somit eine Adressdatenverarbeitung außerhalb der Arztpraxis bzw. Klinik notwendig.

Aus der Sicht der Datenschutzaufsicht ist es wichtig, die Teilnahme an der Grundstudie von der an der Langzeitstudie zu unterscheiden. Im vorgelegten ersten Entwurf der Einwilligungserklärung wurde jedoch beides miteinander vermengt. Dies war nicht akzeptabel, da die Einwilligungen in die jeweilige Grundstudie bereits vor längerer Zeit eingeholt worden waren und keine neuen Teilnehmerinnen an der Grundstudie mehr gewonnen werden sollten. Dieses war selbst für die Datenschutzaufsichtsbehörde aus den vorgelegten Unterlagen zunächst nicht ersichtlich.

Eine Überarbeitung und Ergänzung der dem Unternehmen bereits vorliegenden alten Einwilligungen durch die neu eingeholte Einwilligung war nicht angebracht. Die Einwilligung in die neue geplante Langzeitstudie ist vielmehr von der in die Grundstudie zu trennen, damit klar wird, was Gegenstand der Einwilligung ist. Dies ist insbesondere notwendig, weil die Patientin die Wahlfreiheit haben muss, sich dafür zu entscheiden, nur an der Grundstudie teilzunehmen, bei welcher die Datenerhebung nur durch die Prüfzentren erfolgt, nicht aber an der Langzeitstudie durch Direktbefragung mit gesonderter Verarbeitung der Adressdaten durch den Treuhänder. Daher ist eine neue separate Einwilligung für die Langzeitstudie einzuholen.

Wichtig für das Konzept der Langzeitstudie ist, dass eine klare Darstellung in der Einwilligung erfolgt und dass eine Treuhandlösung mit entsprechenden Verträgen vorgenommen wird. Als Datentreuhänder fungiert eine spezielle Abteilung einer Klinik, also eine von der Forschungseinrichtung unabhängige Stelle.

Die Fragebögen sollen nunmehr halbjährlich über diesen Treuhänder, welcher die Adressdaten verwaltet und über keinerlei medizinische Daten verfügt, versendet werden. Die Patientin hat im Rahmen der Langzeitstudie auch die Möglichkeit, anzugeben, dass sie - etwa wegen einer Verschlechterung des Gesundheitszustands - künftig nicht mehr selbst angeschrieben werden möchte. Sie kann in diesem Fall eine Kontaktperson benennen, welche die Auskünfte erteilt. Auch von dieser Person wird dann auf dem entsprechenden Formular eine Einwilligung zur Verarbeitung und Nutzung ihrer Adressdaten eingeholt.

Für die Rücksendung der Unterlagen erhält die Patientin zwei Briefumschläge: der Fragebogen mit den medizinischen Daten geht direkt an das Forschungsunternehmen. Dieser Fragebogen enthält lediglich ein Pseudonym (Patientenidentifikationsnummer.) Der Bogen, in welchem die Patientin Adressänderungen mitteilt und ggf. die Erklärung abgeben kann, dass sie keinen Kontakt mehr wünscht oder die Einwilligung widerruft, wird an den Treuhänder versandt.

Das Forschungsunternehmen selbst kann also die Patientin nicht identifizieren, es erhält keine Adressdaten etc. Lediglich anhand des Pseudonyms können die medizinischen Daten ausgewertet und mit den Daten aus der Grundstudie zusammengeführt werden.

Aufgrund eingehender Beratung durch die Aufsichtsbehörde wurde der Text der Einwilligungserklärung dahingehend abgeändert, dass den Patientinnen diese Datenverarbeitungen bewusst werden. Die Einholung der Einwilligungen und entsprechende Aufklärung erfolgt noch durch das jeweilige Prüfzentrum, welches die Krebsbehandlung durchgeführt hat.

Wiesbaden, 28. August 2009

Der Hessische Ministerpräsident:
Koch

Der Hessische Minister des Innern und für Sport:
Bouffier