16. Wahlperiode

Drucksache **16/7646**

HESSISCHER LANDTAG

22. 08. 2007

Vorlage
der Landesregierung

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

Vorgelegt mit der Stellungnahme zum Fünfunddreißigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten - Drucks. 16/6929 - nach § 30 Abs. 2 des Hessischen Datenschutzgesetzes in der Fassung vom 7. Januar 1999.

Eingegangen am 22. August 2007 · Ausgegeben am 29. August 2007
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 im nicht öffentlichen Bereich nach § 38 Abs. 1 BDSG die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz in Hessen, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln.

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

Die telefonischen Beratungen wurden dabei bis auf wenige Ausnahmen ebenso wenig erfasst wie Anfragen, die durch die Versendung von Informationsmaterial und Orientierungshilfen erledigt werden konnten.

Die 603 Überprüfungen auf Grund von Eingaben, Beschwerden und Pressemeldungen durch das Regierungspräsidium Darmstadt betrafen:

- in 139 Fällen die Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA),
- in 93 Fällen Anbieter von Tele- und Mediendiensten (Anbieter von Internetzugängen, -diensten und -inhalten, unverlangte E-Mail-Werbung),
- in 58 Fällen Handels- und Wirtschaftsauskunfteien,
- in 51 Fällen Banken, Kreditinstitute und EDV-Dienstleister im Zahlungsverkehr,
- in 33 Fällen Unternehmen der Direktmarketing- und Werbewirtschaft,
- in 29 Fällen Unternehmen des Groß- und Einzelhandels,
- in 26 Fällen den Datenschutz in Arbeitsverhältnissen und bei Arbeitsvermittlern,
- in 25 Fällen Unternehmen der Freizeit-, Touristik- und Reisebranche,
- in 22 Fällen Versicherungsgesellschaften,
- in 21 Fällen die Videoüberwachung von Grundstücken, Häusern und Wohnungen,
- in 20 Fällen den Gesundheitssektor (Ärzte, Krankenhäuser, Senioren- und Pflegeheime),
- in 17 Fällen Vereine (Sport, Soziales, Kultur) sowie deren Landes- und Bundesverbände,
- in 16 Fällen Adresshandelsunternehmen,
- in 10 Fällen Inkassounternehmen,
- in 9 Fällen Vermieter sowie Wohnungs- und Immobilienverwaltungsfirmen,
- in 8 Fällen Unternehmen des Verlags- und Medienbereichs,
- in 8 Fällen Anwaltskanzleien,
- in 6 Fällen Unternehmen der Versandhandelsbranche,
- in 3 Fällen Markt- und Meinungsforschungsunternehmen,
- in 2 Fällen Kreditkartenunternehmen,
- in 1 Fall die Auslandsdatenverarbeitung,
- in 6 Fällen sonstige Stellen.

Bei ca. 20 % der Beschwerden konnte zeitnah festgestellt werden, dass diese begründet waren. In insgesamt 122 Fällen wurden bei den Nachforschungen der Aufsichtsbehörde unzulässige Verarbeitungen personenbezogener Daten und andere Verstöße gegen Vorschriften des Datenschutzrechts und des Rechts der Tele- und Mediendienste festgestellt, die zu Beanstandungen der jeweiligen Verarbeitungsverfahren bei den betroffenen Stellen führten.

Die bei den Überprüfungen beanstandeten 122 Verstöße gegen Datenschutzbestimmungen wurden festgestellt:

- in 27 Fällen bei der SCHUFA, davon war in 14 Fällen ein Verstoß durch den Vertragspartner der SCHUFA ursächlich,
- in 25 Fällen bei Anbietern von Tele- und Mediendiensten,
- in 13 Fällen im Groß- und Einzelhandel,
- in 12 Fällen bei Kreditinstituten und Banken,
- in 11 Fällen bei Unternehmen der Direktmarketing- und Werbebranche,
- in 5 Fällen bei der Verarbeitung von Arbeitnehmer- und Bewerberdaten,
- in 5 Fällen im Gesundheitssektor,
- in 5 Fällen im Bereich Adresshandel,
- in 4 Fällen bei Versicherungsgesellschaften,
- in 3 Fällen bei Handels- und Wirtschaftsauskunfteien,
- in 2 Fällen bei Unternehmen der Freizeit-, Touristik- und Reisebranche,
- in 2 Fällen in der Versandhandelsbranche,
- in 2 Fällen bei Vereinen und Verbänden,
- in 2 Fällen bei der Videoüberwachung

sowie in jeweils einem Fall bei einem Inkassounternehmen, einem Kreditkartenunternehmen, bei der Markt- und Meinungsforschung sowie im Verlags- und Medienbereich.

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

1.2 Erledigung von Eingaben und Beschwerden aus den Vorjahren

Von den noch aus den Vorjahren anhängigen Beschwerden, die oftmals sehr vielschichtige Verarbeitungszusammenhänge betrafen, wurden im Berichtsjahr 163 Fälle abgeschlossen. Die Beurteilung dieser in der Regel nur mit hohem Ermittlungsaufwand aufklärbaren Eingaben ergab, dass davon 82 Eingaben begründet waren. Damit musste die Aufsichtsbehörde bei etwas mehr als 50 % dieser Fälle einen Datenschutzverstoß feststellen.

Die beanstandeten 82 Verstöße gegen Datenschutzbestimmungen wurden festgestellt:

- in 14 Fällen bei Unternehmen der Werbewirtschaft und werbenden Einzelhändlern,
- in 13 Fällen bei Anbietern von Telediensten,
- in 11 Fällen bei der SCHUFA,
- in 6 Fällen bei Arbeitgebern und Arbeitsvermittlern,
- in 6 Fällen bei der Videoüberwachung,
- in 5 Fällen im Gesundheitswesen,
- in 3 Fällen bei Banken,
- in 3 Fällen bei Unternehmen der Freizeit-, Touristik- und Reisebranche,
- in 2 Fällen bei Inkassounternehmen,
- in 2 Fällen bei Vermietern, Wohnungs- und Immobilienfirmen,
- in 2 Fällen bei Handelsauskunfteien,
- in 2 Fällen bei Vereinen und Verbänden,
- in 2 Fällen beim Versandhandel,
- in 2 Fällen bei Kreditkartenunternehmen

sowie in jeweils einem Fall bei einem Adresshändler, bei der Auslandsdatenverarbeitung, im Presse- und Medienbereich, bei einem Versicherungsunternehmen sowie bei fünf sonstigen Stellen.

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

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

Einen besonderen Schwerpunkt bildete – wie bereits im vorigen Berichtszeitraum – die Fußballweltmeisterschaft 2006 (siehe hierzu Ziff. 11.).
Insgesamt wurden im Berichtsjahr 39 Kontrollen vor Ort durchgeführt. Diese betrafen folgende Branchen/Bereiche:

- Videoüberwachungssysteme 15
- Ärztliche Praxen/Kliniken/Laboratorien/Verrechnungsstellen 3

- Vereine/Verbände/Stadionbetreiber 6
- Markt- und Meinungsforschung 1
- Industrie/Handel/Dienstleistung 12
- Inkasso-Unternehmen 2

Dabei wurden folgende Mängel am häufigsten festgestellt:

- Voraussetzungen des § 6b BDSG (Videoüberwachung) nicht erfüllt,
- fehlendes oder nicht ausreichendes Verfahrensverzeichnis, erforderliche Vorabkontrolle nicht durchgeführt,
- Mängel in den Bereichen der Datensicherheit, z.B. fehlende oder nicht ausreichende Passwörter, zu weit gehende Zugriffsrechte für einzelne Mitarbeiter,
- Mangelnde Fachkunde der zum Datenschutzbeauftragten bestellten Personen.

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

Die Ausübung der Kontrolle nach § 38 BDSG ist nicht auf den Einzelfall oder einen Anlass beschränkt. Eine Pflicht zur Voranmeldung der Überprüfung durch die Aufsichtsbehörde besteht nicht. Üblicherweise werden Kontrollen von der Aufsichtsbehörde aber nach Absprache mit der Unternehmensleitung und dem betrieblichen Datenschutzbeauftragten terminiert. Bei der anlassbezogenen Prüfung macht es allerdings häufig wenig Sinn, sich anzukündigen, weil dann für die Unternehmen die Möglichkeit besteht, den Datenbestand zu bereinigen.Ebenso ist auf eine Ankündigung zu verzichten, wenn Unterlagen unsachgemäß entsorgt werden, beispielsweise wenn ein Bürger zufällig brisante ärztliche Unterlagen oder Akten eines Finanzberaters in einem Restmüllcontainer entdeckt. In einem solchen Fall muss die Aufsichtsbehörde sofort handeln und vor Ort gehen, um den Verursacher zu ermitteln und dafür zu sorgen, dass die Unterlagen vor unbefugten Zugriffen geschützt werden. Dabei sind bei Bedarf Polizei und ggf. Staatsanwaltschaft einzubeziehen. Die Unterlagen müssen sicher und ordnungsgemäß bis zum Abschluss des Verfahrens aufbewahrt werden. Bei der verantwortlichen Stelle sind umgehend Überprüfungen durchzuführen.

Nach § 38 Abs. 4 BDSG sind die von der Aufsichtsbehörde mit der Kontrolle beauftragten Personen befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Sie können geschäftliche Unterlagen, insbesondere die Übersicht nach § 4g Abs. 2 Satz 1 BDSG sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen. § 24 Abs. 6 BDSG gilt entsprechend, d. h. die Kontrollbefugnis erstreckt sich auch auf Daten, die einem besonderen rechtlichen Schutz, z. B. der ärztlichen Schweigepflicht, unterliegen. Der Auskunftspflichtige hat die Kontrollmaßnahmen zu dulden.Wird den Mitarbeitern der Aufsichtsbehörde das Betreten der Geschäftsräume verweigert oder werden Auskünfte nicht erteilt, erfüllt dies den Tatbestand einer Ordnungswidrigkeit (§ 43 Abs. 1 Nr. 10 BDSG).

Innerhalb des Berichtszeitraums wurde den Mitarbeitern der Aufsichtsbehörde bei zwei Überprüfungen der Zutritt zu den Geschäftsräumen tatverdächtiger Unternehmen verweigert bzw. wurden diese aufgefordert, das Grundstück zu verlassen. Da in beiden Fällen schwerwiegende Verstöße gegen datenschutzrechtliche Bestimmungen aufzuklären waren und von weiteren Tathandlungen sowie dem Vernichten von Beweismitteln ausgegangen werden musste, bestand die Notwendigkeit, einen richterlichen Durchsuchungsbeschluss zu erwirken. Bei der Durchsuchung handelt es sich um eine Zwangsmaßnahme zur Strafverfolgung (§ 102 StPO), die der Tatverdächtige zu dulden hat. Da die Gesetze über das Strafverfahren für das Bußgeldverfahren sinngemäß Anwendung finden (§ 46 OWiG), konnte die Aufsichtsbehörde in entsprechender Weise tätig werden, auch wenn zum Zeitpunkt der Ermittlungen noch nicht sicher feststand, ob die Verstöße strafrechtlich oder im Rahmen eines Ordnungswidrigkeitenverfahrens zu ahnden sein werden. Aufgrund der Beweismittel und der bereits gewonnenen Erkenntnisse sahen die Amtsrichter die Voraussetzungen für die Anordnung von Durchsuchungsbeschlüssen als erfüllt an. In einem der Fälle waren zwei Müllsäcke, gefüllt mit Unterlagen zu den gesundheitlichen Verhältnissen einer Vielzahl

von Personen, in einem öffentlich zugänglichen Container gefunden worden. Der zweite Fall bezog sich auf die unrechtmäßige Verarbeitung sehr persönlicher Daten einzelner Betroffener. Die Prüfungen konnten mit Unterstützung der Polizei jeweils erfolgreich durchgeführt werden. Da die Verfahren noch nicht abgeschlossen sind, werden die Sachverhalte im nächsten Tätigkeitsbericht ausführlicher dargestellt.

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 294 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 werden bis auf wenige Ausnahmen nicht statistisch erfasst.

Die statistische Auswertung der 294 Fälle ergab folgende inhaltliche Schwerpunkte:

40 Anfragen zum Arbeitnehmerdatenschutz:
Zeitraum der Speicherung von Bewerberdaten, datenschutzkonformer Umgang mit Bewerberdaten bei E-Mail-Bewerbung, Weitergabe von Mitarbeiterdaten an Betriebsrat (z. B. Krankheitstage der Mitarbeiter, Namen der Beschäftigten von Fremdfirmen für Betriebsratswahl), mögliche Verletzungen datenschutzrechtlicher Bestimmungen bzw. des Briefgeheimnisses bei Zustellung von Kündigungsschreiben durch Kurierfahrer, Zugriff des Arbeitgebers auf die Dateien eines Arbeitnehmers nach längerer Krankheit und anschließender Verrentung, Fortbestand des E-Mail-Accounts nach Ausscheiden aus dem Unternehmen, private Nutzung von E-Mail und Internet am Arbeitsplatz, Zugriff auf den betrieblichen Alarmierungsplan (mit den persönlichen Daten der Abteilungsleiter) für alle Mitarbeiter einer Abteilung, Zugriff des Arbeitgebers auf medizinische Daten von Piloten und Flugbegleitern, beabsichtigte Gesprächsaufzeichnung durch den Werkschutz, Weitergabe von personenbezogenen Daten an Dritte im Rahmen der Arbeitnehmerüberlassung, Veröffentlichung von "Rennlisten" in einem Pharmaunternehmen, Auskunftsersuchen eines Gläubigers an den Arbeitgeber nach neuer Adresse eines Arbeitnehmers, Speicherung von Mitarbeiterdaten für Bonussysteme, Leserechte des Leiters der Datenverarbeitung für die Mailboxen des Betriebsrates, Einführung einer elektronischen Personalakte, Weitergabe personenbezogener Daten durch den Arbeitgeber zur Ausstellung einer Kreditkarte für den Mitarbeiter, Zulässigkeit des Mitschnitts einer betrieblichen Telefonkonferenz durch Moderatoren, Gestaltung eines Fragebogens zur Mitarbeiterbefragung, Einrichtung einer Datenbank zur Arbeitnehmervermittlung und Gestaltung von Bewerberfragebögen, Protokollierung der Verkehrsdaten der ein- und ausgehenden Telefonate aller Mitarbeiter, Whistleblowing (siehe hierzu Ziff. 2.2 und Ziff. 10.1), Nutzung der Arbeitnehmerdaten bei Versand einer Zeitung, Verarbeitung von Daten betreffend die Nutzung des für dienstliche Zwecke eingesetzten privaten Kraftfahrzeugs durch den Arbeitgeber.

39 Anfragen zur Datenverarbeitung im Ausland:
Fragen zur Datenübermittlung in so genannte "Drittstaaten" (Staaten außerhalb der Europäischen Union und des Abkommens über den Europäischen Wirtschaftsraum), insbesondere der Transfer von Arbeitnehmerdaten an außereuropäische Konzern-Muttergesellschaften und an außereuropäische Datenverarbeitungsdienstleister, Anfragen zum Abschluss von verbindlichen Unternehmensregelungen und deren Abstimmung auf europäischer Ebene, Fragen zu EU-Standardvertragsklauseln (siehe hierzu Ziff. 9.), Anwendbarkeit des BDSG hinsichtlich der US-Streitkräfte, Erläuterungen zum Safe Habour Verfahren, Bewertung eines Rechtsgutachtens zur Übermittlung sensibler Daten in einen Drittstaat.

26 Anfragen zur SCHUFA:
Allgemeine Fragen zu den SCHUFA-Verfahren, insbesondere Unterscheidung der Verfahren, Merkmale, Speicher- und Löschfristen, allgemeine Fragen zum Scoring-Verfahren, Informationen über die Rechte der Betroffenen, Sicherheitssystem beim Online-Abruf der SCHUFA-Selbstauskunft (siehe hierzu Ziff. 7.2), Beratung der SCHUFA zur Neugestaltung der SCHUFA-Klausel, Informationen zu neuen SCHUFA-Produkten.

26 Anfragen zur Datenverarbeitung durch Vereine und Dachverbände:
Anfragen zur Zulässigkeit der Datenverarbeitung des Deutschen Fußball-Bundes anlässlich der Fußball-WM 2006 (siehe hierzu Ziff. 11.), Auskunftsersuchen einer Stadtverwaltung an den Deutschen Fußball-Bund wegen Aufenthaltsbestimmung einer Person, Datenverarbeitung im Rahmen der Veröffentlichung eines Heimatgeschichte-Vereins, Einwilligungserklärung auf sportärztlichem Untersuchungsbogen, Veröffentlichung der Richterberichte bei Hundeschauen, Aushang der Vereinsmitgliederliste im Flur eines Vereinsheims und Veröffentlichung von nicht gezahlten Beiträgen, Herausgabe der Mitgliederliste an einzelne Vereinsmitglieder, Versendung einer Zeitschrift durch eine Gewerkschaft an ihre Mitglieder, Veröffentlichung personenbezogener Daten im Internet bei Verhängung einer Spielsperre, Erstellung von Eintrittsbuttons und Parkausweisen für eine Vereinsveranstaltung.

25 Anfragen zum betrieblichen Datenschutzbeauftragten:
Fragen zur Abberufung und Neubestellung sowie zur Kündigung von Datenschutzbeauftragten, Information und Beratung zu Rolle, Stellung, erforderliche Qualifikation und Aufgaben des Datenschutzbeauftragten, Haftung des Datenschutzbeauftragten, Fragen zur Beauftragung von externen Datenschutzbeauftragten, u. a. externe Datenschutzbeauftragte in Arztpraxen und Apotheken (siehe Ziff. 2.2: Merkblatt), Fragen zur Inkompatibilität der Aufgaben des Datenschutzbeauftragten mit anderen Aufgaben (IT-Leiter, Geldwäschebeauftragter, Personalleiter), Fragen zur hierarchischen Einbindung des Datenschutzbeauftragten im Unternehmen.

24 Anfragen aus dem Gesundheitssektor:
Stellungnahme zu diversen Forschungsprojekten, u. a. Beurteilung eines Pilotprojektes zur wissenschaftlichen Überwachung und Anwendung von Influenza-Erkrankungen, Zulässigkeit der Weitergabe der Pflegedokumentation an den Medizinischen Dienst, Zugriffsmöglichkeiten niedergelassener Ärzte auf Daten stationär behandelter Patienten, Austausch klientenbezogener Daten zwischen den Mitarbeitern verschiedener Bereiche einer Suchthilfeeinrichtung, visuelle Betreuung von Pflegebedürftigen (siehe hierzu Ziff. 14.), Fragen zur ärztlichen Schweigepflicht im Zusammenhang mit Auskünften an die Krankenversicherung, Weitergabe von Patientendaten in einer Erbschaftsangelegenheit, Stellungnahme zur Versendung ärztlicher Befunde per Telefax.

20 Anfragen zum Datenschutz bei Banken:
Anforderungen an die Einführung eines Customer Relationship Management (CRM) Moduls, Einsatz biometrischer Verfahren, Veröffentlichung des Unterschriftenverzeichnisses der Mitarbeiter, Handhabung der Protokollierung der lesenden Zugriffe auf Kontodaten, Einschaltung der Polizei wegen des Verdachtes der Erpressung eines Bankkunden, datenschutzrechtliche Aspekte eines neu gestalteten Kundenempfehlungsprogramms (siehe hierzu Ziff. 13.), SCHUFA-Merkmal "Konditionsanfragen" (siehe hierzu Ziff. 7.3), Hinweise zu Form und Inhalt einer Allfinanzklausel, Anfrage zur datenschutzgerechten Gestaltung von Research-Systemen zur Aufdeckung von Geldwäsche, Zulässigkeit der Weitergabe von Kontodaten an das Amt für Ausländerangelegenheiten einer Stadtverwaltung.

18 Anfragen zum Datenschutz im Internet:
Beratung zu Internet-Foren, Löschung von Beiträgen in Online-Foren, Datenschutz in einem Chatroom, Datenschutzhinweis nach § 4 Abs. 1 TDDSG, Umgang mit unerwünschten Werbefaxen, Veröffentlichung eines Fotos auf einer Homepage, Ermittlung eines Webmasters, Informationen zu Phishing-Mails und Online-Banking, Datenschutz bei Internet-Zugangsanbietern , Erläuterungen zur Verantwortlichkeit des "admin-c:", datenschutzrechtliche Aspekte von Altersverifikationssystemen, Fragen zur Speicherung von Verbindungsdaten, Beratung zur Einführung eines Ferndiagnosesystems für Kundenrechner, Managementsystem für Online-Bewerbungen, Stellungnahme zur internationalen Entwicklung des "Whois-Dienstes", Zulässigkeit der

Übermittlung von Informationen über den TK-Provider der Telefonanschlussinhaber an Verlage, die Teilnehmer-Verzeichnisse veröffentlichen.

10 Anfragen zur Videoüberwachung
Stellungnahmen zur Videoüberwachung des öffentlichen Raums (Bürgersteige, Straßen, Parkplätze, Haltestellen, Brunnen) durch Privatpersonen und Unternehmen, Beratung hinsichtlich der Videoüberwachung von Privatgrundstücken (Gebäude, Hoffläche, Einfriedung) durch die Eigentümer, Hinweise zur Einrichtung einer Videoüberwachung in Teilbereichen eines Hotels, Fragen zur Videoaufzeichnung durch den Arbeitgeber am Arbeitsplatz.

6 Anfragen zur Versicherungsbranche
Datenschutzrechtliche Beratung in Bezug auf eine Berufsunfähigkeitsversicherung, Übermittlung personenbezogener Daten in einem Regressfall, Kündigung einer Rechtsschutzversicherung und damit verbundenes Auskunftsersuchen, Bewertung eines Pilotprojektes einer Kfz-Versicherung für ein neues Tarifmodell.

6 Anfragen zu Handels- und Wirtschaftsauskunfteien
Beratung zur Arbeitsweise von Auskunfteien, Aufklärung von Bürgern zu Datenschutzrechten (Auskunft, Löschung, Sperrung), Übermittlung von Kundendaten eines Versandhändlers an eine Auskunftei ohne Einwilligung der Kunden, Beratung einer Auskunftei hinsichtlich des Webservices.

4 Anfragen zum Datenschutz durch Technik und zur Datensicherheit
Auswertung von sichergestellten Datenträgern und Unterlagen im Rahmen eines Ermittlungsverfahrens, Anfrage zu einem Fingerabdruck-Bezahlsystem (Biometrie), Hinweise zum Aufbau der IT-Infrastruktur bei telemedizinischen Anwendungen, Anfrage zu Telematik-Anwendungen in Kraftfahrzeugen.

4 Anfragen zur Werbewirtschaft und dem Adresshandel
Beratung zum Umgang mit unverlangter Werbung, Beratung eines Verbandes zur Nutzung der Kundendaten für Werbezwecke.

4 Anfragen aus dem Bereich Miete und Wohnen
Bekanntgabe der abrechnungsrelevanten Verbrauchsdaten durch die Hausverwaltung an alle Wohnungseigentümer bzw. Mieter in der Nebenkostenabrechnung, Anfragen zur Erhebung und Verarbeitung von Daten von Mietern und Mietbewerbern, Beratung einer Hausverwaltung bezüglich der Weitergabe von Mieterdaten auf Verlangen einer Bank.

2 Anfragen zur Meldepflicht nach §§ 4d, 4e BDSG
Beratung zu Fragen der gesetzlichen Meldepflicht.

2 Anfragen zur Markt- und Meinungsforschung
Beratung zum Umgang mit unerwünschten Anrufen von Call-Centern (z. B. zwecks Teilnahme an einer Umfrage zu Schlafgewohnheiten), Zulässigkeit der Speicherung von Telefonnummern in einer Sperrdatei nach Widerspruch des Betroffenen nach § 28 Abs. 4 BDSG.

38 Anfragen aus unterschiedlichen Wirtschafts- und Lebensbereichen
Es gibt kaum noch einen Wirtschaftssektor oder einen Lebensbereich, in dem personenbezogene Daten nicht automatisiert verarbeitet werden. Daher waren die Anfragen an die Aufsichtsbehörde auch sehr breit gestreut und betrafen unter anderem die Erhebung und Verarbeitung personenbezogener Daten in den Branchen Einzel- und Versandhandel, Reise und Touristik sowie bei Datenverarbeitungsdienstleistern, den Umgang mit persönlichen Daten bei Seminarveranstaltungen, die Erforderlichkeit einer Ausweiskopie für eine Auskunft nach § 34 Abs. 1 BDSG, die Zulässigkeit des Abgleichs von Kunden-, Lieferanten- und Mitarbeiterlisten mit "Antiterrorlisten" und das Betreiben einer Internet-Seite zur Bewertung von Produkten und Leistungen von Unternehmen mit schlechter Zahlungsmoral.

2.2 Vorträge, Informationsmaterial und Orientierungshilfen

Im Rahmen von Informationsveranstaltungen diverser Institutionen und Stellen hat das Regierungspräsidium Darmstadt auch im Jahr 2006 wieder Fragen zum Datenschutz beantwortet und Vorträge gehalten.

Bei der Frühjahrstagung des Erfahrungsaustauschkreises Hessen der Gesellschaft für Datenschutz und Datensicherheit e. V. referierte eine Vertreterin der Aufsichtsbehörde zum Thema "Auslandsdatentransfer" (siehe hierzu Ziff. 9.). Dem an die Aufsichtsbehörde herangetragenen Wunsch, anlässlich der Herbsttagung über das Thema "Whistleblowing" (siehe hierzu Ziff. 10.1) zu informieren, wurde ebenfalls entsprochen.

Auch an einer Veranstaltung des Erfahrungskreises des Deutschen Instituts für Betriebswirtschaft (DIB) nahmen Vertreterinnen der Aufsichtsbehörde teil und standen für die Beantwortung von Fragen der anwesenden Unternehmensvertreter zur Verfügung.

Bei einem Hospizverein wurde über Fragen zur Datenverarbeitung referiert.

Des Weiteren informierte die Aufsichtsbehörde auf einer gemeinsamen Veranstaltung der Industrie- und Handelskammern Darmstadt, Offenbach und Wiesbaden über das Thema "Der betriebliche Datenschutzbeauftragte" und beantwortete die anschließenden Fragen der Unternehmensvertreter.

Wie schon in den vergangenen Jahren hat sich die Aufsichtsbehörde wieder eingehend mit der RFID-Technik beschäftigt, die z. B. bei der Fußball-Weltmeisterschaft 2006 zum Einsatz gekommen ist. Auch im Berichtsjahr nutzte die Aufsichtsbehörde die Gelegenheit, im Rahmen verschiedener Veranstaltungen (Arbeitskreis Technik der Landesdatenschutzbeauftragten, Open Ohr Festival Mainz, 9. Europäischer Polizeikongress, Fraunhofer Forum im Rahmen der Cebit) über diese Thematik zu informieren.

Das Angebot an Informationsmaterial, das die Datenschutzaufsichtsbehörde zu unterschiedlichsten Fragestellungen des Datenschutzrechts bereithält, wurde auch im Berichtsjahr wieder gut angenommen.
Aufgrund des Gesetzes zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft vom 22. August 2006 (BGBl. I, Seite 1970), mit dem auch das Bundesdatenschutzgesetz novelliert wurde, hat die Aufsichtsbehörde ihr "Merkblatt zum betrieblichen Datenschutzbeauftragten" überarbeitet und den gesetzlichen Änderungen angepasst. Das überarbeitete Merkblatt von der Website der Aufsichtsbehörde abrufbar. Diese wurde im Berichtsjahr neu gestaltet und ist jetzt erreichbar unter "http://www.rp-darmstadt.hessen.de" im Bereich "Sicherheit und Ordnung" unter der Rubrik "Datenschutz". Hier können Mustertexte, Meldeformulare sowie weitere Merk- und Hinweisblätter zu den unterschiedlichsten Themen abgerufen werden.

3. Genehmigungsverfahren nach § 4c Abs. 2 BDSG

Im Rahmen der vielfältigen Beratungen zum Drittstaatentransfer stellte sich häufig die Frage eines Genehmigungserfordernisses nach § 4c Abs. 2 BDSG. Letztlich konnte die Frage aber bis auf einen Fall, bei dem die Klärung noch nicht abgeschlossen ist, jeweils verneint werden.
Die Unternehmen entschlossen sich zur wörtlichen Verwendung der EU-Standardvertragsklauseln, bei der keine Genehmigungspflicht besteht. Vertragsbeitritte zu den Standardvertragsklauseln wurden von der Aufsichtsbehörde als nicht genehmigungspflichtig bewertet (siehe hierzu Ziff. 9.3 und 9.4).

Ein Pharmakonzern mit Hauptsitz in Hessen legte der Aufsichtsbehörde eine verbindliche Unternehmensregelung zum Datenschutz vor, mit der konzernweit für ein angemessenes Datenschutzniveau gesorgt und somit die datenschutzrechtlichen Voraussetzungen für den weltweiten Austausch von personenbezogenen Daten erfüllt werden sollen.Diese Unternehmensregelung war von dem fachkundigen betrieblichen Datenschutzbeauftragten des Unternehmens erarbeitet worden, sodass nur wenige Ergänzungen bzw. Änderungen erforderlich waren.

Nach Abstimmung in der Arbeitsgruppe Internationaler Datenverkehr (siehe Ziff. 6.) konnte die Aufsichtsbehörde daher bestätigen, dass die Unternehmensregelungen als Grundlage für ein angemessenes Datenschutzniveau nach § 4b Abs. 2 Nr. 3 BDSG anzusehen ist. Die Aufsichtsbehörde konnte sich in Übereinstimmung mit dieser Arbeitsgruppe auch der Auffassung des betrieblichen Datenschutzbeauftragten anschließen, dass nur die hessische Muttergesellschaft des Konzerns datenexportierende Stelle ist, nicht aber deren Tochtergesellschaften in Deutschland und anderen europäischen Ländern (siehe hierzu Ziff. 9.1).

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 94 Verfahren von 86 verantwortlichen Stellen im Melderegister eingetragen. Nur vier verantwortliche Stellen haben mehr als ein Verfahren gemeldet.

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

5. Ordnungswidrigkeitenverfahren

Im Berichtsjahr wurden vom Regierungspräsidium Darmstadt neun Verfahren nach dem Ordnungswidrigkeitengesetz (OWiG) eingeleitet:

nach § 43	Grund der Einleitung	Ausgang des Verfahrens
Abs. 1 Nr. 1 u.10 BDSG	unvollständige Meldung und Nichterteilung von Auskünften	eingestellt
Abs. 1 Nr. 2 u. 10 und Abs. 2 Nr. 1 BDSG	mehrfache Verstöße gegen Vorschriften des BDSG	noch anhängig
Abs. 1 Nr. 10 BDSG	Nichterteilung von Auskünften	eingestellt (2 Verfahren)
Abs. 1 Nr. 10 BDSG	Nichterteilung von Auskünften	noch anhängig
Abs. 2 Nr. 1 und 3 BDSG	unbefugte Verarbeitung	Bußgeld rechtskräftig
Abs. 2 Nr. 3 BDSG	unbefugtes Beschaffen	Bußgeld rechtskräftig
Abs. 2 Nr. 3 BDSG	unbefugtes Beschaffen	Abgabe an Amtsgericht
Abs. 2 Nr. 4 BDSG	Erschleichen von Daten	eingestellt

Ein Teil der Verfahren, die wegen einer Verletzung formaler Pflichten eingeleitet wurden, konnte letztlich eingestellt werden, nachdem sich die verantwortlichen Personen kooperativ zeigten oder sich vom Tatvorwurf entlasten konnten.

Von einer weiteren Verfolgung wurde auch bei einem Sachverhalt abgesehen, den der Vermieter eines Mehrfamilienhauses zur Anzeige gebracht hat. Dieser wollte einen materiellen Datenschutzverstoß darin erkannt haben, dass ein Mieter sich nach einem Streit über die Nebenkostenabrechnung direkt bei dem Versicherer des Wohnhauses über die Zusammensetzung einer bestehenden Immobilienversicherung erkundigte und auch eine detaillierte Aufstellung ausgehändigt bekam. Die Informationen seien dem Mieter gegeben worden, weil dieser angegeben hätte, im Auftrag des Vermieters zu handeln, worin der Anzeigeerstatter den Tatbestand des Erschleichens personenbezogener Daten durch unrichtige Angaben verwirklicht sah. Nach Darstellung des Beschuldigten hatte sich dieser allerdings keineswegs als Bevollmächtigter ausgegeben, sondern eindeutig als Mieter. Da die Anfrage des Mieters telefonisch erfolgte, konnte der Sachverhalt nicht abschließend geklärt werden. Das Verfahren wurde daher eingestellt und der Beschuldigte belehrt, dass er in seiner Eigenschaft als Mieter zwar einen Rechtsanspruch darauf hat, alle der Abrechnung zugrunde liegenden Verträge einzusehen,

dies jedoch nicht dazu berechtigt, solche Daten eigenmächtig bei den Vertragspartnern des Vermieters einzuholen.

Eindeutig stellte sich die Beweislage in einem Fall dar, bei dem sich ein Bankangestellter unberechtigt über den Kontostand eines Kunden informiert hatte, um daraus persönliche Neugierde zu befriedigen. Auf die Darstellung unter Ziff. 8.2 wird Bezug genommen.

In einem weiteren Verfahren musste sich die Aufsichtsbehörde mit einem Bankmitarbeiter auseinandersetzen, dem von einem Beschwerdeführer vorgeworfen wurde, eine SCHUFA-Anfrage für private Zwecke vorgenommen zu haben. Die Ermittlungen ergaben, dass der Beschuldigte die SCHUFA-Auskunft einholte, um sich Kenntnisse zur Bonität eines Mietinteressenten zu verschaffen. Dem Anzeigeerstatter waren entsprechende Eintragungen in der SCHUFA-Selbstauskunft aufgefallen, die den Tatverdacht begründeten. Dem Beschuldigten wurde wegen unbefugten Abrufens nicht allgemein zugänglicher Daten eine Geldbuße in Höhe von 300,-- € auferlegt.

Bei drei Sachverhalten waren die Verfahren bei Redaktionsschluss dieses Berichtes noch nicht abgeschlossen.

6. Teilnahme an bundesweiten Arbeitsgruppen des Düsseldorfer Kreises

Das Regierungspräsidium Darmstadt beteiligt sich regelmäßig an der Arbeit des sog. "Düsseldorfer Kreises". In diesem bundesweiten Gremium der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich werden datenschutzrechtliche Problemstellungen übergreifend erörtert mit dem Ziel, die Rechtspositionen der Datenschutzaufsichtsbehörden der Bundesländer grundsätzlich aufeinander abzustimmen und das Vorgehen der Landesaufsichtsbehörden gegenüber den für die Verarbeitung personenbezogener Daten verantwortlichen Stellen in den Ländern zu koordinieren.

Die Sitzungen des Düsseldorfer Kreises werden zunächst in branchen- oder themenspezifischen Arbeitsgruppen (AG) vorbereitet, die sich in der Regel zweimal jährlich treffen. Es handelt sich dabei um die AG Auskunfteien, die AG Versicherungswirtschaft, die AG Kreditwirtschaft, die AG Telekommunikation, Tele- und Mediendienste, die AG Internationaler Datenverkehr und die neu gebildete AG Beschäftigtendatenschutz.

In den Arbeitsgruppen werden u. a. Informationen über aktuelle Datenschutzthemen ausgetauscht, problematische datenschutzrechtliche Fragestellungen vorbesprochen, möglichst gemeinsame Rechtspositionen gefunden, Formulierungsvorschläge ausgearbeitet und Beschlussvorlagen für den Düsseldorfer Kreis erstellt. In einigen Arbeitsgruppen setzen sich die Mitglieder auch direkt mit großen Unternehmen oder deren Interessenverbänden auseinander und diskutieren möglichst frühzeitig mit den bundesweit tätigen Unternehmen die datenschutzrechtlich relevanten Aspekte von neuen Projekten und Planungen sowie die Auswirkungen gesetzlicher Änderungen auf bestehende Datenverarbeitungen in den jeweiligen Branchen.

Das Regierungspräsidium Darmstadt ist in fast allen Arbeitsgruppen des Düsseldorfer Kreises vertreten und nimmt bei Bedarf auch gemeinsam mit dem Ministerium des Innern und für Sport an den Sitzungen des Düsseldorfer Kreises teil. In der AG Auskunfteien hat Hessen aufgrund des Wiesbadener Sitzes der SCHUFA Holding AG den Vorsitz inne. Dieser wird vom Ministerium des Innern und für Sport wahrgenommen, das Regierungspräsidium Darmstadt ist jedoch umfassend eingebunden (Vor- und Nachbereitung). In der AG Internationaler Datenverkehr ist das Regierungspräsidium Darmstadt ebenfalls besonders intensiv beteiligt, da im Rhein-Main-Gebiet viele international tätige Unternehmen ihren Sitz haben und daher eine Vielzahl von Grundsatzfragen an die Aufsichtsbehörde herangetragen werden, die diese aufarbeitet und in die AG einbringt (siehe hierzu Ziff. 9.).

Im Rahmen der verstärkten Zusammenarbeit zwischen den Dienststellen, die als Aufsichtsbehörden für den nicht öffentlichen Bereich nach § 38 BDSG tätig sind und den für den öffentlichen Bereich zuständigen Landesdatenschutzbeauftragten, hat ein Vertreter der hessischen Datenschutzaufsichtsbehörde im Jahr 2006 von dem Angebot der Konferenz der Datenschutzbeauf-

tragten Gebrauch gemacht, an einer Sitzung des dortigen Arbeitskreises Technik teilzunehmen. Auch in der gemeinsamen Unterarbeitsgruppe Fehler- und Unfalldatenspeicher, in der sowohl Vertreter der Datenschutzaufsichtsbehörden als auch Mitarbeiter von Landesdatenschutzbeauftragten vertreten sind, und deren Vorsitz der Hessische Datenschutzbeauftragte übernommen hat, wirkt das Regierungspräsidium Darmstadt mit.

Ausgesuchte Probleme und Einzelfälle

7. Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA)

7.1 Das Merkmal "Versandhauskonto" und die fortlaufende Übermittlung von Nachmeldungen an die Versandhändler

Versandhändler richten oft schon bei der ersten Bestellung ein "Kundenkonto" mit einer Kundennummer für den Besteller ein. Dies geschieht in der Erwartung, dass der Besteller dauerhaft Kunde wird und soll der erleichterten Abwicklung von Bestellungen dienen. Die Kundennummer ist dabei zentrales Steuerungs- und Abwicklungskennzeichen.

Der Versandhandel spricht in diesem Zusammenhang von dauerhaften Kundenbeziehungen und weist die Besteller teilweise in den Katalogen darauf hin, dass während des Bestehens eines "kündbaren Kundenkontos" Bonitätsauskünfte eingeholt werden. Unter diesen Voraussetzungen melden Versandhändler, die Vertragspartner der SCHUFA sind, das Merkmal "Versandhauskonto" im SCHUFA-B-Verfahren ein.Nach dem bisherigen Verfahren erhalten sie ab diesem Zeitpunkt fortlaufend Nachmeldungen zu dem Kunden im Rahmen des B-Verfahrens, selbst wenn die erste Bestellung die einzige bleibt oder der Kunde ab einem späteren Zeitpunkt keine Bestellung mehr bei dem Versandhändler tätigt. Für das Merkmal "Versandhauskonto" gilt nach dem SCHUFA-Verfahren grundsätzlich die allgemeine Löschfrist von drei Kalenderjahren. Aufgrund individueller Vereinbarungen lassen sich manche Versandhändler nur zwei Jahre lang mit Nachmeldungen beliefern.
In der Arbeitsgruppe Auskunfteien des Düsseldorfer Kreises bestand Einigkeit zwischen den Aufsichtsbehörden, dass die undifferenzierte Lieferung von Nachmeldungen nicht datenschutzkonform ist.

Nachmeldungen an Versandhändler sind nicht zu beanstanden, wenn ein Ratenzahlungskredit oder ein Dispo-Kredit, z. B. für Bestellungen bis 2.000,-- €, eingeräumt wurde. In allen anderen Fällen ist das Rechtsgeschäft nach Abwicklung des einzelnen Kaufgeschäfts für den Versandhandel abgeschlossen, es kann also kein berechtigtes Interesse mehr belegt werden. Damit sind Nachmeldungen in diesen Fällen rechtswidrig.
Der Argumentation des Bundesverbandes des deutschen Versandhandels, die Annahme einer dauerhaften Kundenbeziehung rechtfertige die fortlaufenden Nachmeldungen, kann nicht gefolgt werden, denn sie bedeutet, dass ein Dauerschuldverhältnis fingiert wird, das es aber nicht gibt. Ob die Versandhändler intern zur Erleichterung der Geschäftsabläufe ein "Versandhauskonto" einrichten, ist datenschutzrechtlich unerheblich, denn damit wird im Verhältnis zum Kunden jedenfalls keine Dauerrechtsbeziehung begründet. Selbst bei Sammelbestellern ist nicht ersichtlich, dass eine echte Dauerrechtsbeziehung besteht, sodass auch in diesen Fällen kein berechtigtes Interesse für Nachmeldungen erkennbar ist.

Den Versandhändlern bleibt es selbstverständlich unbenommen, bei jeder neuen Bestellung mit dem Merkmal "Anfrage des Versandhandels wegen Lieferung oder Leistung" eine aktuelle SCHUFA-B-Auskunft einzuholen. Die Aufsichtsbehörde hat den Bundesverband des deutschen Versandhandels über die datenschutzrechtliche Beurteilung des Merkmals "Versandhauskonto" und seiner Handhabung im SCHUFA-Verfahren in Kenntnis gesetzt und die SCHUFA aufgefordert, das Verfahren so abzuändern, dass Nachmeldungen nur in den oben genannten zulässigen Fällen erfolgen.

Grundsätzlich problematisch ist es darüber hinaus, wenn das Merkmal "Versandhauskonto" oder das oben genannte Anfragemerkmal für Scoring-Zwecke verwendet wird, ohne dass der Betroffene davon weiß und eingewilligt hat. Die Aufsichtsbehörden beabsichtigen, diese Problematik mit dem Bundesverband des deutschen Versandhandels zu erörtern.

7.2 SCHUFA Online Auskunft

Die SCHUFA hat nach einer Projektphase im Jahr 2006 allgemein die Möglichkeit der Online-Abfrage des eigenen Datensatzes als eine neue Variante der Selbstauskunft nach § 34 BDSG eingeführt. Damit können die Betroffenen nach dem Durchlaufen einer Anmeldung mit anschließendem Postident-Verfahren und einer Registrierung die bei der SCHUFA zu ihrer Person gespeicherten Daten jederzeit über das Verbraucher-Portal der SCHUFA im Internet abrufen ("www.meine-schufa.de").

Diese Variante besteht nun neben den bereits bekannten Möglichkeiten bei der SCHUFA eine Auskunft nach § 34 BDSG zu erhalten, nämlich Beantragung einer schriftlichen Selbstauskunft bzw. kostenlose Einblicknahme in den eigenen Datensatz in einer der SCHUFA-Geschäftsstellen.

Die Aufsichtsbehörde begrüßt grundsätzlich die Einrichtung der Online-Abfragemöglichkeit als weitere, dem Stand der Technik angepasste Variante der Auskunftserteilung. Auch die technische Seite des Verfahrens ist aus datenschutzrechtlicher Sicht nicht zu beanstanden. Die gewählte Identifizierung durch das Postident-Verfahren sowie ein wechselnder Zugangscode scheinen nach dem technischen Stand geeignet, um Dritte von unberechtigten Zugriffen auf fremde Datensätze auszuschließen.

Als problematisch wird jedoch die Höhe der Gebühr angesehen. Die Online-Abfrage kann für eine vierteljährliche Gebühr von nunmehr 7,80 € bezogen werden.
Die von der SCHUFA vertretene Position, bei der Online-Auskunft handele es sich nicht um eine "Auskunft" sondern um einen zusätzlichen Service für den Verbraucher, wird von der Aufsichtsbehörde nicht akzeptiert. Aus der Gestaltung der Internetseite der SCHUFA, aus deren eigenen Presseverlautbarungen sowie aus eigenen sonstigen Formulierungen des Unternehmens geht hervor, dass die SCHUFA selbst die Online-Auskunft als eine Möglichkeit ansieht, mit der Betroffene ihr Auskunftsrecht nach § 34 BDSG wahrnehmen können und mit der die gesetzliche Auskunftspflicht erfüllt wird.

Die Gebührenerhebung muss folglich mit den Anforderungen des § 34 Abs. 5 Satz 2 BDSG vereinbar sein. Danach dürfen nur die direkt zurechenbaren Kosten in die Preiskalkulation einfließen. Eine Mischkalkulation in der Weise, dass die Kosten für die einzelnen Auskunftsarten gemittelt werden und damit für die Online-Auskunft höhere als die unmittelbar hierfür zurechenbaren Kosten verlangt werden, wird von der Arbeitsgruppe Auskunfteien des Düsseldorfer Kreises als nicht zulässig angesehen. Die Bildung einer getrennten Pauschale für die Online-Auskunft wäre nicht zu beanstanden. Die SCHUFA wurde daher gebeten, Ihre Gebührenkalkulation zu überprüfen und der Aufsichtsbehörde darzulegen, wie sich die Gebühren für die Erteilung von Selbstauskünften, insbesondere der Betrag für die Online-Auskunft, errechnen.

7.3 Neues SCHUFA-Merkmal "Konditionenanfrage" - Nutzung des Merkmals "Kreditanfrage" für die SCHUFA-Score-Berechnung

Im vorangegangenen Tätigkeitsbericht wurde die Verwendung des SCHUFA-Merkmals "Anfrage Kredit" für das Scoring-Verfahren als problematisch beurteilt (vgl. Neunzehnten Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden - Drs. 16/5892 - Ziff. 6.1). Die SCHUFA führte im 4. Quartal des Jahres 2006 das neue Merkmal "Anfrage Kreditkonditionen" ein, das nicht in die Score-Berechnung einfließt. Die Presse wurde von der SCHUFA bereits im Frühjahr über die geplante Einführung informiert. Dies führte verschiedentlich dazu, dass Betroffene, welche die Pressemeldung zur Kenntnis genommen hatten, vermeintliche "Konditionenanfragen" an Kreditinstitute stellten, obwohl diese noch als "Kreditanfrage" in ihren Score einflossen.
Auch nach Einführung des Merkmals stellte sich heraus, dass Kreditinstitute offensichtlich keine Kenntnis hatten, wann das eine oder das andere Merkmal zur Anwendung kommen darf und die Bank-Filialen vor Ort nicht über eine Differenzierung der Anfragemerkmale informiert waren.

Die Aufsichtsbehörden halten es für erforderlich, dass ein schlüssiges Konzept der SCHUFA für die Voraussetzungen der Verwendung des Merkmals "Konditionenanfrage", d. h. die Abgrenzung zu dem Merkmal "Kreditanfrage" vorliegen muss. Es muss eindeutig definiert werden, wann welches Merkmal von den Vertragspartnern gemeldet werden darf. Selbstverständlich kann sich die SCHUFA diesbezüglich mit den Kreditinstituten abstimmen, sie kann die eindeutige Festlegung der Einmeldevoraussetzungen jedoch nicht auf die Kreditinstitute übertragen oder in deren Belieben stellen.

Die Aufsichtsbehörde forderte die SCHUFA daher auf, ein schlüssiges Konzept für die Verwendung der beiden Merkmale vorzulegen, nach dem Vertragspartner bei der Anfrage vorzugehen haben. Die SCHUFA kündigte ein solches Konzept an, bei Redaktionsschluss dieses Berichts lag es aber noch nicht vor.

Trotz Einführung des zusätzlichen und nicht im Score-Verfahren verwendeten Merkmals "Anfrage Kreditkonditionen" und ungeachtet der erforderlichen klaren Differenzierung besteht nach wie vor Kritik gegen die Einbeziehung des Merkmals "Kreditanfrage" in das Score-Verfahren. Es ist zumindest erforderlich, dass eine SCHUFA-Klausel unterschrieben wird.

Ein rein telefonisches oder mündliches Einverständnis wird als nicht ausreichend angesehen. Das vor vielen Jahren von den Aufsichtsbehörden gegenüber der Kreditwirtschaft gemachte "Zugeständnis" einer mündlichen Einwilligung vor der Übermittlung der Adressdaten und des Merkmals Kreditanfrage, ist insoweit überholt.

7.4 Was beeinflusst den SCHUFA-Score?

Im letzten Tätigkeitsbericht wurde über die nicht nachvollziehbare Entwicklung von Score-Werten eines Betroffenen berichtet (siehe Neunzehnten Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden - Drs. 16/5892 - Ziff. 6.1). Der Betroffene selbst hatte vermutet, dass sich das anfängliche Vorhandensein der Anfragen eines Anbieters von Gentests in seinem Datensatz negativ auf die Score-Berechnungen zu seiner Person ausgewirkt habe. Auffällig war damals zumindest, dass sich die Score-Werte drastisch verbesserten, nachdem die Anfragen des Gentestlabors fristgerecht gelöscht waren. Die SCHUFA legte der Aufsichtsbehörde die Gründe für diese Entwicklung nicht offen. Sie versicherte jedoch zwischenzeitlich gegenüber der Aufsichtsbehörde, dass sie in ihrem Scoring-Verfahren nicht nach der Art des Vertragspartners differenziere und teilte im Übrigen mit, dass sie die Zusammenarbeit mit dem Anbieter von Gentests beendet habe. Die Aufsichtsbehörde bekräftigte gegenüber der SCHUFA ihre Auffassung, dass Differenzierungen danach, welcher Vertragspartner ein Merkmal gemeldet hat, grundsätzlich als datenschutzrechtlich unzulässig bewertet werden.

Dieser Sachverhalt bestätigte die im vergangenen Jahr wieder zahlreich eingegangenen Beschwerden darüber, dass die Transparenz des Scoring-Verfahrens der SCHUFA unzureichend und dies für die Betroffenen nicht akzeptabel ist. Insoweit wird das Scoring-Verfahren der SCHUFA nach wie vor als unausgewogen kritisiert, da es keine funktionierenden Interventionsmöglichkeiten eröffnet, wenn Betroffene unzutreffend in eine Risikogruppe eingeordnet wurden bzw. da es nach wie vor zweifelhaft bleibt, ob die SCHUFA-Vertragspartner die individuelle Situation des Betroffenen in jedem Fall ausreichend würdigen. In Gesprächen mit der Aufsichtsbehörde sahen die SCHUFA und Vertreter einzelner Vertragspartner, die den SCHUFA-Score abrufen, keine Notwendigkeit, die Transparenz zu verbessern und verwiesen darauf, dass das System als Massengeschäft funktioniere.

8. Kreditwirtschaft

8.1 Datenweitergabe durch SWIFT

Im Juni 2006 berichteten US-Medien über den Zugriff verschiedener US-amerikanischer Behörden und des Geheimdienstes CIA auf Zahlungsverkehrsdaten des Dienstleisters SWIFT. SWIFT (Society for Worldwide Inter-

bank Financial Telecommunication) ist eine in Belgien ansässige Genossenschaft, der rund 7.800 Geschäftsbanken, eine Reihe von Zentralbanken, Brokerhäuser, Börsen und andere Finanzinstitute in ca. 200 Ländern angeschlossen sind. Über das Netz werden weltweit täglich mehrere Millionen Nachrichten zu Finanztransaktionen mit einem Volumen von rund 5 Billionen Euro ausgetauscht. Hierbei handelt es sich um Zahlungsverkehrsaufträge von Unternehmen, aber auch um Transaktionen, die von Privatpersonen veranlasst werden. Die Zahlungsanweisungen enthalten personenbezogene Daten wie Namen des Zahlungsanweisenden oder des Zahlungsempfängers. Um die Transaktionen abzusichern, unterhält SWIFT zusätzlich zu seinem Rechenzentrum in Belgien je ein Rechenzentrum in den Niederlanden und den USA, wohin der Datenbestand fortwährend gespiegelt wird. Die Zahlungsverkehrsdaten werden dabei über einen Zeitraum von 124 Tagen gespeichert. Nach den Terrorangriffen vom 11. September 2001 forderte das US Finanzministerium gegenüber SWIFT Zugang zu den in den USA gespeicherten Daten. Dieser auf Grundlage behördlicher Beschlagnahmeanordnungen ("subpoenas") gestützten Forderung ist SWIFT bislang nachgekommen.

Die belgische Datenschutzaufsichtsbehörde hat bei SWIFT eine umfassende Prüfung vorgenommen. Sie kommt in ihrem Gutachten zu dem Ergebnis, dass die Datenübermittlung an die US-Behörden weder durch nationales belgisches Datenschutzrecht noch die EU-Datenschutzrichtlinie 95/46/EG erlaubt ist. Die Verantwortlichkeit für die Einhaltung der Datenschutzvorschriften sieht die Aufsichtsbehörde sowohl bei SWIFT als auch bei den angeschlossenen Banken.

Die Problematik betrifft alle Mitgliedstaaten der EU, sodass eine einheitliche Lösung angestrebt wird. Die Artikel 29 Datenschutzgruppe der EU-Mitgliedsstaaten hat sich daher eingehend mit der Thematik befasst und hierzu die Stellungnahme 10/2006 (WP 128) am 22. November 2006 verabschiedet. Auch hier wird die gemeinsame Verantwortung für die Verarbeitung von personenbezogenen Daten von SWIFT und den Finanzinstituten und die Missachtung der EU-Datenschutzrichtlinie festgestellt. Des Weiteren umfasst die Erklärung auch die Forderung nach einer Reihe von Maßnahmen, um die gegenwärtige Situation zu verbessern.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich haben im Beschluss vom 9. November 2006 (abrufbar unter www.bfdi.bund.de, >Entschließungssammlung, >Düsseldorfer Kreis) ebenfalls Lösungen bezüglich der unrechtmäßigen Datenübermittlung angemahnt. Explizit wurde auch auf die Informationspflicht nach § 4 Abs. 3 BDSG hingewiesen. Der Kunde ist darüber zu informieren, wie seine Daten verarbeitet werden und dass US-Behörden Zugriff auf seine Daten erhalten können. Das Regierungspräsidium Darmstadt wird die Informationspolitik der Banken beobachten. Entsprechende Kontrollen wurden eingeleitet, waren aber bei Redaktionsschluss dieses Berichts nicht abgeschlossen. Nach derzeitigen Erkenntnissen haben Kreditinstitute eine Kurzinformation ins Internet eingestellt und stellen diese in den Bankfilialen zur Verfügung.

8.2 Protokollierung von lesenden Zugriffen auf Konten offenbart Missbrauch

Üblicherweise protokollieren Banken auch die lesenden Zugriffe von Mitarbeitern auf die Kundendaten - eine technische Maßnahme nach § 9 BDSG, mit deren Auswirkungen ein unüberlegt handelnder Bankmitarbeiter nicht rechnete.

Ein Bankkunde wandte sich an die Aufsichtsbehörde, da er den Zugriff auf seine Konten durch einen Mitarbeiter seiner Hausbank vermutete. Er befürchtete, dass dieser sich Informationen über seine Vermögensverhältnisse verschafft und diese an seine Ehefrau weitergeleitet habe. Auch der Vorwurf, die Konten könnten von dem Mitarbeiter manipuliert worden sein, wurde erhoben.

Nachdem die Aufsichtsbehörde die Bank informierte hatte, handelte diese schnell und konsequent. Der Mitarbeiter wurde mit sofortiger Wirkung von seiner Tätigkeit freigestellt. Die Auswertung der Protokolle offenbarte den lesenden Zugriff auf die Kontodaten des Beschwerdeführers durch den An-

gestellten. Der Verdacht der Manipulation bestätigte sich nicht. Für den Bankmitarbeiter zog der Verstoß gegen das Datengeheimnis arbeitsrechtliche Schritte nach sich. Die Aufsichtsbehörde verhängte ein Bußgeld gegen ihn, das auch rechtskräftig wurde.

9. Aspekte internationaler Datenverarbeitungen

Die nachfolgend dargestellten Grundsatzfragen haben sich im Rahmen der Beratungstätigkeit des Regierungspräsidiums Darmstadt ergeben. Sie wurden mit den hier entwickelten Lösungen in die Arbeitsgruppe Internationaler Datenverkehr eingebracht (siehe Ziff. 6). Soweit im Folgenden auch das Ergebnis der dort erfolgten Abstimmungen wiedergegeben wird, steht dies unter dem Vorbehalt, dass insoweit die beabsichtigte Veröffentlichung des Düsseldorfer Kreises maßgeblich ist, die bei Redaktionsschluss dieses Berichts noch nicht erfolgt war.

9.1 Bestimmung der "datenexportierenden Stelle" i. S. d. §§ 4b, 4c BDSG

Werden personenbezogene Daten von konzernangehörigen Stellen in ein konzernweites Datenverarbeitungssystem eingegeben und können die Daten dort von allen oder einigen Konzerngesellschaften weltweit abgerufen werden oder werden personenbezogene Daten in sonstiger Weise weltweit im Konzern weitergegeben, stellt sich die Frage, welche der europäischen Stellen des Konzerns "datenexportierende Stellen" i. S. d. §§ 4b, 4c BDSG sind.
Diese Frage hat große Bedeutung u. a. für den Abschluss von EU-Standardverträgen oder individuellen Verträgen zum Drittstaatentransfer (welche Stellen müssen ggf. den Vertrag als Datenexporteure abschließen?), für die Abstimmungen bzgl. verbindlicher Unternehmensregelungen und für die etwaige Genehmigungspflicht nach § 4c Abs. 2 BDSG (welche Stellen müssen eine Genehmigung beantragen?).
a) Zur Frage, ob datenexportierende Stellen grundsätzlich alle europäischen Stellen/ Niederlassungen sind oder nur eine oder einzelne der europäischen Stellen/ Niederlassungen, z.B. nur die europäische Konzernmutter oder die Europazentrale des Konzerns, als datenexportierende Stelle einzustufen ist, vertritt die Aufsichtsbehörde folgende Auffassung:

Maßgebliches Entscheidungskriterium für die Bestimmung des Datenexporteurs nach §§ 4b, 4c BDSG ist die tatsächliche Entscheidungsbefugnis im Hinblick auf den Datenexport in den Drittstaat. Grundsätzlich ist davon auszugehen, dass die Entscheidungsbefugnis beim jeweiligen Datenverarbeiter in Deutschland bzw. in dem EU/EWR-Staat verbleibt, von dem die Daten stammen. Sofern sich herausstellt, dass die Entscheidung im vorgenannten Sinne von einer (Haupt-) Niederlassung oder Konzernmutter zentral getroffen wird, ist nur sie übermittelnde Stelle im Sinne der §§ 4b, 4c BDSG. Als Faustregel ist also darauf abzustellen, wer "das Tor zum Datenexport öffnet". Die Unternehmen haben demnach darzulegen, ob die diesbezügliche Verantwortung auf mehrere/alle Niederlassungen verteilt ist oder ob sie bei nur einer Stelle liegt.

Die Aufsichtsbehörden haben im Falle eines deutschen Konzerns anerkannt, dass nur die Konzernmutter in Berlin als datenexportierende Stelle für den konzerninternen Datentransfer anzusehen ist, da sämtliche betroffenen personenbezogenen Daten von den europäischen Tochtergesellschaften in eine zentrale Datenbank bei der Konzernmutter übermittelt werden und diese ausschließlich über Inhalt und Umfang dieser Datenbank und vor allem über die Übermittlungen aus dieser Datenbank an die weltweiten Tochtergesellschaften/ Niederlassungen, u. a. in Drittstaaten, entscheidet.

Die gleiche Situation wurde vom betrieblichen Datenschutzbeauftragten eines Pharmakonzerns mit Sitz in Hessen vorgetragen, sodass nach der Abstimmung in der Arbeitsgruppe Internationaler Datenverkehr auch hier akzeptiert wurde, dass nur die hessische Muttergesellschaft als datenexportierende Stelle einzustufen ist. Dies hat in beiden Fällen die Konsequenz, dass die verbindlichen Unternehmensregelungen, mit denen der Datentransfer an Tochtergesellschaften in Drittstaaten ermöglicht werden soll, nach Auffassung der deutschen Aufsichtsbehörden keiner europaweiten Abstimmung

oder Genehmigung der jeweiligen Datenschutzaufsichtsbehörden in den EU-Ländern bedürfen, in denen die Tochtergesellschaften ansässig sind, sondern nur die Zuständigkeit der für die Konzernmutter zuständigen deutschen Aufsichtsbehörde gegeben ist. Ob die anderen europäischen Aufsichtsbehörden diese Auffassung teilen werden, bleibt abzuwarten.

In einem weiteren Fall, in dem das Regierungspräsidium Darmstadt um Beratung gebeten wurde, übermittelte eine zu einem US-Konzern gehörige GmbH mit Sitz in Hessen personenbezogene Daten von Mitarbeitern ihrer Kunden an die Europazentrale des Konzerns in London. Dort wurde entschieden, die Datenverarbeitung z. T. nach Singapur und die USA auszulagern. Die Entscheidung über die Datenübermittlung nach Singapur und in die USA wurde ausschließlich von der Europazentrale in London getroffen und auch von dieser durchgeführt. Die deutsche GmbH hatte keinerlei Einfluss hierauf (siehe zu dem Fall auch unter Ziff. 10.2). Auch hier bestand nach Abstimmung mit anderen Aufsichtsbehörden in Deutschland Einvernehmen, dass nur die Europazentrale in London datenexportierende Stelle ist. Diese hat also dafür zu sorgen, dass die Voraussetzungen des Artikels 25 bzw. 26 EG-DSRL bzw. der entsprechenden Vorschriften des britischen Datenschutzrechts für den Datentransfer nach Singapur und in die USA erfüllt sind. Die Datenschutzaufsicht obliegt der britischen Datenschutzaufsichtsbehörde.

In solchen Fällen muss jedoch die deutsche GmbH die Zulässigkeit der Datenübermittlung nach nationalem Recht (BDSG) überprüfen (1. Stufe). Im Rahmen der Abwägung mit den schutzwürdigen Interessen der Betroffenen, z. B. nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG, sind die rechtlichen Gegebenheiten aus englischer Sicht zu berücksichtigen, ob etwa ein Standardvertrag zwischen dem englischen Unternehmen und den Unternehmen in Singapur und den USA geschlossen wird. Diese 2. Stufe wird materiell-rechtlich erst durch das Londoner Unternehmen realisiert. Aber die deutsche GmbH darf nicht die Augen verschließen vor dem, was in London geschieht, sondern muss dies mit berücksichtigen, bevor sie Daten nach London übermittelt.

b) Im Zusammenhang mit den eingangs dargestellten Situationen stellt sich auch die Frage, ob rechtlich unselbständige Niederlassungen datenexportierende Stelle i. S. d. §§ 4b, 4c BDSG sein können. Diese Frage wurde bereits im 19. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden - Drs. 16/5892 - bejaht (siehe hierzu ausführlich unter Ziff. 11.2 des Berichts).

Die Arbeitsgruppe Internationaler Datenverkehr hat nun diese Auffassung einvernehmlich bestätigt. Das Gleiche gilt für die im letzten Tätigkeitsbericht in dem Zusammenhang dargestellte Auffassung zum Einsatz der EU-Standardvertragsklauseln zwischen einem Unternehmen im Drittstaat und der diesem zugehörigen unselbständigen Niederlassung in Deutschland.

Eine andere Frage ist, ob rechtlich unselbständige Niederlassungen Antragsteller und Adressaten eines Genehmigungsverfahrens nach Art. 26 Abs. 2 EG-DSRL (§ 4c Abs. 2 BDSG) sein können. Diese Frage wurde in der Arbeitsgruppe Internationaler Datenverkehr einhellig verneint. Wenn beispielsweise die rechtlich unselbständige deutsche Niederlassung eines französischen Unternehmens personenbezogene Daten in die USA transferiert, müsste die ggf. erforderliche Genehmigung an das französische Unternehmen und nicht an die unselbständige Niederlassung in Deutschland gerichtet werden.
Die sich aufgrund der Zuständigkeit der deutschen Behörden für die deutsche Niederlassung (§ 1 Abs. 5 Satz 1, letzter Halbsatz BDSG) ergebende Frage, ob diese Genehmigung nicht nur von der französischen Datenschutzaufsichtsbehörde, sondern auch von der deutschen Aufsichtsbehörde zu erteilen wäre, dürfte hypothetisch sein, denn in der Praxis dürfte es äußerst selten sein, dass die unselbständige Niederlassung überhaupt eigene Entscheidungskompetenzen bzgl. des Drittstaatentransfers hat. Nach Maßgabe der obigen Ausführungen zu a) dürfte nur das französische Unternehmen als datenexportierende Stelle einzustufen sein. Selbst wenn dies ausnahmsweise einmal anders sein sollte, erschiene es sachgerecht, nur eine Genehmigungszuständigkeit der für das rechtlich selbständige Unternehmen zuständigen Aufsichtsbehörde anzunehmen.

Wenn sich in Europa nur unselbständige Niederlassungen eines Unternehmens mit Sitz in einem Drittstaat befinden, ergibt sich eine besondere Problematik. Hier käme möglicherweise in Betracht, dass die ggf. erforderliche Genehmigung von dem zu bestellenden Inlandsvertreter (§ 1 Abs. 5 Satz 3 BDSG) beantragt und diesem zugestellt würde.

9.2 Arbeitsbericht der ad-hoc Arbeitsgruppe "Konzerninterner Datentransfer" – Auswirkungen bzw. Bedeutung und Umsetzung der Ergebnisse beim Drittstaatentransfer

Im Jahr 2004 hat sich eine ad-hoc-Arbeitsgruppe aus Vertretern der Aufsichtsbehörden und der Wirtschaft mit der Frage befasst, unter welchen Voraussetzungen der Austausch von Mitarbeiterdaten innerhalb eines Konzerns zulässig ist. Diese Arbeitsgruppe hat sich auf die Problematik der sog. 1. Stufe beschränkt, also die Fragen des Drittstaatentransfers (2. Stufe) ausgeklammert (siehe 18. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden - Drs. 16/4752 - unter Ziff. 10). Der vom Regierungspräsidium Darmstadt verfasste und mit den Teilnehmern abgestimmte Abschlussbericht ist von der Internetseite des Regierungspräsidiums Darmstadt abrufbar ("http://www.rp-darmstadt.hessen.de").

Die ad-hoc-Arbeitsgruppe kam zu dem Ergebnis, dass der Erlaubnistatbestand des § 28 Abs. 1 Satz 1 Nr. 2 BDSG bzw. des § 28 Abs. 3 Nr. 1 BDSG nur erfüllt sein kann, wenn folgende Voraussetzungen vorliegen:

- Die Übermittlung darf nicht dazu führen, dass andere Konzernunternehmen die Daten in einer Weise nutzen, die dem Arbeitgeber selbst verwehrt wäre.
- Die Übermittlung darf nur mit klarer Festlegung der Zweckbindung erfolgen und nur, wenn und soweit die personenbezogenen Daten für die von anderen Konzernunternehmen jeweils übernommene Funktion erforderlich sind.
- Der Konzern muss grundsätzlich besondere Maßnahmen ergreifen, um den Interessen der Betroffenen Rechnung zu tragen (Position der Aufsichtsbehörden). Dazu gehört
  - ein konzernweites Datenschutzkonzept,
  - dass das Arbeitgeber-Unternehmen - zusätzlich - umfassend datenschutzrechtlicher Ansprechpartner für seinen Arbeitnehmer bleibt, z.B. betreffend Schadensersatz, Auskunft etc.,
  - dass die entsprechenden Regelungen intern (im Konzern) und extern (gegenüber den Betroffenen) verbindlich sind.

Sofern diese Anforderungen im konkreten Fall einer Datenübermittlung gelten und diese Übermittlung in einen Drittstaat erfolgt, stellt sich die Frage, wie diese Anforderungen erfüllt werden können bzw. inwieweit es "Konflikte" mit den spezifischen Regelungen für den Drittstaatentransfer gibt.

Das Regierungspräsidium Darmstadt sieht hier folgende Möglichkeiten:

a) Betriebsvereinbarungen

Während Konzern-Betriebsvereinbarungen bei Datenübermittlungen innerhalb Deutschlands gut geeignet sind, die o. g. Anforderungen umzusetzen, sind sie beim Drittstaatentransfer insofern unzureichend, als die Konzernstellen im Drittstaat nicht per se daran gebunden sind. Wenn sich diese jedoch der Betriebsvereinbarung unterwerfen, können damit die o. g. Voraussetzungen erfüllt werden.

b) Standardvertrag vom 15. Juni 2001

Dieser Standardvertrag enthält Regelungen, die mit den o. g. Anforderungen korrespondieren. In Klausel 6 Abs. 2 ist die gesamtschuldnerische Haftung des Datenexporteurs und des Datenimporteurs vorgesehen. Nach Klausel 4d verpflichtet sich der Datenexporteur, Anfragen der betroffenen Personen bzgl. der Datenverarbeitung durch den Datenimporteur zu beantworten. Damit bleibt der Arbeitgeber, wenn er Datenexporteur ist, Ansprechpartner für den Betroffenen. Wesentliche der oben unter Punkt 3 genannten Anforderungen sind damit erfüllt. Anlage 2 Nr. 1 regelt die Zweckbindung, ebenso

Anlage 3 Nr. 1. Wenn beim Ausfüllen des Anhangs 1 die Zweckbestimmung und die Zugriffsbefugnisse detailliert geregelt werden, kann damit den o. g. Anforderungen unter Punkt 1 und 2 Rechnung getragen werden. Dies kann aber auch durch eine zusätzliche Betriebsvereinbarung geschehen, auf die im Anhang 1 Bezug genommen wird oder der sich der Datenimporteur separat unterwirft (s. o.). Selbstverständlich wäre auch eine gesonderte vertragliche Regelung möglich. Somit ist der Standardvertrag vom 15. Juni 2001, der ja an sich nur die Anforderungen der 2. Stufe betrifft, geeignet, zugleich wesentliche Anforderungen der 1. Stufe zu erfüllen. Grundsätzlich ist zu beachten, dass eine separate Betrachtung der beiden Stufen jedenfalls nicht zu einem Wertungswiderspruch führen darf. Beim Standardvertrag vom 15. Juni 2001 besteht eine solche Gefahr nur bzgl. der werblichen Nutzung und Verarbeitung von Arbeitnehmerdaten. Bei der Nutzung von Arbeitnehmerdaten zu Werbezwecken ist grundsätzlich eine Einwilligung erforderlich (1. Stufe), während der Standardvertrag vom 15. Juni 2001 nur ein Widerspruchsrecht (in Anlage 2 Nr. 8) bzw. gar keine Regelung (in Anlage 3, die nach Klausel 5 b alternativ zu Klausel 2 gewählt werden kann) enthält. Hier müsste daher entweder der Standardvertrag bzw. konkret die Anlagen entsprechend geändert oder eine Zusatzvereinbarung unter Berücksichtigung des Einwilligungserfordernisses geschlossen werden. Da eine entsprechende Änderung des Standardvertrags eindeutig zugunsten des Betroffenen erfolgen würde, entsteht nach Auffassung der Aufsichtsbehörde keine Genehmigungspflicht nach § 4c Abs. 2 BDSG für Datenübermittlungen auf dieser Grundlage. Bei der Aufsichtsbehörde ist aber zu erfragen, ob der geänderte Vertrag zur Prüfung im vorgenannten Sinne vorzulegen ist.

c) Standardvertrag vom 27. Dezember 2004 ("alternativer Standardvertrag")

Bei diesem Standardvertrag ist das Problem eines Wertungswiderspruchs in besonderem Maße gegeben: Nach Klausel III a besteht keine gesamtschuldnerische Haftung. Der Datenexporteur haftet grundsätzlich nur für die Schäden, die er verursacht hat. Klausel 1d sieht grundsätzlich keine Auskunftspflicht des Datenexporteurs bzgl. der Datenverarbeitung beim Datenimporteur vor. Nach Klausel III b kann der Betroffene seine Rechte grundsätzlich nur gegenüber dem Datenimporteur geltend machen, wenn er diesem eine Vertragsverletzung vorwirft. Diese Regelungen stehen im Widerspruch zu den o. g. Anforderungen.
Ein weiteres Problem ist auch hier, dass in Anhang A Nr. 7 nur ein opt-out (Widerspruchsrecht) beim Direktmarketing vorgesehen ist. Die Anerkennung der Standardverträge durch die EU-Kommission betrifft nur die 2. Stufe. Die Anforderungen der 1. Stufe (materielle Zulässigkeit nach nationalem Recht) dürften nicht durch den Abschluss von Regelungen auf der 2. Stufe umgangen werden. Dass auch die Europäische Kommission von der zweistufigen Prüfung bei Verwendung der Standardverträge ausgeht, ergibt sich aus den Erwägungsgründen (6) und (15) ihrer Entscheidung vom 15. Juni 2001. Falls die Prüfung der 1. Stufe ergibt, dass die eingangs genannten Anforderungen gelten, ist daher der Abschluss des Standardvertrags vom Dezember 2004 problematisch. Der Standardvertrag vom Juni 2001 wäre vorzuziehen. Gegebenenfalls ist nach Auffassung der Aufsichtsbehörde darüber nachzudenken, den alternativen Standardvertrag dergestalt zu ergänzen bzw. zu ändern, dass seine Verwendung für Arbeitnehmerdaten ermöglicht wird. Teilweise wird von Unternehmen vorgetragen, die dargestellte Problematik stelle sich nicht, weil sich bereits aus der Fürsorgepflicht des Arbeitgebers ergebe, dass er umfassend für Datenschutzverstöße einzustehen und Auskünfte zu erteilen habe. Allerdings ist die Reichweite der Fürsorgepflicht fraglich. Solange nicht durch fundierte arbeitsrechtliche Bewertungen belegt ist, dass sich die Fürsorgepflicht des Arbeitgebers auch auf datenschutzwidrige Verarbeitungen beim Datenimporteur erstreckt, kann die Aufsichtsbehörde daher dieser Argumentation nicht folgen. Aber selbst wenn dies belegt werden könnte, bliebe das Problem der Widersprüchlichkeit zu den Regelungen des alternativen Standardvertrags.

d) Safe Harbor

Die in Form von "häufig gestellten Fragen" (FAQ) gefassten Leitlinien zur Umsetzung der Safe Harbor-Grundsätze enthalten spezielle Ausführungen betreffend Personaldaten (FAQ 9). Hierin ist zur Frage der Rechtsdurchsetzung (F 4) ausgeführt, dass in erster Linie die in der EU ansässige Organisation verantwortlich bleibe, soweit Personaldaten nur im Rahmen des Beschäftigungsverhältnisses verwendet würden. Die Aufsichtsbehörde ist der Ansicht, dass diese Ausführungen nur deklaratorische Bedeutung und keine konstitutive Wirkung haben, also Rechte gegen den Arbeitgeber in Deutschland/der EU weder begründen noch beschränken können, sondern nur das Verständnis der US-Seite bzgl. des EU-Rechts wiedergeben. Die Aufsichtsbehörde sieht daher die Darlegungslast bezüglich der Arbeitnehmerrechte bzw. der eingangs dargestellten Anforderungen der 1. Stufe, die sicherzustellen sind, bei den Unternehmen (vgl. oben zu c).

9.3 Datenverarbeitungsdienstleistung in Deutschland für einen Auftraggeber im Drittstaat

Wenn ein in Deutschland ansässiger Datenverarbeitungsdienstleister (DV-Dienstleister) personenbezogene Daten im Auftrag eines in einem Drittstaat ansässigen Unternehmens verarbeitet, stellt sich die Frage, welche datenschutzrechtlichen Pflichten für diese beiden Unternehmen jeweils gelten. Insbesondere stellt sich die Frage, ob bei der Datenweitergabe durch den DV-Dienstleister in Deutschland an seinen Auftraggeber im Drittstaat die Anforderungen der §§ 4b, 4c BDSG gelten. Diese Problematik kann sich bei folgenden Fallgruppen ergeben:

A. Ein in Deutschland ansässiges Unternehmen beauftragt einen im Drittstaat ansässigen
DV-Dienstleister mit der Verarbeitung personenbezogener Daten und schließt mit diesem den Standardvertrag vom Dezember 2001 (Controller - Processor) oder einen entsprechenden individuellen Vertrag. Der DV-Dienstleister im Drittstaat schaltet einen DV-Dienstleister in Deutschland ein, welcher die Daten nach Erledigung des Auftrags an das Unternehmen im Drittstaat rücktransferiert.

B. Ein in Deutschland ansässiges Unternehmen übermittelt Daten an ein Unternehmen im Drittstaat und schließt mit diesem den Standardvertrag vom Juni 2001 oder Dezember 2004 (Controller – Controller) oder einen entsprechenden individuellen Vertrag. Das Unternehmen im Drittstaat schaltet einen DV-Dienstleister in Deutschland ein, welcher die Daten nach Erledigung des Auftrags an das Unternehmen im Drittstaat rücktransferiert.

C. Fallgestaltung wie B., aber zwischen dem in Deutschland ansässigen Unternehmen und dem Unternehmen im Drittstaat wird kein "Drittstaatenvertrag" nach § 4c Abs. 2 BDSG abgeschlossen, weil eine der Katalogausnahmen des § 4c Abs. 1 BDSG gegeben ist.

D. Ein in Deutschland ansässiger DV-Dienstleister wird von einem in einem Drittstaat ansässigen Unternehmen beauftragt, in Deutschland personenbezogene Daten zu erheben und zu verarbeiten und dann an den Auftraggeber im Drittstaat zu transferieren.

E. Ein in Deutschland ansässiger DV-Dienstleister wird von einem in einem Drittstaat ansässigen Unternehmen beauftragt, personenbezogene Daten zu verarbeiten und danach an den Auftraggeber zu transferieren. Die Daten stammen aus der EU/EWR, sie wurden hier entweder vom Auftraggeber selbst oder in dessen Auftrag von einem anderen DV-Dienstleister erhoben.

F. Fallgestaltung wie Buchst. E, aber die Daten stammen nicht aus der EU/EWR.

G. Fallgestaltung wie Buchst. A, B, C, E oder F, aber der EU/EWR Dienstleister erhält die Daten in verschlüsselter Form und kann von dem Inhalt keine Kenntnis nehmen (Black Box).

Nach § 1 Abs. 5 Satz 2 BDSG findet das BDSG Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Für die Verarbeitung durch den DV-Dienstleister in Deutschland gilt somit das BDSG. Der DV-Dienstleister ist jedoch grundsätzlich nur für die Datensicherheit der von ihm durchgeführten Datenverarbeitung verantwortlich (§ 11 i. V. m. § 9 BDSG, Art. 17 EG-DSRL). Im Übrigen ist jedoch der Auftraggeber im Drittstaat selbst verantwortlich. Er ist Adressat der übrigen Vorschriften. Der Auftragnehmer ist nicht verpflichtet, zu prüfen und sicherzustellen, dass beim Rücktransfer der Daten die Voraussetzung der §§ 4b, 4c BDSG erfüllt sind. Diese Vorschriften gelten für den Rücktransfer durch den Auftragnehmer nicht. Diese Auffassung ergibt sich aus folgenden Erwägungen: Würde man die Anwendbarkeit der §§ 4b, 4c BDSG bejahen, müsste der Auftragnehmer eine umfassende Prüfung der gesamten Datenverarbeitung vornehmen, also eine umfassende Prüfung des Zwecks der gesamten Datenverarbeitung sowie des Kontextes und der Umstände der Datenverarbeitung. Die bloße Vereinbarung mit dem Auftraggeber im Drittstaat, dass die Daten von jenem nur zu dem Zweck weiterverarbeitet werden dürfen, zu dem der Auftragnehmer die Daten erhalten hat, würde keinesfalls reichen. Eine Verantwortung nach §§ 4b, 4c BDSG würde vielmehr eine eigenständige umfassende Prüfung durch den Auftragnehmer erfordern.
Die Fallgruppen A - C sind dadurch gekennzeichnet, dass die Daten von einer verantwortlichen Stelle, die quasi der "Primär-Exporteur" ist, in die EU/EWR transferiert wurden und hierbei die Voraussetzungen des § 4c BDSG erfüllt wurden. Hier mag sich der DV-Dienstleister, der quasi der "Sekundär-Exporteur" ist, noch an dem vom "Primär-Exporteur" geschaffenen bzw. für diesen geltenden Zulässigkeitsrahmen orientieren können, falls sich seine DV-Dienstleistung im Rahmen der Zweckbestimmung des Primär-Exporteurs bewegt, was bei Fall A zutrifft, aber bei den Fällen B und C unklar sein kann. Andererseits bestehen folgende Probleme: Da bei Fallgruppe A Zweck und Umfang der zulässigen Datenverarbeitung, die einzuhaltenden Datensicherheitsmaßnahmen etc. bereits in dem Vertrag zwischen dem EU/EWR-Auftraggeber und dem Drittstaaten-Auftragnehmer geregelt sind, besteht für den EU/EWR-Unterauftragnehmer weder ein Erfordernis noch ein Spielraum für eigenständige Vorgaben gegenüber dem Drittstaatenunternehmen in Bezug auf die dortige Datenverarbeitung. Würde man einen individuellen - genehmigungsbedürftigen - Vertrag zwischen dem EU/EWR-Unterauftragnehmer für erforderlich halten, die Standardverträge würden ja nicht passen, dann würde dies sogar die Gefahr bergen, dass Regelungen getroffen werden, die dem Vertrag zwischen dem EU-Auftraggeber und dem Drittstaaten-Unternehmen widersprechen.

In den Fallgruppen C-G besteht zwar dieses Problem nicht, aber es dürfte für den DV-Dienstleister noch schwieriger sein, eine umfassende Prüfung i. S. d. §§ 4b, 4c BDSG vorzunehmen. Höchstwahrscheinlich kennt dieser nur einen kleinen Ausschnitt der Datenverarbeitung und des Verwendungszusammenhangs. Wie soll der DV-Dienstleister beispielsweise die Rechtmäßigkeit der Verarbeitung von Daten im Konzernzusammenhang beurteilen? Er kann im Unterschied zu den Fallgruppen A – C gerade nicht auf einen vorhandenen Regelungsrahmen verweisen oder Bezug nehmen. Daher muss man konstatieren, dass es letztlich in den allermeisten Fällen für den Auftragsverarbeiter in Deutschland (EU/EWR) unmöglich sein dürfte, eine umfassende Prüfung i. S. d. §§ 4b, 4c BDSG vorzunehmen, um beurteilen zu können, ob eine Katalogausnahme gegeben ist, oder um vertragliche Regelungen i. S. d. § 4c Abs. 2 BDSG treffen zu können. In Bezug auf etwaige vertragliche Regelungen i. S. d. § 4c Abs. 2 BDSG wäre im Übrigen völlig unklar, welche Pflichten der Auftragsverarbeiter hierin übernehmen sollte.

All dies zeigt, dass für den Rücktransfer durch den Auftragsverarbeiter in Deutschland die Regelungen der §§ 4b, 4c BDSG nicht gelten können. Hierfür spricht auch, dass nach § 3 Abs. 8 Satz 3 BDSG der Auftragnehmer in Deutschland nicht Dritter im Verhältnis zur verantwortlichen Stelle ist und somit keine Übermittlung i. S. d. § 3 Abs. 4 Nr. 3 BDSG stattfindet. Die Rückausnahme, die § 3 Abs. 8 Satz 3 BDSG selbst impliziert, dass nämlich Auftragnehmer außerhalb des EWR Dritte sind, greift nicht für den Auftraggeber im Drittstaat.

Da der Gesetzgeber in § 1 Abs. 5 BDSG der Stelle im Drittstaat selbst die umfassende Verantwortung für die Vereinbarkeit der Datenverarbeitung mit dem BDSG zugewiesen hat und nicht dem Auftragsverarbeiter, dessen sich der Auftraggeber im Drittstaat bedient, ist der Auftraggeber im Übrigen Adressat der "materiell-rechtlichen" Vorschriften; allerdings gelten auch für ihn nicht die §§ 4b, 4c BDSG. Dem Auftraggeber in Deutschland kann allenfalls eine Remonstrationspflicht entsprechend § 11 Abs. 3 Satz 2 BDSG sowie unter Umständen eine Pflicht zur materiellen Plausibilitätsprüfung in Bezug auf die von ihm selbst in Deutschland vorgenommenen Datenerhebungen, -verarbeitungen und -nutzungen obliegen. Konkret ergeben sich daraus folgende Konsequenzen:

a) Fallgruppe E

Die DV-Dienstleistung wird häufig in der Rechenzentrums-Dienstleistung bestehen, sodass eine inhaltliche Kenntnisnahme der Daten durch den Auftragsverarbeiter gar nicht vorgesehen ist. Der Auftragsverarbeiter hat lediglich für die Datensicherheit zu sorgen, er hat keine Prüfungspflicht bzgl. der Vereinbarkeit der Datenverarbeitung mit dem BDSG. Soweit ihm jedoch bekannt wird, z.B. aufgrund besonderer Hinweise Dritter, dass diese gegen das BDSG verstößt, hat er eine Remonstrationspflicht entsprechend § 11 Abs. 3 Satz 2 BDSG. In den Fällen, in denen der Auftraggeber einen gravierenden Missstand trotz Hinweises des Auftragsverarbeiters nicht abstellt, kann eine Hinweis- bzw. Anzeigepflicht des Auftragsverarbeiters gegenüber der Datenschutzaufsichtsbehörde angenommen werden. Ferner könnte ggf. die Pflicht des Auftragsverarbeiters bestehen, die weitere Ausführung des Auftrages einzustellen. Dann könnte die Aufsichtsbehörde entscheiden, wie weiter zu verfahren ist.

b) Fallgruppe D
Wenn der DV-Dienstleister die Daten selbst zu erheben hat, ist damit in aller Regel eine inhaltliche Kenntnisnahme der Daten verbunden. Daher hat der DV-Dienstleister summarisch auf Plausibilität zu prüfen, ob die Datenerhebung und -verarbeitung und die diesbezüglichen Weisungen des Auftraggebers mit dem BDSG vereinbar sind. Wenn nein, gelten die unter a) genannten Anforderungen.

c) Fallgruppe F
In Drittstaaten können bestimmte Verarbeitungen personenbezogener Daten explizit vorgeschrieben sein, die in Deutschland unzulässig wären, z.B. die Sozialversicherungsnummer. Zwar gilt das BDSG grundsätzlich unabhängig davon, ob die betroffenen Personen in Deutschland ansässig sind oder nicht. Allerdings wird mit der Sondervorschrift des § 1 Abs. 5 Satz 2 BDSG der reguläre Anwendungsbereich des BDSG ohnehin ausgedehnt, sodass hier eine Relativierung möglich erscheint. Ob der Gesetzgeber bzw. die EG-DSRL bei der Regelung des § 1 Abs. 5 Satz 2 BDSG (bzw. Artikel 4c EG-DSRL) einen "EU/EWR-Bezug" der Daten stillschweigend unterstellt hat, bleibt unklar. Die Lösung könnte darin bestehen, dass zwar aus § 1 Abs. 5 Satz 2 BDSG keine umfassende Geltung des deutschen Datenschutzrechts abzuleiten wäre, aber Verarbeitungen, die eindeutig gegen unseren "ordre public" verstoßen, z. B. bei Menschenrechtsverletzungen, unzulässig sind, auch wenn die Daten keinerlei EU/EWR-Bezug aufweisen. Demzufolge würde die ggf. bestehende Remonstrationspflicht des Auftragsverarbeiters (siehe oben 2a) grundsätzlich nur bei derartigen Verstößen bestehen.

d) Fallgruppen A - C
Hier gilt die obige Bewertung der Fallgruppen D bis G zunächst entsprechend, je nachdem in welcher Form der DV-Dienstleister in Deutschland die Daten erhält, woher die Daten stammen und welche konkrete Aufgabe der DV-Dienstleister hat. Obwohl die §§ 4b, 4c für seinen Rücktransfer der Daten in den Drittstaat nicht gelten, ist in den Fallgruppen A und B ein Beitritt des DV-Dienstleisters zu dem zwischen dem "Primärexporteur" und dem Unternehmen im Drittstaat geschlossenen Vertrag sinnvoll. Wenn zwischen dem Unternehmen im Drittstaat und dem DV-Dienstleister in Deutschland kein Vertrag existiert, durch den sichergestellt wird, dass die zwischen dem "Primärexporteur" in Deutschland getroffenen Regelungen zur Datenver-

arbeitung auch durch den DV-Dienstleister in Deutschland umgesetzt werden, kann diese Lücke durch einen Beitritt geschlossen werden.

9.4 Unterauftragnehmer im Drittstaat, der für Auftraggeber und deren Auftragnehmer mit Sitz in Deutschland tätig wird

Bereits vor einigen Jahren haben sich die Aufsichtsbehörden mit Fällen befasst, bei denen eine verantwortliche Stelle, die in Deutschland oder einem anderen Mitgliedsstaat der Europäischen Union oder des Europäischen Wirtschaftsraumes ansässig ist, die Datenverarbeitung auf einen ebenfalls in diesem Raum ansässigen Auftragsdatenverarbeiter ausgelagert hat und dieser dann seinerseits einen Unterauftragnehmer in einem Drittstaat einschaltet. Hier stellt sich insbesondere die Frage, wie der EU-Standardvertrag vom 27. Dezember 2001 zum Einsatz kommen kann. Der Abschluss eines Standardvertrags zwischen dem Auftragnehmer und dem Unterauftragnehmer wurde von den Aufsichtsbehörden als nicht sachgerecht bewertet, weil der Auftragnehmer, anders als der Datenexporteur in den Standardverträgen, nicht verantwortliche Stelle ist. Es bestand also Einigkeit, dass der Auftraggeber als Datenexporteur i. S. d. §§ 4b, 4c BDSG und der Unterauftragnehmer selbstverständlich als Datenimporteur einzustufen sind und diese daher Vertragsparteien des Standardvertrags vom Dezember 2001 sein müssen. Da wegen der möglichen Vielzahl von Auftraggebern entsprechend viele Standardverträge mit den Unterauftragnehmern abgeschlossen werden müssten, wurde es als praktikable Lösung angesehen und akzeptiert, dass der Auftragnehmer in Vertretung der Auftraggeber den Standardvertrag vom Dezember 2001 mit dem Unterauftragnehmer abschließt (siehe hierzu die ausführliche Darstellung im 16. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden - Drs. 16/1680 - Ziff. 8.3). Diese Bewertung der Aufsichtsbehörden gilt nach wie vor. Das Regierungspräsidium Darmstadt wurde jedoch bei entsprechender Beratung von Unternehmen auf die Problematik aufmerksam gemacht, dass bei Verwendung des Standardvertrags vom 27. Dezember 2001 und einer Verfahrensweise wie von den Aufsichtsbehörden gefordert, die EU-Auftragnehmer gar nicht als Vertragspartei in den Standardvertrag einbezogen werden und insoweit also weder Rechte noch Pflichten haben. Dies entspricht aber nicht den wirtschaftlichen Realitäten bzw. Interessenlagen. Auch in datenschutzrechtlicher Hinsicht ist es nach Auffassung des Regierungspräsidiums Darmstadt unbefriedigend, dass der EU-Auftragnehmer keinerlei Verpflichtungen bzgl. des Drittstaatentransfers hat, sondern nur beim Abschluss des Standardvertrags als Stellvertreter seines/seiner Auftraggeber(s) auftritt. Datenschutzrechtliche Pflichten der EU-Auftragnehmer müssen sich zwar aus den Verträgen mit den Auftraggebern ergeben. Allerdings sind die EU-Auftragnehmer in dem speziell den Drittstaatentransfer betreffenden Standardvertrag quasi "außen vor gelassen". Aufgrund dieser Inkongruenz der vertraglichen Regelungen können sich Probleme ergeben, sodass die effektive Umsetzung des Standardvertrags möglicherweise nicht gewährleistet ist. Daher erscheint es nach Auffassung des Regierungspräsidiums Darmstadt sachgerecht, dass auch die EU-Auftragnehmer dem Vertrag beitreten.
In der Arbeitsgruppe Internationaler Datenverkehr bestand Einigkeit, dass ein solcher Beitritt jedenfalls sinnvoll ist.

Folgender Text kann für einen Beitritt verwendet werden: "Die vorstehenden Regelungen gelten mit folgender Maßgabe auch für den DV-Dienstleister in Europa [Name, Sitz], der insoweit dem Vertrag beitritt. Da der Datenexporteur einen Datenverarbeitungsdienstleistungsvertrag mit [Name des DV-Dienstleisters in Europa] geschlossen hat (als Auftragsdatenverarbeitung nach § 11 BDSG / Art. 2e, 17 Abs. 3 EG-Datenschutzrichtlinie 95/46/EG und den hierzu erlassenen nationalen Vorschriften) und der Datenimporteur als "Unterauftragnehmer" (oder: Subunternehmer) für [Name des DV-Dienstleisters in Europa] fungiert, ist der/die [Name des DV-Dienstleisters in Europa] gegenüber dem Datenexporteur primär verantwortlich, dass der Datenimporteur die Pflichten gemäß diesem Vertrag erfüllt. Der/die [Name des DV-Dienstleisters in Europa] hat zu diesem Zweck entsprechende abgeleitete Kontrollpflichten gegenüber dem Datenimporteur und kann hierfür die in diesem Vertrag beschriebenen Kontrollbefugnisse des Datenexporteurs wahrnehmen. Dieser bleibt verpflichtet, die Ausübung der Kontrollbefugnisse zu überwachen und kann jederzeit auch selbst diese Kontrolle gegenüber dem Unterauftragnehmer ausüben."

Ein solcher Vertragsbeitritt löst keine Genehmigungspflicht nach § 4c Abs. 2 BDSG aus.

10. Arbeitnehmerdatenschutz

10.1 Whistleblowing

Unter Whistleblowing versteht man Meldungen über tatsächliches oder vermeintliches Fehlverhalten, z. B. Korruption, Betrug, sonstige Rechtsverstöße oder Verstöße gegen Ethikrichtlinien, innerhalb des Unternehmens durch einen Arbeitnehmer. Mit der Einrichtung von Whistleblowing-Hotlines soll den Mitarbeitern ermöglicht werden, über einen bestimmten Informationsweg Hinweise auf interne Missstände zu geben.

Eine besondere Bedeutung gewonnen haben Whistleblowing-Systeme durch den US-amerikanischen Sarbanes-Oxley Act von 2002, wonach US-Aktiengesellschaften und ihre Unternehmenseinheiten außerhalb der USA sowie nicht-US-Unternehmen, die an einer US-Börse notiert sind, Verfahren zur Entgegennahme, Speicherung und Bearbeitung von Beschwerden in Bezug auf Rechnungslegung, interne Rechnungslegungskontrollen und Wirtschaftsprüfungsfragen einführen müssen.

Die mit der Meldung von Verstößen einhergehende Erhebung, Speicherung und Übermittlung von personenbezogenen Daten, insbesondere der Hinweisgeber und der Beschuldigten, stößt auf nicht unerhebliche datenschutzrechtliche Probleme. Die Artikel-29-Datenschutzgruppe der EU-Mitgliedstaaten hat in ihrer Stellungnahme 1/2006 (WP 117) Leitlinien zum datenschutzkonformen Einsatz von Whistleblowing-Systemen vorgegeben. Es handelt sich hierbei allerdings noch nicht um eine umfassende Stellungnahme zur Meldung von Missständen im Allgemeinen. Die Gruppe hat sich zunächst auf die vom Sarbanes-Oxley-Act erfassten Bereiche beschränkt. Hier sah man wegen des auch für EU-Unternehmen bestehenden Sanktionsrisikos den dringendsten Handlungsbedarf, durch entsprechende Leitlinien zu gewährleisten, dass die Umsetzung interner Meldeverfahren in den Unternehmen unter Beachtung der EU-Datenschutzvorschriften erfolgt.

Im Frühjahr 2006 hat sich die ad hoc-Arbeitsgruppe "Beschäftigtendatenschutz" des Düsseldorfer Kreises mit der Thematik befasst. Der Arbeitsbericht "Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz" befindet sich noch in der Abstimmung.

Das Regierungspräsidium Darmstadt beschäftigte sich im Berichtsjahr bei verschiedenen Gelegenheiten mit dem Thema Whistleblowing. Es beriet mehrfach betriebliche Datenschutzbeauftragte in dieser Frage. Eine Mitarbeiterin der Aufsichtsbehörde hielt zu der Thematik auch einen Vortrag bei einer Informationsveranstaltung (vgl. Ziff. 2.2).

10.2 Verarbeitung von Arbeitnehmerdaten in Zusammenhang mit der Erbringung von Finanzdienstleistungen

Ein internationaler Konzern für Finanzdienstleistungen mit Sitz in London hat seinen Kunden vertraglich zugesichert, rund um die Uhr mit dem Support Kontakt aufnehmen zu können. Anrufe über eine Service-Hotline werden tagsüber von Mitarbeitern an Helpdesks in England und der Schweiz, ab 20:00 Uhr in den USA bzw. Singapur angenommen. Um eine optimale Kundenbetreuung zu gewährleisten, werden die Daten der Endnutzer (Mitarbeiter der Kunden) in einer zentralen Datenbank in London gespeichert und sind von jedem Helpdesk aus einsehbar, damit von dort aus ein direkter Kontakt zu den Mitarbeitern möglich ist.

Eine in Hessen ansässige Tochtergesellschaft des Unternehmens verlangte von allen Mitarbeitern ihrer Vertragspartner, eine konzernweit eingesetzte Einwilligungserklärung zu unterschreiben. Die Einwilligung erstreckte sich sowohl auf die Verwendung der Daten für den Support, einschließlich des Datentransfers in Drittstaaten, als auch auf deren Nutzung zu Marketing-Zwecken.

Aufgrund von Anfragen bzw. Eingaben verschiedener Vertragspartner des Unternehmens hat sich die Aufsichtsbehörde eingehend mit der Thematik befasst und ihre datenschutzrechtlichen Bedenken gegenüber dem Unternehmen dargelegt.

Es bestanden generelle Zweifel an der Rechtswirksamkeit der Einwilligungserklärung, da eine Freiwilligkeit (§ 4a Abs. 1 BDSG) aufgrund des Arbeitsverhältnisses zweifelhaft war, soweit es um die Verwendung der Mitarbeiterdaten im Rahmen der vereinbarten Dienstleistung ging. Die Aufsichtsbehörde sah insoweit ohnehin keine Notwendigkeit für eine Einwilligung, da das Erheben, Verarbeiten und Nutzen der Daten im Rahmen der Zulässigkeitsvoraussetzungen von § 28 Abs. 1 Nr. 1 und Nr. 2 BDSG erfolgt und sich hierauf zu beschränken hat. Die Aufsichtsbehörde vertrat weiterhin die Auffassung, dass eine weitergehende Datennutzung zu Marketing-Zwecken zunächst in der alleinigen Entscheidungskompetenz des jeweiligen Arbeitgebers liegt. Der Arbeitgeber muss die Möglichkeit haben, diese Nutzung im Dienstleistungsvertrag mit dem Finanzdienstleister auszuschließen. Für den Fall, dass der Arbeitgeber eine werbliche Ansprache am Arbeitsplatz nicht ausgeschlossen hat, muss der Anwender dann die Wahl haben, in die Nutzung seiner Daten zu Marketing-Zwecken einzuwilligen oder diese Einwilligung zu verweigern.

Zunächst wurden seitens der Aufsichtsbehörde Verhandlungen mit dem Datenschutzbeauftragten des deutschen Tochterunternehmens geführt, mit dem bereits eine weitgehende Einigung über die künftige Verfahrensweise erzielt werden konnte. Da sowohl von dem Unternehmen selbst als auch von mehreren seiner Vertragspartner der Wunsch geäußert wurde, die künftige Praxis wegen der grundsätzlichen Bedeutung in einem größeren Kreis mit Vertretern der Unternehmenskunden und weiteren Aufsichtsbehörden abzustimmen, fand auf Einladung des Regierungspräsidiums Darmstadt im Juni 2006 eine Besprechung zu dieser Thematik statt.

Nach dem Ergebnis der Gespräche zwischen der Aufsichtsbehörde und dem Unternehmen sowie der anschließenden Abstimmung wird in Zukunft auf eine Einwilligungserklärung der Endnutzer bzgl. der Datenverarbeitung im Rahmen des Support verzichtet. Eine Datenerhebung und -nutzung erfolgt nur in dem zur Erfüllung der vertraglich vereinbarten Leistungen erforderlichen Umfang. Die Mitarbeiterdaten werden dem Unternehmen von dem jeweiligen Vertragspartner im Rahmen der Zulässigkeitsvoraussetzungen des § 28 Abs. 1 Nr. 1 und 2 BDSG übermittelt. Die bestehenden Informationspflichten wird der Finanzdienstleister in Zusammenarbeit mit dem jeweiligen Arbeitgeber dergestalt erfüllen, dass jeder Mitarbeiter einen von dem Datenschutzbeauftragten des Unternehmens entworfenen und mit den Besprechungsteilnehmern abgestimmten Datenschutzhinweis erhält.

Für den Fall, dass seitens des Arbeitgebers eine werbliche Nutzung der Daten nicht ausgeschlossen wird, erhalten die Mitarbeiter darüber hinaus den Text einer Einwilligungserklärung. Mit seiner Unterschrift stimmt der einzelne Mitarbeiter zu, dass der Finanzdienstleister ihm Werbung zu seinen Produkten zukommen lässt einschließlich der Angebote, neue Dienstleistungen zu testen oder an Kundenveranstaltungen teilzunehmen. Für diese Verarbeitung und Nutzung wurde die Einwilligungslösung von allen an der Besprechung teilnehmenden Aufsichtsbehörden und von der überwiegenden Mehrheit der übrigen Teilnehmer als notwendig erachtet, da der Datenkatalog, der genutzt wird, über das Listenprivileg hinausgeht und außerdem Telefon-, Fax- und E-Mail-Werbung vorgesehen ist. Der Mitarbeiter muss entscheiden können, ob er Werbung erhalten will oder nicht.

Etwas anderes kann nur gelten, wenn der Arbeitgeber die Entgegennahme dieser Werbung und ggf. die Befassung damit als Bestandteil der vom Arbeitnehmer zu erbringenden Arbeitsleistung ansieht und so als arbeitsvertragliche Pflicht gestaltet. Dies dürfte allerdings nicht die Regel sein. Vielmehr ist es in der Regel nur die Aufgabe eines oder mehrer spezieller Mitarbeiter, sich mit der Beschaffung neuer Produkte zu beschäftigen.
Es ist dem einzelnen Arbeitgeber aber nicht verwehrt, die Arbeitsinhalte anders zu definieren, insbesondere wenn er von den Erfahrungen aller Mitarbeiter, auch zu neuen Produktangeboten, profitieren will, sodass § 28 Abs. 1 Nr. 1 BDSG die Rechtsgrundlage wäre.

Vom Grundsatz her hält die Aufsichtsbehörde aber ein Festhalten an der Einwilligungslösung für angezeigt, soweit es um die Verwendung der Daten für werbliche Zwecke geht.

Im Zusammenhang mit der Datenübermittlung innerhalb des Finanzdienstleistungskonzerns wurde auch die Problematik des Drittstaatentransfers erörtert. Da sich die zentrale Datenbank in London befindet und die Entscheidungsbefugnis bezüglich der Helpdesks und der diesbezüglichen Datenübermittlungen nach USA und Singapur ausschließlich bei der Konzernzentrale in London liegt, ist nur diese datenexportierende Stelle i. S. d. Art. 25, 26 EG-DSRL, nicht aber das in Hessen ansässige Tochterunternehmen (vgl. auch Ziff. 9.1 a).

Für den Drittstaatentransfer wäre somit britisches Recht anwendbar. Davon ausgehend, dass dieses Regelungen enthält, die Art. 25, 26 EG-DSRL (§§ 4b, 4c BDSG) entsprechen, gelangte die Aufsichtsbehörde zu der Auffassung, dass die Ausnahmetatbestände des Art. 26 Abs. 1 a), b) und c) EG-DSRL (§ 4c Abs. 1 Nr. 1, 2 und 3 BDSG) nicht vorliegen. Die derzeitigen Datenschutzregelungen des Unternehmens bieten keine ausreichenden Garantien für ein angemessenes Datenschutzniveau, da u. a. Regelungen zur Verbindlichmachung fehlen.

Obwohl der betriebliche Datenschutzbeauftragte der deutschen Unternehmenstochter anlässlich der Besprechung versicherte, dass die für den Gesamtkonzern bestellte Datenschutzbeauftragte bereits mit der Erarbeitung verbindlicher Unternehmensregelungen befasst sei, liegen der Aufsichtsbehörde bislang keine entsprechende Informationen vor. Die Erfüllung dieser Verpflichtung wurde angemahnt. Ggf. wird sich die Aufsichtsbehörde mit der britischen Datenschutzaufsichtsbehörde in Verbindung setzen.

11. Fußball WM 2006

11.1 Ticketing-Verfahren

Seit Sommer 2004 war das Regierungspräsidium Darmstadt mit der Klärung von Fragen des Datenschutzes bei der Fußball-WM 2006 beschäftigt (vgl. 18. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden - Drs. 16/4752 - Ziff. 11 und 19. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden - Drs. 16/5892 - Ziff.16).

Wie bereits in den Vorjahren umfassend dargestellt, wurde im Rahmen des Ticketings (Kartenverkauf und Einlasskontrolle bei Besuch der Stadien) ein sehr komplexes IT-System eingesetzt, bei dem verschiedenste Dienstleister des Deutschen Fußball-Bundes als Auftragsdatenverarbeiter nach § 11 BDSG beteiligt waren. Dabei handelte es sich u. a. um Datenerfasser, Web-Seiten-Verwalter, die beiden Ticketing-Vertriebspartner mit deren Subunternehmen und Rechenzentren sowie die einzelnen Stadionbetreiber. Im Berichtsjahr wurden vom DFB noch ausstehende Verträge nach § 11 BDSG und die erforderlichen Weisungen in Schriftform verfasst und von der Aufsichtsbehörde überprüft.

Bezüglich der unterschiedlichen Zugangskontrollsysteme und der jeweiligen Implementierung in die Stadionrechner mussten die entsprechenden Betriebskonzepte für die WM-Stadien vorgelegt werden. Die für die Stadien zuständigen Datenschutzaufsichtsbehörden bzw. Landesbeauftragten für den Datenschutz wurden vom Regierungspräsidium Darmstadt zu einer gemeinsamen Besprechung mit dem DFB eingeladen, um Informationen auszutauschen und die Prüfungen in den Stadien vorzubereiten und zu koordinieren.

Bei allen beteiligten datenverarbeitenden Stellen (Organisationskomitee des DFB und von diesen beauftragte Unternehmen) fanden zahlreiche Überprüfungen vor Ort statt. Dabei wurden die Datenflüsse, die Zugriffskontrolle und alle Maßnahmen zur Datensicherheit intensiv überprüft. Insgesamt wiesen die technisch-organisatorischen Maßnahmen zur Datensicherheit einen hohen Standard auf. Gewisse Änderungen, z. B. im Rahmen des Zugriffkonzeptes und dessen Verwaltung, wurden auf Anregung der Aufsichtsbehörde aufgenommen und umgesetzt. In bestimmten Bereichen musste der

zugriffsberechtigte Personenkreis auf Anregung der Aufsichtsbehörde eingeschränkt werden. Auch diese Maßnahmen wurden umgehend umgesetzt.

Bei einer Prüfung im Frankfurter Stadion gab das Regierungspräsidium Darmstadt einer Mitarbeiterin des Hessischen Datenschutzbeauftragten Gelegenheit, die Aufsichtsbehörde zu begleiten. Im 35. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten - Drs. 16/6929, Ziff. 4.3 - befindet sich dazu eine ausführliche Darstellung, auf die hier verwiesen sei.

Eine werbliche Nutzung der im Rahmen des Ticketings erhobenen personenbezogenen Daten erfolgte auch im Berichtsjahr nicht, wie eine entsprechende Prüfung ergab. Nach Abschluss der Fußballweltmeisterschaft kann somit eine werbliche Nutzung ausgeschlossen werden, obwohl sie bei Personen, die hierzu ihre Einwilligung gegeben hatten, zulässig gewesen wäre.

Ferner wurde die datenschutzrechtlich vorgegebene fristgerechte Datenlöschung überprüft. Die Nachweise wurden eingefordert und vor Ort geprüft.

11.2 Akkreditierungsverfahren

Auch das Akkreditierungsverfahren war Anlass einer intensiven Überprüfung beim Organisationskomitee der Fußball WM. Dabei wurde die für Sammelakkreditierungsanträge von Unternehmen und anderen Stellen datenschutzrechtlich geforderte Erklärung der Supervisoren (siehe 18. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden - Drs. 16/4752 - Ziff. 11.2.2) auf deren Vollständigkeit und richtige Unterzeichnung geprüft. Stichprobenhafte Überprüfungen fanden bei den jeweiligen Stellen statt und führten zu keiner Beanstandung. Darüber hinaus erfolgte eine Beteiligung der Datenschutzaufsichtsbehörden und Landesdatenschutzbeauftragten anderer Bundesländer, damit diese entsprechende Vorortkontrollen in deren Zuständigkeitsbereich vornehmen konnten.

Hinsichtlich der im Frankfurter Stadion durchgeführten Überprüfungen zum Akkreditierungsverfahren wird ebenfalls auf die Darstellung im 35. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten - Drs. 16/6929, Ziff. 4.3 - verwiesen.

12. Tele- und Mediendienste

12.1 Unzulässige Inverssuche mit Platzhaltern auf einer Telefon-CD

Anlässlich der Überprüfung eines auf einer CD enthaltenen öffentlichen Verzeichnisses von Fernsprechteilnehmern musste das Regierungspräsidium Darmstadt feststellen, dass die Herausgeber der Telefon-CD die seit der Novellierung des Telekommunikationsgesetzes (TKG) im Jahr 2004 nach § 105 Abs. 3 TKG zulässige Inverssuche (Rückwärtssuche nach Namen und Anschrift des Teilnehmers bei bekannter Telefonnummer) um eine neue Funktion erweitert hatten. Das Menü der CD bot die Möglichkeit, mittels Platzhaltern (? oder *) auch bei nur teilweise bekannten Rufnummern eine Suche über den Datenbestand der CD durchzuführen. Als Suchergebnis wurde bei diesen so genannten Joker-Abfragen eine Liste mit Rufnummern und ggf. auch mit den Anschriften aller Teilnehmer ausgeworfen, für die der angegebene Suchbegriff zutraf.

Die Bewertung dieser neuen Funktion durch die Datenschutzaufsichtsbehörde war eindeutig. Das Angebot einer Inverssuche mit Platzhaltern (Jokerzeichen) für elektronische Teilnehmerverzeichnisse verstößt gegen geltendes Datenschutzrecht. Anbieter einer Telefon-CD, die eine Suchfunktion der Inverssuche mit Platzhaltern beinhaltet, verstoßen gegen § 29 Abs. 4 i. V. m. § 28 Abs. 5 BDSG, da die Verarbeitung oder Nutzung von übermittelten Daten einer strengen Zweckbindung unterliegt.

Der Übermittlungszweck ergibt sich vorliegend aus § 47 Abs. 1 TKG. Telekommunikationsunternehmen sind danach verpflichtet, unter Beachtung der anzuwendenden datenschutzrechtlichen Regelungen jedem Unternehmen auf Antrag Teilnehmerdaten zum Zwecke der Bereitstellung von öffentlich zugänglichen Telefonverzeichnissen zur Verfügung zu stellen. Diese Daten

dürfen aber nur zur Direkt- oder Inversauskunft nach § 105 TKG genutzt werden. Nach dem Wortlaut des § 105 Abs. 3 TKG muss die Rufnummer des gesuchten Teilnehmers bei der Inverssuche "bekannt" sein. Daraus folgt, dass für die Inverssuche immer die vollständige Rufnummer vorliegen muss. Diese Auffassung wird ergänzend durch die Vorschrift des § 112 Abs. 1 Nr. 2 TKG gestützt, worin eine gesetzliche Regelung für die Inverssuche mit Platzhaltern geschaffen wurde, welche diese den Sicherheitsbehörden vorbehält. Im Ergebnis werden somit, wenn eine Inverssuche mit Platzhaltern angeboten wird, die personenbezogenen Daten entgegen §§ 29 Abs. 4 i. V. m. 28 Abs. 5 BDSG durch die Herausgeber des Telekommunikationsverzeichnisses verarbeitet und diese zweckfremde Verarbeitung an die Personen übermittelt, die die entsprechenden Verzeichnisse auf CDs erwerben. Die Datenübermittlung an diese Dritten erfolgte mangels einer gesetzlichen Grundlage in unbefugter Weise und erfüllt damit den Tatbestand einer - zumindest fahrlässig begangenen - Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 5 BDSG.

Die Rechtsauffassung des Regierungspräsidiums Darmstadt wurde von der Arbeitsgruppe Telekommunikation, Tele- und Mediendienste bestätigt und so mit den obersten Aufsichtsbehörden der Bundesländer für den Datenschutz im nicht öffentlichen Bereich abgestimmt. Da die Anbieter der Telefon-CD sich dieser Rechtsauffassung nicht sofort anschließen wollten, wurden wegen des starken TKG-Bezugs des Sachverhalts auch der Bundesbeauftragte für den Datenschutz und die Bundesnetzagentur um Stellungnahmen gebeten, die nach § 115 Abs. 4 TKG als Aufsichtsbehörden für Telekommunikationsanbieter zuständig sind. Beide Dienststellen stimmten mit der Datenschutzaufsichtsbehörde überein, dass die Joker-Inverssuche den Rahmen der durch das TKG gesetzten Zweckbindung überschreitet und daher unzulässig ist.

Die Herausgeber der Telefon-CD konnten aber dennoch leider erst durch die Androhung eines Bußgeldverfahrens nach § 43 Abs. 2 Nr. 5 BDSG umgestimmt werden und sagten zu, die Inverssuche mit Platzhaltern von künftigen Telefonverzeichnis-CDs zu entfernen. Das Regierungspräsidium Darmstadt wird diese Zusage anhand der im Handel befindlichen Telefon-CDs überprüfen.

12.2 Mangelnde Sorgfalt beim Versenden von E-Mails an einen großen Empfängerkreis

Mehrfach wurden der Datenschutzaufsichtsbehörde im Berichtsjahr von Bürgerinnen und Bürgern empfangene E-Mails vorgelegt, in denen in den offen lesbaren Adressierfeldern "An" oder "cc" die E-Mail-Adressen sämtlicher Empfänger dieser Massen-E-Mails aufgeführt waren. Teilweise wurden dabei hunderte von personenbezogenen E-Mail-Adressen offen lesbar angegeben. Diese Fälle waren nicht branchen- oder themenspezifisch, sondern betrafen den Newsletter-Versand eines Online-Shops genauso wie z. B. die Zahlungserinnerungen eines PC-Versandhändlers, die Fachinformationen eines wissenschaftlichen Fördervereins und die Kundeninformationen eines Telekommunikations-Providers.

In allen Fällen wurden die für den E-Mail-Versand verantwortlichen Stellen darauf hingewiesen, dass das Aufführen der E-Mail-Adressen aller Empfänger in den offen lesbaren Feldern "An" oder "cc" dazu führt, dass alle diese E-Mail-Adressen allen E-Mail-Empfängern bekannt gegeben werden. Aus datenschutzrechtlicher Sicht handelte es sich dabei in jedem Einzelfall um die Übermittlung personenbezogener Daten, die jeweils nicht erforderlich war, also ohne Rechtsgrundlage erfolgte und damit datenschutzrechtlich unzulässig war.

Zusätzlich werden ganz unabhängig von der datenschutzrechtlichen Unzulässigkeit solcher Übermittlungen durch diese Adressiervarianten die E-Mail-Adressen der Empfänger einer kaum einschätzbaren Gefährdung durch Schadprogramme ausgesetzt. Wenn z. B. auch nur ein einziger der E-Mail-Empfänger nicht über einen aktuellen Virenschutz verfügt, kann ein entsprechendes Schadprogramm auf seinem PC die mit der Massen-E-Mail übermittelten Daten zur eigenen Weiterverbreitung oder zur Fälschung der Absenderangaben entsprechender Trojaner-E-Mails nutzen.

Hinzu kommt noch die Gefahr, dass andere E-Mail-Empfänger die erhaltenen E-Mail-Adressen ebenfalls für unverlangte Werbe-E-Mails nutzen und die hohe Zahl der eingehenden E-Mails zur Funktionsunfähigkeit eines E-Mail-Accounts führen kann. Z. B. erhielt in einem vom OLG Düsseldorf entschiedenen Fall ein Rechtsanwalt in Folge des ersten E-Mail-Empfangs, in der alle Empfänger im "An" offen erkennbar waren, innerhalb weniger Tage noch ca. 2000 weitere unverlangte E-Mails, was das Gericht in seinem Urteil vom 24.05.06 (Az.: I-15 U 45/06) auf das sorgfaltswidrige Verhalten des ursprünglichen Versenders der Massen-E-Mail zurückführte.

Alle zur Stellungnahme zum dargestellten Sachverhalt aufgeforderten Unternehmen erklärten die unzulässige Versendeform mit im Einzelfall aufgetretenen menschlichen Fehlern. Die jeweiligen Mitarbeiter hätten die notwendige Sorgfalt vermissen lassen und sich nicht an die durchaus existierenden betrieblichen Vorgaben gehalten, Massen-E-Mails nur als Blindkopie über das Feld "bcc" oder über eigens dafür angelegte nicht offen lesbare E-Mail-Verteiler zu versenden. Alle Stellen sagten zu, ihre Mitarbeiter bzw. die Mitarbeiter der für den E-Mail-Versand eingesetzten Dienstleistungsunternehmen entsprechend zu schulen und so auch für die möglichen Probleme zu sensibilisieren, die durch solche Versehen auftreten können.

Sämtliche Vorfälle wurden ausdrücklich beanstandet mit dem Hinweis, dass die Einleitung eines Bußgeldverfahrens nach § 43 Abs. 2 Nr. 1 BDSG i. V. m. § 9 OWiG gegen die Geschäftsführung des Unternehmens geprüft werden wird, falls sich ein solcher Vorfall wiederholen sollte. Da sich alle betroffenen Stellen einsichtig zeigten und geeignete Maßnahmen einleiteten, die hinreichend sicherstellen, dass solche Fehler künftig nicht mehr auftreten werden, konnte die Datenschutzaufsichtsbehörde bislang auf bußgeldrechtliche Sanktionen verzichten.

Grundsätzlich gilt, dass sich E-Mails mit offen gelegten E-Mail-Adressen oder für alle Empfänger offen lesbaren E-Mail-Verteilern nur für geschlossene Benutzergruppen, z. B. innerhalb eines Unternehmens, eignen und ansonsten nur als Blindkopie ("bcc") verschickt werden dürfen.

13. Werbewirtschaft

Kundenempfehlungsprogramm über das Internet

Mit der datenschutzkonformen Ausgestaltung von Kundenempfehlungsprogrammen hatte sich die Aufsichtsbehörde zu befassen, nachdem ein Kreditinstitut beabsichtigte, ein bereits bestehendes Verfahren zur Kundenwerbung mit neuen Elementen zu beleben.

Bislang stellte das Unternehmen auf seiner Internetseite ein Formular zur Verfügung, das sich Bankkunden ausdrucken konnten, um Personen aus ihrem Bekanntenkreis als potentielle Neukunden zu empfehlen. Der Vordruck enthielt Angaben zum Empfehler, dessen Wunschprämie und die Kontaktdaten des Interessenten, wobei die Nennung der Telefonnummer freigestellt blieb. Durch Hinweise zu den Teilnahmebedingungen, zur Zweckbestimmung der Datenerhebung, der Speicherdauer und zum Widerspruchsrecht erfolgte eine umfassende Information der Interessenten, deren Zustimmung zur Teilnahme am Empfehlungsprogramm schließlich durch Unterschrift bestätigt wurde.

Vorgesehen war nun, den Werbern die Möglichkeit zu geben, das Formular direkt am PC auszufüllen und dem Kreditinstitut auf elektronischem Weg zukommen zu lassen. Die Interessenten sollten später per Brief darüber informiert werden, dass sie als Kunde empfohlen wurden und eine Einladung zu einem Beratungsgespräch erhalten. In dem Schreiben sollte auch ein Datenschutzhinweis und ein Hinweis zum Widerspruchsrecht enthalten sein.

Bei der datenschutzrechtlichen Erörterung mit dem Kreditinstitut wurde zunächst festgestellt, dass bei dem "Altverfahren" eine frühestmögliche Einbindung des Interessenten erfolgt und die Entscheidung, ob es überhaupt zu einer Speicherung von personenbezogenen Daten kommt, beim Betroffenen verbleibt, da die Verarbeitung erst durch eine Unterschrift legitimiert wird. Damit wird dem in § 4 Abs. 2 BDSG normierten Grundsatz der Di-

rekterhebung Rechnung getragen und durch Kenntnis- und Mitwirkungsmöglichkeiten den betroffenen Personen ein transparentes Verfahren angeboten.

Das "Neuverfahren" ließ eine solch eindeutig günstige Beurteilung aus datenschutzrechtlicher Sicht im Hinblick auf die Schutzwürdigkeit der Interessen Betroffener zunächst nicht mehr zu, da die Erhebung der Interessentendaten nunmehr ohne Mitwirkung der potentiellen Neukunden erfolgen sollte.

Nach § 4 Abs. 2 Satz 2 Nr. 1, 1. Alt. BDSG dürfen personenbezogene Daten ohne Mitwirkung des Betroffenen nur erhoben werden, wenn eine Rechtsvorschrift dies vorsieht. Als solche Rechtsvorschrift kam vorliegend allenfalls § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht, wodurch die Verwendung der Daten unter den Vorbehalt einer Interessenabwägung zwischen den berechtigten Interessen des Kreditinstitutes und den schutzwürdigen Interessen der Betroffenen gestellt ist. Auch die alternativ heranziehbaren Regelungen der §§ 4 Abs. 2 Satz 2 Nr. 2a und Nr. 2b BDSG führen bei Vorliegen der dort genannten Voraussetzungen zu einer solchen Interessenabwägung.

Die Aufsichtsbehörde sah die Belange der zu Bewerbenden zunächst darin tangiert, dass diese nicht mehr in das Verfahren eingebunden sind und mit Erhalt des ersten Werbeschreibens bereits "vor vollendete Tatsachen gestellt werden." Weiterhin wird der gemeldete Interessent gezwungen, der Speicherung seiner Daten aktiv zu widersprechen (opt-out-Lösung), worin eine deutliche Erschwernis zu Lasten des Beworbenen gegenüber der aktuellen Variante zu sehen ist.
Allerdings war aus Sicht des Betroffenen positiv zu verzeichnen, dass die erstmalige Kontaktaufnahme nicht telefonisch bzw. per E-Mail, sondern auf postalischem Wege vorgesehen ist. Damit konnte das Verfahren noch in die Nähe einer "herkömmlichen" Direktwerbung eingeordnet werden.

Für eine positive Beurteilung des "Neuverfahrens" wurde das Vorliegen folgender Rahmenbedingungen als erforderlich betrachtet:

Zunächst dürfen nur Adressdaten im Sinne des § 28 Abs. 3 Satz 1 Nr. 3 BDSG ("Listenprivileg") erhoben werden. Angaben zu Telefonnummer, Fax-Nummer und E-Mail-Adresse werden nicht abgefragt, auch nicht mit einer Kennzeichnung als "freiwillige Daten". Beabsichtigte "Nachfassaktionen" gegenüber potentiellen Neukunden müssen sich im Rahmen der branchenüblichen Praxis bewegen und dürfen keinesfalls über zuvor ermittelte Telefonnummern, Fax-Nummern oder E-Mail-Adressen erfolgen.

Weiterhin ist sicherzustellen, dass die Betroffenen auf eine für sie komfortable Weise Widerspruch einlegen können, auch telefonisch, und dieser umgehend berücksichtigt und dokumentiert wird. Durch Einrichtung einer Sperrdatei ist auszuschließen, dass es zu einer erneuten Ansprache im Rahmen der Kundenempfehlung kommen kann. In der Praxis sind Fälle denkbar, bei denen verschiedene Empfehler eine Person als Interessenten "melden" – hier muss ein einziger Widerspruch ausreichen, um weitere Werbeaktivitäten im Vorfeld unterbinden zu können.

Das Unternehmen sagte zu, diese Vorgaben bei der Entwicklung der "Online-Empfehlung" zu berücksichtigen.

14. Videoüberwachung

Betreuung pflegebedürftiger Personen

Die Aufsichtsbehörde wurde um Beratung zu einem Konzept gebeten, das die Videobeobachtung pflegebedürftiger Menschen vorsieht.

Allein lebende pflegebedürftige Menschen müssen oftmals relativ früh in einem Pflegeheim untergebracht werden, wenn die Betreuung, die zusätzlich zu den Besuchen durch den Pflegedienst notwendig ist, durch Angehörige oder Freunde und Bekannte nicht mehr geleistet werden kann. Ein Diensteanbieter entwickelte daher ein Konzept, das in Zusammenarbeit mit dem jeweiligen Pflegedienst dem Pflegebedürftigen ermöglichen soll, länger in seiner gewohnten Umgebung zu verbleiben.

Hierbei soll über Videokameras, die in der Wohnung des Pflegebedürftigen installiert werden, eine "Fernbetreuung" durch den Pflegedienst zusätzlich zu der vor Ort vorgenommen Betreuung erfolgen. Die nötige Hard- und Software wird dabei von dem Diensteanbieter dem jeweiligen Pflegedienst zur Verfügung gestellt, welcher die Betreuung per Video dann dem Pflegebedürftigen anbietet. Zusammen mit dem Pflegebedürftigen und dessen Angehörigen wird hierbei in einem Betreuungsplan schriftlich festgelegt, in welchen Zeiträumen die Beobachtung erfolgt und wo die Kameras installiert werden. Außerdem wird ein so genannter Eskalationsplan erstellt. Hierin wird geregelt, welche Maßnahmen, z. B. telefonische Verständigung von Angehörigen, Alarmierung eines Arztes, getroffen werden sollen, wenn während der Beobachtung eine Verschlechterung des Gesundheitszustands festgestellt wird.
Die Kameras werden entsprechend der vertraglichen Festlegung zwischen Pflegedienst und Pflegebedürftigem in der Wohnung des Betreuten angebracht. Die Betreuung erfolgt zentral durch dem Betreuten bekannte Pfleger, welche über Bildschirme mehrere Betreute gleichzeitig beobachten. Zwischen den einzelnen Besuchen des Pflegedienstes ist es so möglich, gesundheitliche Veränderungen frühzeitig zu erkennen. Auch hat der Pflegebedürftige die Möglichkeit, sich in einem Notfall oder mit der Mitteilung, dass er die Kameras für einen bestimmten Zeitraum deaktivieren wird, telefonisch mit den Betreuern in Verbindung zu setzen.
Wichtig ist aus datenschutzrechtlicher Sicht, dass die Einwilligung in die Beobachtung durch den Betroffenen selbst erfolgt, die Betreuung jederzeit vom Betroffen unterbrochen und auch kurzfristig ganz beendet werden kann. In bestimmten Zeitabständen oder bei einer Verschlechterung des Gesundheitszustands muss überprüft werden, ob der Betroffene noch über ausreichende Einsichts- und Entscheidungsfähigkeit verfügt, um die Einwilligung ggf. widerrufen zu können, da ansonsten das Recht auf informationelle Selbstbestimmung nicht gewahrt ist. Besucher müssen durch einen schriftlichen Hinweis im Eingangsbereich der Wohnung auf die Videoüberwachung aufmerksam gemacht werden. Es ist dafür Sorge zu tragen, dass die Übertragung der Daten durch einen VPN-Tunnel gegen den Zugriff Dritter geschützt wird (Ein Virtuelles Privates Netzwerk (VPN) ist ein Computernetz, das zum Transport privater Daten ein öffentliches Netzwerk, z. B. das Internet, nutzt. Der VPN-Tunnel gewährleistet, dass Daten wie in einem lokalen Netzwerk ausgetauscht werden können. Dazu wird die Verbindung über das öffentliche Netzwerk verschlüsselt). Die Bildschirme dürfen nur nach Eingabe von Benutzernamen und Passwort verfügbar sein und eine Speicherung von Bilddaten nur soweit nötig erfolgen. Die visuellen Daten darf nur der Pflegedienst erhalten und personenbezogene Daten dürfen vom Diensteanbieter nur zu Abrechungszwecken verwendet werden. Wenn Leistungen durch einen Kooperationspartner erfolgen, hat der Pflegedienst den Betroffenen darauf hinzuweisen. Die technische Sicherheit hat sich an den Vorgaben des Grundschutzhandbuchs des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) zu orientieren und sollte von einer hierfür anerkannten Prüfstelle geprüft und attestiert werden.

Der Dienstanbieter legte der Aufsichtsbehörde Entwürfe der notwendigen Verträge und Einwilligungserklärungen vor, die nach Maßgabe der Aufsichtsbehörde abgeändert wurden. Unabhängig von der datenschutzrechtlichen Prüfung erfolgt noch eine Prüfung nach ethischen Gesichtspunkten, u. a. unter Beteiligung des Hessischen Sozialministeriums. Jedenfalls bis zum Abschluss dieser Prüfung darf die Einwilligung von Betroffenen nicht durch die Einwilligung eines Vormunds ersetzt werden.

15. Sonstiges

15.1 Kinderbetreuung nur gegen Personalausweisnummer?

Auf wenig Verständnis stieß bei einem Elternpaar, dass für die Kinderbetreuung in einem großen Möbelhaus neben den Adressdaten und dem Alter des Kindes auch die Personalausweisnummer eines Elternteils über ein Formular erhoben wurde. Da die Betroffenen der Gefahr eines Missbrauchs der Personalausweisdaten vorbeugen wollten und generell die Erforderlichkeit der Erhebung in Frage stellten, machten sie die Aufsichtsbehörde auf den Sachverhalt aufmerksam.

Vor einer Bewertung des Sachverhalts anhand der Vorschriften des BDSG war zunächst zu prüfen, ob die Erhebung und Verarbeitung der Personalausweisnummer nach dem Personalausweisgesetz (PersAuswG) zulässig ist. Nach § 4 PersAuswG darf der Personalausweis auch im nicht öffentlichen Bereich als Ausweis- und Legitimationspapier benutzt werden, wobei die Seriennummer nicht in einer Weise verwendet werden darf, dass mit ihrer Hilfe ein Abruf personenbezogener Daten aus Dateien oder eine Verknüpfung von Dateien möglich ist. Der Gesetzgeber wollte die Gefahr einer Nutzung der Seriennummer des Ausweises als eindeutige Personenkennziffer ausschließen. Aus der Stellungnahme des Möbelhauses ging hervor, dass die erhobenen Daten allerdings nicht automatisiert verarbeitet werden. Die Formulare würden nach Abwicklung der Betreuung noch bis zu sechs Monate lang archiviert und dann vernichtet. Für statistische Zwecke erfolge lediglich eine PC-gestützte Auswertung ohne Personenbezug im Hinblick auf die Anzahl der betreuten Kinder und die Zeiten, zu welchen diese angenommen und wieder abgeholt würden. Die Personalausweisnummer diene ausschließlich dazu, den Erziehungsberechtigten eindeutig zu identifizieren. Ein Abrufen des Datensatzes anhand der Personalausweisnummer bzw. eine Verwendung der Nummer als Ordnungsmerkmal sei in Ermangelung einer entsprechenden Verarbeitung nicht möglich. Unter diesen Voraussetzungen konnte das Erheben der Personalausweisnummer als mit dem PersAuswG vereinbar erachtet werden.

Aus datenschutzrechtlicher Sicht darf eine Erhebung personenbezogener Daten nur in dem jeweils erforderlichen Umfang erfolgen. Nach § 28 Abs. 1 Nr. 1 BDSG ist eine Datenerhebung, -verarbeitung und -nutzung für eigene Geschäftszwecke zulässig, wenn diese der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.

Auch wenn die angebotene Kinderbetreuung nicht "eigentlicher Geschäftszweck" eines Möbelhauses ist, wird dieser Service doch für eigene gewerbliche Zwecke angeboten. Der Kundschaft soll ein bequemeres Einkaufen ermöglicht werden, wovon man sich eine Steigerung des Absatzes und höhere Akzeptanz des Unternehmens erhofft. Das Betreuen der Kinder erfolgt dabei im Rahmen eines Vertragsverhältnisses, das der Kunde durch Anmeldung des Kindes mit dem Möbelhaus abschließt.

Soll sich die Verarbeitung der Daten auf die Regelung des § 28 Abs. 1 BDSG stützen können, bedarf es eines unmittelbaren sachlichen Zusammenhangs zwischen der beabsichtigten Verwendung und dem konkreten Vertragszweck. Dies war bei dem zu bewertenden Sachverhalt gegeben, da die Personalausweisnummern ausschließlich zur reibungslosen "Abwicklung" der Beaufsichtigung verarbeitet werden.

Weiterhin muss sich die verantwortliche Stelle auf die Verwendung der für den konkreten Vertragszweck objektiv dienlichen Daten beschränken. Welche Daten im Einzelnen verarbeitet werden dürfen, lässt sich dabei nicht abstrakt angeben. In Betracht kommt grundsätzlich eine Verwendung aller für den Abschluss und die Erfüllung eines Vertragsverhältnisses benötigten Angaben, was dann im Einzelfall zu prüfen ist.

Zur "Erfüllung" gehört im Fall der Kinderbetreuung zweifelsfrei, dass das Kind nach Beendigung des Aufenthalts wieder in die Obhut der Person gelangt, die das Kind "abgegeben" hat. Fraglich ist jedoch, ob dazu auch das Erfassen der Personalausweisnummer erforderlich ist.

Das Möbelhaus teilte dazu mit, dass bis zum Jahr 2005 ein anderes Kontrollverfahren praktiziert worden sei, das folgende Elemente enthielt: Unterschrift der Begleitperson, ein gemeinsamer Stempel mit individuellem Symbol- und Nummerncode. Zur Änderung des Verfahrens habe man sich entschieden, da im Rahmen einer Reportage über familienfreundliche Möbelhäuser von einer Rundfunkanstalt ein Bericht über deren Kinderbetreuungseinrichtung erstellt worden sei. Dabei hätte ein Reporter testweise "einen flüchtigen Bekannten" an Stelle des "richtigen Vaters" zum Abholen eines betreuten Kindes "geschickt" mit dem Ergebnis, dass der Junge unberechtigterweise herausgegeben worden sei. Eine interne Prüfung des Vorfalls habe ergeben, dass eine große Ähnlichkeit zwischen den beiden Unterschriften bestanden habe. Weiterhin sei es zu mehreren Vorfällen gekommen, die auf Kinderhandel hinwiesen. Offensichtlich würden Bandenmitglieder die Eltern

bei der Abgabe ihrer Kinder beobachten, sich Namen und Adressen merken und dann versuchen, unter Nutzung dieser Angaben und oft auch manipulierter Ausweisdokumente, die Kinder abzuholen. Dabei sei eine bloße Kontrolle des Lichtbilds wenig hilfreich, da bei den Bandenfällen das Lichtbild eindeutig den Abholenden zeige. Der Name werde - wie dargestellt - bei der Abgabe herausgefunden und sei daher kein sicheres Abgrenzungsmerkmal; ähnliches gelte für die Adresse.

Als Alternative - zur Verwendung der Personalausweisnummer - fertigen andere Möbelhäuser ein Foto der Begleitperson, wobei durch interne Regelungen festgelegt wurde, dass nur derjenigen Person das Kind übergeben werden darf, die auf dem gespeicherten Bild erkennbar ist; zusätzlich erfolgt auch hier eine Sicherung durch ein Armband mit Kontrollabschnitt.

Bei Vergleich beider Verfahren war festzustellen, dass beide geeignet sind, die Begleitpersonen zuverlässig zu identifizieren. Nach der Argumentation des von der Beschwerde betroffenen Möbelhauses sei deren Kontrolle dann sicherer, wenn sich Personen zum Verwechseln ähnlich sehen.

Aus den von Seiten der Möbelhäuser gegebenen Informationen ließ sich erkennen, dass eine völlig sichere Abwicklung der Betreuungen ausschließlich anhand von Adresse, Unterschrift und Kontrollarmband nicht möglich ist und es einer zusätzlichen Information (Foto oder Personalausweisnummer) bedarf. Beide Verarbeitungen tangieren das Recht auf informationelle Selbstbestimmung der Betroffenen, wobei die verschiedenen Maßnahmen sicherlich individuell unterschiedlich wahrgenommen werden. Zweifellos empfinden es einige Personen als störender, fotografiert zu werden und das eigene Bild gespeichert zu wissen.

Unter Würdigung der von Seiten des Möbelhauses vorgetragenen Gesichtspunkte - insbesondere der Gefährdungslage – wurde es aus datenschutzrechtlicher Sicht prinzipiell für zulässig und auch erforderlich eingeschätzt, durch Erhebung und Verarbeitung der Personalausweisnummer das Identifikationsverfahren zu optimieren. Insbesondere bei hohem Andrang bei der Kinderbetreuung wurde eine Gefahr von Fehlleistungen des dort tätigen Personals erkannt. Der Vergleich der Personalausweisnummer stellt eine relativ sichere Möglichkeit dar, um Fehler zu vermeiden. Allerdings muss sichergestellt sein, dass die Daten nur entsprechend ihrer Zweckbestimmung verwendet und danach gelöscht werden.
Im konkreten Fall war dies – nach entsprechender Beratung durch die Aufsichtsbehörde, die auch eine datenschutzfreundlichere Gestaltung des Aufnahmeformulars und eine Verringerung der Aufbewahrungsdauer auf maximal drei Monate mit sich brachte – letztlich gewährleistet.

15.2 Pflegedaten auf Tour

Offenbar aus Unachtsamkeit ließ die Mitarbeiterin eines ambulanten Pflegedienstes einen aufgeschlagenen Ordner auf dem Beifahrersitz ihres Einsatzfahrzeuges liegen. Passanten fiel auf, dass bei einem Blick durch die Seitenscheibe des abgestellten PKW der eingeheftete Tagesplan mit Informationen zu den zu besuchenden Pflegebedürftigen studiert werden konnte. Durch vor Ort aufgenommene Digitalbilder hielten die Passanten dies eindrucksvoll fest. Da - bei allem Verständnis für Termindruck und hohe Beanspruchung des Pflegepersonals - nicht hingenommen werden kann, dass sensible Daten dieser Art Dritten zur Kenntnis gelangen, wurde die Leiterin des Pflegedienstes auf die bestehenden datenschutzrechtlichen Bestimmungen aufmerksam gemacht. Diese bedauerte den Vorfall sehr und versicherte, die Mitarbeiterinnen für die datenschutzrechtliche Problematik zu sensibilisieren.

Wiesbaden, 20. August 2007

Der Hessische Ministerpräsident:
Koch

Der Hessische Minister des Innern und für Sport:
Bouffier