16. Wahlperiode

Drucksache **16/1680**

HESSISCHER LANDTAG

11. 12. 2003

Vorlage
der Landesregierung

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

Vorgelegt mit der Stellungnahme zum Einunddreißigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten - Drucks. 15/4790 - nach § 30 Abs. 2 des Hessischen Datenschutzgesetzes in der Fassung vom 7. Januar 1999

Eingegangen am 11. Dezember 2003 · Ausgegeben am 15. Januar 2004

Druck: Druckerei Chmielorz GmbH · Ostring 13 · 65205 Wiesbaden · Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

Allgemeiner Teil (Überblick, Statistik)

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

1.1 Erneut deutlicher Anstieg der eingehenden Eingaben und Beschwerden

Die Regierungspräsidien überprüfen als Aufsichtsbehörde gemäß § 38 Abs. 1 BDSG die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz in Hessen, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln.

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

Wie die folgende Übersicht zeigt, schlägt sich die zunehmende Technisierung von Geschäftsprozessen und der immer weiter ansteigende Einsatz moderner Informations- und Kommunikationstechniken im kommerziellen und privaten Bereich auch in der Entwicklung der Anzahl der bei den Regierungspräsidien anfallenden Verfahren nieder, wovon das Regierungspräsidium Darmstadt am stärksten betroffen ist. Der Arbeitsanfall bei der Beschwerdebearbeitung hat sich innerhalb von fünf Jahren mehr als verdoppelt:

Jahr	Fallzahl Land Hessen		Fallzahl RP Darmstadt	
1998	184		146	
1999	233	+49 (+27 v.H.)	184	+38 (+26 v.H.)
2000	273	+40 (+18 v.H.)	227	+43 (+23 v.H.)
2001	358	+85 (+31 v.H.)	308	+81 (+36 v.H.)
2002	421	+63 (+18 v.H.)	375	+67 (+22 v.H.)

Dabei umfassten die genannten Zahlen nur Beschwerdefälle, die eine aktenmäßige Bearbeitung erforderlich machten.
Eingaben, die telefonisch abgehandelt werden konnten, wie z.B. durch Hinweis auf eine bereits erfolgte Überprüfung einer verarbeitenden Stelle oder die Nichtanwendbarkeit des BDSG auf einen Sachverhalt, oder auch durch ausführliche telefonische Erörterung der vorgetragenen Problematik, sind nicht in diese Statistik eingeflossen. Ebenso wenig wurden Fälle erfasst, die aufgrund von örtlicher Unzuständigkeit an die zuständige Datenschutzaufsichtsbehörde eines anderen Bundeslandes abgegeben wurden. Die Zahl dieser Fälle dürfte mindestens in der gleichen Größenordung liegen, wie die Zahl der schriftlich bearbeiteten Fälle.

Die Bearbeitung der ebenfalls gestiegenen Zahl von Anfragen und Beratungsersuchen ist in den o.g. Zahlen nicht enthalten. Diese wird unter Nr. 3 dieses Tätigkeitsberichtes gesondert aufgeführt.

1.2 Bearbeitung von aktuellen Eingaben und Beschwerden

Im Berichtsjahr wurden von den hessischen Datenschutzaufsichtsbehörden in 421 Fällen Überprüfungen von nicht-öffentlichen Stellen vorgenommen, die Datenverarbeitung gemäß § 28 BDSG für die Erfüllung eigener Geschäftszwecke betreiben oder personenbezogene Daten gemäß §§ 29, 30 BDSG zur personenbezogenen oder anonymisierten Übermittlung speichern und nutzen.

Die 421 Überprüfungen von Eingaben, Beschwerden und Pressemeldungen durch die Regierungspräsidien betrafen:

- in 76 Fällen Teledienstеanbieter (Anbieter von Internetzugängen, -diensten und -inhalten),

- in 57 Fällen Banken, Kreditinstitute, und EDV-Dienstleister im Zahlungsverkehr,
- in 47 Fällen Handels- und Wirtschaftsauskunfteien,
- in 37 Fällen die Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA),
- in 37 Fällen Stellen und Unternehmen der Direktmarketing- und Werbewirtschaft,
- in 33 Fällen den Datenschutz in Arbeitsverhältnissen und bei Arbeitsvermittlern,
- in 17 Fällen das Gesundheitswesen (Apotheken, Ärzte, Krankenhäuser und Pflegeheime),
- in 16 Fällen Versender unverlangter E-Mail-Werbung (E-Mail-Spam),
- in 12 Fällen Versicherungsgesellschaften,
- in 10 Fällen Unternehmen des Groß- und Einzelhandels,
- in 9 Fällen Vereine (Sport, Soziales, Kultur), sowie deren Landes- u. Bundesverbände,
- in 7 Fällen Unternehmen der Freizeit-, Touristik- und Reisebranche,
- in 6 Fällen Unternehmen der Versandhandelsbranche,
- in 6 Fällen Vermieter sowie Wohnungs- u. Immobilienverwaltungsfirmen,
- in 6 Fällen Inkassounternehmen,
- in 5 Fällen Vermögensberater und Kapitalanlagegesellschaften,
- in 5 Fällen Adressverlage und Herausgeber öffentlicher Verzeichnisse,
- in 4 Fällen Zeitungs- und Buchverlage,
- in 3 Fällen Kreditkartenunternehmen,
- in 3 Fällen die Videoüberwachung von Grundstücken, Häusern und Wohnungen,
- in 2 Fällen Versender unverlangter Telefaxwerbung (Fax-Spam),
- in 2 Fällen Markt- und Meinungsforschungsunternehmen,
- in 21 Fällen sonstige Stellen (z.B. Public-Relations-Unternehmen, politische Partei,Gewerkschaft, Soft- und Hardwarehersteller, Paketdienst, Spedition, Rechtsanwalt, Call-Center).

Bei knapp einem Viertel der Beschwerden konnte zeitnah festgestellt werden, dass diese begründet waren. In insgesamt 97 Fällen wurden bei den Nachforschungen der Aufsichtsbehörden 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 Verstöße gegen Datenschutzbestimmungen wurden festgestellt:

- in 16 Fällen bei Kreditinstituten und Banken,
- in 15 Fällen bei der Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA),
- in 12 Fällen bei Anbietern von Tele- und Mediendiensten (Access- und Content-Provider),
- in 12 Fällen bei der Verarbeitung von Arbeitnehmer- und Bewerberdaten,
- in 10 Fällen bei Versendern von Werbe-E-Mails (E-Mail-Spam),
- in 9 Fällen bei Unternehmen der Direktmarketing- und Werbebranche,
- in 7 Fällen bei Handels- und Wirtschaftsauskunfteien,
- in 5 Fällen im Gesundheitssektor (Arzt, Krankenhaus),
- in 2 Fällen im Wohnungswesen (Vermieter, Immobilienmakler),
- in 2 Fällen bei Versicherungen,
- in 2 Fällen bei Einzelhandelsunternehmen,
- in 2 Fällen bei eingetragenen Vereinen,
- sowie in jeweils einem Fall bei einem Softwarehersteller, einem Call-Center und einem Inkassounternehmen.

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

1.3 Erledigung von Eingaben und Beschwerden aus den Vorjahren

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

jahr 85 Fälle abgeschlossen. Die Beurteilung dieser in der Regel nur mit hohem Ermittlungsaufwand aufklärbaren Eingaben durch die Regierungspräsidien ergab, dass davon 52 Eingaben begründet waren. Damit mussten die Aufsichtsbehörden in mehr als 60 v.H. dieser Fälle einen Datenschutzverstoß feststellen.

Die beanstandeten 52 Verstöße gegen Datenschutzbestimmungen wurden festgestellt:

- in 23 Fällen bei Unternehmen der Werbewirtschaft und werbenden Einzelhändlern,
- in 9 Fällen bei Anbietern von Telediensten (Internetprovider),
- in 5 Fällen bei einem Adressverlag,
- in 5 Fällen bei Banken,
- in 2 Fällen bei Handels- und Wirtschaftsauskunfteien,
- in 2 Fällen in der Reise- und Touristikbranche,
- sowie in jeweils einem Fall bei einer Versicherung, einem Arzt, einem Versandhändler und einem eingetragenen Verein, die personenbezogene Daten unzulässig gespeichert, genutzt oder übermittelt hatten.

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

Bei den im Berichtsjahr insgesamt durchgeführten Prüfungen von Eingaben, Beschwerden und Hinweisen auf Datenschutzverstöße bestand in 18 Fällen Veranlassung für eine Überprüfung vor Ort. Nur auf diese Weise ließ sich zuverlässig feststellen, ob ein Datenschutzverstoß vorlag. Die Prüfdauer variierte dabei - je nach Komplexität der Datenverarbeitung und der Schwere des Vorwurfs - von kurzen ein- bis zweistündigen Prüfungen bis zu ganztätigen Prüfungen, Vor- und Nachbereitungszeit nicht eingerechnet (vgl. auch die ergänzende Darstellung unter Nr. 6).

2. Bearbeitung von Anfragen zu datenschutzrechtlichen Problemstellungen und Beratungstätigkeit

2.1 Entwicklung der Anfragebearbeitung und der Beratungstätigkeit

Die Zahl der an die Datenschutzaufsichtsbehörden herangetragenen Anfragen und Beratungsersuchen von Unternehmen, Vereinen und Verbänden, aber auch von Bürgerinnen und Bürgern, insbesondere von Arbeitnehmern und Betriebsräten zu Datenschutzfragen am Arbeitsplatz, hat erneut stark zugenommen. Die stetig steigende Bedeutung der Information und Aufklärung von Betroffenen sowie der vorbeugenden datenschutzrechtlichen Beratung der verantwortlichen Stellen durch die Aufsichtsbehörden wird insbesondere durch die Beratungsstatistik des Regierungspräsidiums Darmstadt belegt, wo sich das Aufkommen an Anfragen und Beratungsersuchen innerhalb von vier Jahren verdreifacht hat:

Jahr	Fallzahl RP Darmstadt	Zunahme
1999	52	
2000	93	+41 (+80 v.H.)
2001	138	+45 (+49 v.H.)
2002	166	+28 (+20 v.H.)

Insgesamt gingen im Jahr 2002 bei den hessischen Datenschutzaufsichtsbehörden 211 Beratungsersuchen ein.

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

Ein Grund für die Zunahme der Beratungsersuchen ist, dass die Computerisierung nicht nur auf der Seite der Unternehmen fortschreitet. Auch in der Bevölkerung werden moderne technikgestützte Möglichkeiten des Informierens, Kommunizierens, Einkaufens, Bestellens und Ersteigerns immer beliebter, allen voran der Teledienst "E-Mail" und das sogenannte "WorldWideWeb" (WWW). Hier nutzen immer mehr Bürgerinnen und Bürger die einfach zu erreichenden und äußerst vielfältigen Angebote und übermitteln dabei - im Internet oftmals sogar unbewusst - einer Vielzahl von

dabei - im Internet oftmals sogar unbewusst - einer Vielzahl von Stellen ihre Daten zur anschließenden Verarbeitung in automatisierten Verfahren. Die Vielfalt der Anwendungsmöglichkeiten moderner Informations- und Kommunikationstechnologie bildet sich auch in der inhaltlich mehr als breit gefächerten Palette von Anfragen zu datenschutzrechtlichen Problemstellungen ab, die - trotz der im folgenden dargestellten klaren Schwerpunkte - fast überall in der modernen Informationsgesellschaft zu finden sind.

2.2 Statistische Auswertung der eingegangenen Anfragen

Bei den an die Regierungspräsidien im Berichtsjahr herangetragenen 211 Beratungsersuchen ergaben sich folgende inhaltliche Schwerpunkte:

27 Anfragen von betrieblichen Datenschutzbeauftragten (DSB). Die Anfragen erfolgten im Zusammenhang mit der praktischen Umsetzung der Anforderungen des BDSG im Betrieb, z.B. zur Erstellung eines Verfahrensverzeichnisses gemäß § 4g Abs. 2 BDSG, zum Umfang der Auskunftserteilung nach § 34 BDSG, zur Fernwartung, einem Outsourcing-Projekt, zum Umfang der Kontrolle eines Auftragnehmers nach § 11 Abs. 2 BDSG.

Einem großen Teil der zum betrieblichen DSB eingegangen Fragen, hauptsächlich von Arbeitnehmern und Betriebsräten, lagen leider erneut erhebliche Unsicherheiten und Defizite von Betrieben und anderen verarbeitenden Stellen bezüglich der Bestellung eines betrieblichen DSB zu Grunde. Nach § 4f BDSG ist jeder Selbständige, Freiberufler, Arzt, Betrieb, Verein, Kaufmann etc., der mehr als 4 Beschäftigte - sei es auch nur gelegentlich - mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten befasst, zur Bestellung eines betrieblichen Datenschutzbeauftragten und zu dessen Unterstützung bei der Umsetzung seiner gesetzlichen Pflichten im Betrieb nach § 4g BDSG verpflichtet. Während der Beratungen der Anfrager durch die Aufsichtsbehörden stellte sich auf Nachfrage aber oftmals heraus, dass diese gesetzliche Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten von Unternehmen nicht eingehalten wurde. Die Aufsichtsbehörden mussten diese anlässlich von Anfragen und Beratungsersuchen aufgefallenen Unternehmen, Vereine und Verbände im Anschluss an die Beratungen regelmäßig davon überzeugen, dass die Bestellung nicht nur gesetzlich zwingend erforderlich, sondern - richtig umgesetzt - vielfach auch ökonomisch sinnvoll ist. Leider reagierten einige Stellen erst nach dem Hinweis auf die Androhung eines Bußgeldes gemäß § 43 Abs. 1 Nr. 2 BDSG und die mögliche Bußgeldhöhe von bis zu 25.000 Euro.

Wie bereits im letzten Jahr war Gegenstand mancher Anfragen von betrieblichen Datenschutzbeauftragten der angemessene Umfang der Unterstützung durch die jeweilige Unternehmensführung, der zumeist als zu gering empfunden wurde. Der Datenschutzbeauftragte muss von dem Unternehmen selbstverständlich nicht nur formal korrekt bestellt, sondern natürlich auch entsprechend materiell und personell ausgestattet und im erforderlichen Umfang von betrieblichen Aufgaben freigestellt werden, wenn er den gesetzlichen Anforderungen an die Tätigkeit eines betrieblichen DSB gerecht werden soll.

Weitere Fragen der Datenschutzbeauftragten betrafen den Umfang des eigenen Schulungsbedarfs und dessen betriebliche Durchsetzung, die beabsichtigte Kündigung von DSB, die Vorabkontrolle gemäß § 4d Abs. 5 BDSG sowie Fragen zur Bestellung von externen Personen zum DSB.

24 Anfragen aus dem Bereich des Arbeitnehmerdatenschutzes. Hier war ein starker Anstieg der Beratungsersuchen durch Betriebsräte zu verzeichnen, die Unterstützung bei der Ausgestaltung und Formulierung von Betriebsvereinbarungen zur Nutzung des betrieblichen Internetanschlusses (WWW und E-Mail) durch die Beschäftigten suchten. Die immer häufigere Übermittlung von Arbeitnehmerdaten an beherrschende Konzernunternehmen oder auch externe Outsourcing-Dienstleister war ebenfalls Anlass für kritische Nachfragen von betroffenen Arbeitnehmern und Betriebsräten. Bei einigen Eingaben handelte es sich um allgemeine Beratungsersuchen zum Umgang mit Bewerberdaten bei Stellenvermittlern und Bewerberservices (siehe auch Nr. 6).

21 Anfragen zum Datenschutz im Internet. Bei vielen Anbietern von Tele- und Mediendiensten im Internet, also bei den Betreibern von WWW-Seiten sowie E-Mail- und Newsletter-Anbietern, herrscht leider häufig immer noch

Unsicherheit, wie sie die gesetzlichen Anforderungen des Teledienstedatenschutzgesetzes und des Mediendienste-Staatsvertrages an Diensteanbieter praktisch auf ihren Internet-Seiten umsetzen sollen, um Ihre Dienste datenschutzfreundlicher im WWW präsentieren zu können. Hier waren in der Regel Ausgestaltungs- und Formulierungshilfen für den für WWW-Anbieter vorgeschriebenen Datenschutzhinweis zu geben.
Zudem ist bei den Anbietern oftmals nicht bekannt, welche Daten mit welchen Hinweisen erhoben und dann verarbeitet werden dürfen, welche Daten lediglich als freiwillige Angaben erhoben werden dürfen, dass diese Freiwilligkeit deutlich gemacht werden muss, und für viele Verarbeitungsvarianten, z.B. für die werbliche Nutzung, eine ausdrückliche Einwilligung einzuholen ist. Falls diese Einwilligung "online" gegeben wird, muss dies immer per E-Mail im Double-Opt-In-Verfahren erfolgen, um einen möglichen Missbrauch durch Unberechtigte ausschließen zu können (siehe Nr. 11.2).

Andere Fragen betrafen die Bedrohungen im Internet durch Schadprogramme (Viren, Würmer und Trojaner) und "Hacker-Angriffe" sowie geeignete Schutzmaßnahmen, den geschäftsmäßigen Handel mit E-Mail-Adressen und den geplanten Betrieb einer Internet-Auskunftei. Dieses Projekt wurde nach Darstellung der datenschutzrechtlichen Erfordernisse aber nicht weiter verfolgt (siehe Nr. 12).

18 Anfragen zur Auftrags-Datenverarbeitung gemäß § 11 BDSG. Dabei ging es sowohl um die korrekte Ausgestaltung von Vertragstexten im Sinne dieser Vorschrift als auch um den Wegfall der Meldepflicht für die Dienstleistungsdatenverarbeitung nach der letzten BDSG-Novellierung 2001 (siehe auch Nr. 5). So traten beispielsweise Auftraggeber auf, die von ihren EDV-Dienstleistern in Unkenntnis der gesetzlichen Änderungen immer noch die Vorlage der Registermeldung verlangten und drohten, ansonsten den Auftrag zu entziehen. Die Aufsichtsbehörde war in diesen Fällen immer bereit, zur Klärung beizutragen, den Auftraggeber mit der aktuellen Rechtslage vertraut zu machen und bei der Änderung seiner Vertragstexte zu unterstützten. In vier Fällen wurde anlässlich der Anfrage nach der vermeintlich bestehenden Meldepflicht festgestellt, dass beteiligte Unternehmen ihrer Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten gemäß § 4f BDSG nicht nachgekommen waren.

17 Anfragen aus dem Gesundheitssektor, darunter, neben den immer wiederkehrenden Fragen zu den Modalitäten und Mindestfristen für die Aufbewahrung von Patientenunterlagen, auch die Bitte um datenschutzrechtliche Bewertung einer Geschäftsidee zur Zweitvermarktung gebrauchter Arzt-PCs und um die Beurteilung der Übermittlung von Patientendaten von einer Arztpraxis an eine externe privatärztliche Abrechnungsstelle. Weitere Beratungsersuchen drehten sich um die gemäß § 30 BDSG erforderlichen Anonymisierungsmaßnahmen bei einem Marktforschungsprojekt und die Frage eines Arztes, ob und gegebenenfalls unter welchen Voraussetzungen er Telefonate mit seinen Patienten aufzeichnen darf.

16 Anfragen zur Auslands-Datenverarbeitung, zum Teil zur datenschutzrechtlichen Zulässigkeit der Übermittlung von Personal- und Kundendaten in die USA oder andere außereuropäische Drittstaaten. Weitere Beratungen erfolgten zur Übermittlung personenbezogener Schuldnerdaten in die USA und zur vorherigen Durchführung eines Datenschutzaudits nach § 9a BDSG.

13 Anfragen von Vereinen und Dachverbänden mit sportlichem, sozialem und kulturellem Hintergrund, die den datenschutzgerechten Umgang mit den personenbezogenen Daten der eigenen Mitglieder zum Gegenstand hatten. Hierbei wurden Fragen zur werblichen Nutzung von Mitgliederdaten, der genauen Formulierung von Einwilligungserklärungen, der Übermittlung von Daten an externe und vereinsinterne Empfänger und zur Datenerhebung beim Besuch von Sportveranstaltungen gestellt. Mehrfach wurde angefragt, ob ein Verein Daten von Vereinsmitgliedern auf Internet-Seiten im WWW ohne deren ausdrückliche Einwilligung und ohne entsprechende Regelung in der Vereinssatzung veröffentlichen darf (z.B. auf Vereins-Homepages oder auch im Rahmen der Online-Berichterstattung über Ergebnisse von Sportveranstaltungen). Dies war grundsätzlich zu verneinen.

11 Anfragen zur Datenverarbeitung durch die SCHUFA. Dabei war ganz grundsätzlich die Arbeitsweise der Schufa, insbesondere die Zusammenar-

beit der Schufa mit den verschiedenen A- und B-Vertragsteilnehmern, z.B. Banken und Versandhändler, zu erläutern, die den Betroffenen oftmals nur schemenhaft bekannt ist. Einige Anfrager baten um Informationen zu dem von der Schufa angewandten Scoring-Verfahren, auf das unter Nr. 10.1 noch genauer eingegangen wird.

7 Anfragen zur Verarbeitung und Übermittlung von personenbezogenen Daten durch Handels- und Wirtschaftsauskunfteien und Detekteien. Dabei handelte es sich großteils um Fragen von Verbrauchern und Betroffenen, die sich anlässlich der Benachrichtigung gemäß § 33 BDSG über die erstmalige Übermittlung ihrer Daten durch eine Auskunftei an einen Anfrager ratsuchend an die Aufsichtsbehörden wandten, um Informationen über die Geschäftstätigkeit von Auskunfteien und deren datenschutzrechtliche Grenzen zu erhalten. Weiterhin hatten sich die Regierungspräsidien mit Beratungsersuchen zu befassen, mit denen nach den Erwartungen der Anfrager die Planungen zur Einrichtung von branchenspezifischen Warnlisten - im Sinne von sogenannten "schwarzen Listen" - datenschutzrechtlich abgesichert werden sollten (siehe Nr. 12).

7 Anfragen zu Videoüberwachungsmaßnahmen bei Wohnanlagen. Eigentümer, Vermieter und Hausverwaltungen baten um Beratung, welche Anforderungen bei der Durchführung solcher Maßnahmen zu beachten sind. Immer wieder erläuterten die Aufsichtsbehörden die Voraussetzungen des § 6b BDSG und die zivilrechtliche Rechtsprechung. Insbesondere machten sie darauf aufmerksam, dass auf die Videobeobachtung nach § 6 b Abs. 2 BSDG hingewiesen werden muss, z.B. durch eine geeignete Beschilderung, und dass die Videoaufzeichnungen nicht beliebig lange aufbewahrt werden dürfen, da § 6b Abs. 5 BDSG eine Löschung fordert, wenn die Aufnahmen zur Erreichung des Beobachtungszwecks nicht mehr erforderlich sind, was in der Regel schon nach wenigen Stunden oder Tagen der Fall ist.

5 Anfragen bezogen sich auf die Nutzung personenbezogener Adressdaten durch die Werbewirtschaft. Die anfragenden Bürgerinnen und Bürger hatten unaufgefordert personalisierte Briefwerbung von Unternehmen erhalten, mit denen noch nie ein Geschäftskontakt bestand und baten um allgemeine Beratung. In der "Offline-Welt" gilt für die Werbewirtschaft das "Opt-Out-Prinzip", also die Zulässigkeit der werblichen Datennutzung auch ohne Einwilligung, solange der oder die Betroffene dem nicht widerspricht. Die Anfrager wurden über die Zulässigkeit des Adresshandels gemäß §§ 28, 29 BDSG und über ihr unabdingbares Recht auf Auskunftserteilung aufgeklärt und bei der Formulierung von Widersprüchen gegen die werbliche Nutzung ihrer Adressdaten beraten.

Weitere Anfragen betrafen den Empfang unverlangter Erotik-E-Mails (Spam) und Werbe-Telefaxe, oftmals im Zusammenhang mit einer teueren 0190-Mehrwertrufnummer, zu deren Nutzung die Verbraucher verleitet werden sollten. Viele ratsuchende Bürgerinnen und Bürger legten ihren Schreiben an die Datenschutzaufsichtsbehörden auch Kopien unverlangt empfangener Telefaxe und Werbe-E-Mails bei, mit der Bitte um Mitteilung, wie und vor allem bei wem man sich gegen diese unlauteren und unseriösen Werbemethoden wehren könne, da sich die Absender regelmäßig nicht zu erkennen gaben oder die Angaben zum Absender wie auch die Kontaktinformationen zur Abmeldung sogar gefälscht waren (vgl. dazu ausführlich auch im 15. Tätigkeitsbericht, LT-Drucks. 15/4659, Nr. 8.8).

Leider können auch die Datenschutzaufsichtsbehörden in solchen Fällen nur sehr begrenzt weiterhelfen, da die verantwortlichen werbetreibenden Stellen in den wenigsten Fällen ermittelt werden können. Immerhin konnten die Ratsuchenden am Ende des Berichtszeitraumes auf die zwischenzeitlich aus Verbraucherschutzgründen erfolgte Änderung der Telekommunikations-Kundenschutzverordung (TKV) hingewiesen werden, die dafür sorgen soll, dass sich Verbraucher gegen unverlangte Fax-, E-Mail- und SMS-Werbung für 0190er Nummern besser wehren können. Nach § 13a TKV besteht für solche Netzbetreiber, die anderen Unternehmen 0190er-Mehrwertdiensterufnummern zur Nutzung überlassen, die Verpflichtung, Rechtsverstöße durch diese Unternehmen zu unterbinden, indem sie die unverlangt beworbenen und damit missbräuchlich verwendeten 0190er-Nummern sperren. Die Regulierungsbehörde für Post und Telekommunikation, die die 0190er-Mehrwertdiensterufnummern in Blöcken an die Netzbetreiber vergibt, hat unter http://www.regtp.de/reg_tele/02675/index.html

eine Suchmaschine für Verbraucher zur Ermittlung des jeweils betroffenen Netzbetreibers ins WWW eingestellt. Ob die Änderungen in der TKV und die Angebote der Regulierungsbehörde im WWW wirklich zu einem Nachlassen der Flut unverlangter Fax-, E-Mail- und SMS-Werbung für 0190er Nummern führen werden, bleibt abzuwarten. Da auch für das Gesetz zur Bekämpfung des unlauteren Wettbewerbs (UWG) zum Zeitpunkt der Berichterstattung Änderungsvorschläge mit dem Ziel der besseren wettbewerbsrechtlichen Bekämpfung unverlangter Werbebotschaften diskutiert wurden, bleibt zu hoffen, dass dieses Maßnahmenbündel nach Inkrafttreten in Zukunft spürbar Wirkung entfalten kann (siehe auch Nr. 11.4).

Die übrigen Beratungsersuchen betrafen den Datenschutz von Mietern, die Verarbeitung bzw. Löschung von Daten bei Alltagsgeschäften, die Veröffentlichung personenbezogener Daten in öffentlichen Verzeichnissen, Aktenaufbewahrungsmöglichkeiten und -fristen, technische Fragen zu geeigneten Verschlüsselungsprogrammen zur geschützten Kommunikation per E-Mail und zur sicheren Datenübermittlung im WWW sowie datenschutzgerechte Lösungen für ein wissenschaftliches Forschungsprojekt.

2.3 Versendung von Informationsmaterial und Orientierungshilfen

Das datenschutzrechtliche Informationsmaterial für Bürgerinnen und Bürger sowie für Unternehmen und deren Datenschutzbeauftragte, das die hessischen Datenschutzaufsichtsbehörden zu unterschiedlichsten Fragestellungen des Datenschutzrechts bereithalten, wurde im Berichtsjahr von Interessierten in großem Umfang angefordert. Die meisten Bitten um die Zusendung von Informationsmaterial, Merkblättern und Hinweisen erfolgten durch die betrieblichen Datenschutzbeauftragten von Unternehmen, die um Unterlagen und Hilfen zur Aufgabenerfüllung im Betrieb baten. Als weiterer Schwerpunkt waren Informationen zur datenschutzgerechten Auslandsdatenverarbeitung auszumachen, gefolgt von Bitten um Informationsmaterial zur Bekämpfung unverlangter E-Mail-Werbung.

Insbesondere die Homepage des Datenschutzdezernates beim RP Darmstadt im WWW (http://www.rpda.de/dezernate/datenschutz) wird gerne genutzt, um Mustertexte, Meldeformulare sowie Merk- und Hinweisblätter abzurufen.

3. Genehmigungsverfahren gemäß § 4c Abs. 2 BDSG

Wie bereits in den vorangegangenen Tätigkeitsberichten dargestellt (zuletzt: 15. Tätigkeitsbericht vom 26. November 2002, LT-Drucks. 15/4659, Nr. 1 und Nr. 7), wurde mit der BDSG-Novelle vom 23. Mai 2001 erstmals ein Genehmigungserfordernis für bestimmte Datenverarbeitungen begründet.

Die Übermittlung personenbezogener Daten in sogenannte "Drittstaaten", Staaten außerhalb der Europäischen Union und des Europäischen Wirtschaftsraumes, in denen kein angemessenes Datenschutzniveau besteht, darf - sofern nicht gesetzliche Ausnahmetatbestände gegeben sind - nur erfolgen, wenn die Aufsichtsbehörden die Übermittlung zuvor genehmigt haben.

Im Berichtsjahr waren drei konkrete Genehmigungsanträge beim Regierungspräsidium Darmstadt anhängig.

Der erste Antrag war bereits Ende 2001 eingegangen und betraf die Übermittlung von Personaldaten eines hier ansässigen Unternehmens an die Konzernzentrale in den USA. Nach Erörterungen mit der Aufsichtsbehörde wurde der Antrag jedoch nicht weiter verfolgt bzw. als ruhend erklärt. Da auch andere konzernangehörige Unternehmen in Europa Daten an die Konzernzentrale in USA übermitteln, wird das deutsche Unternehmen sich um eine möglichst konzernweit einheitliche Lösung bemühen. Es wird angestrebt, die Standardverträge der EU wörtlich zu verwenden, so dass das Genehmigungserfordernis entfiele (s. hierzu bereits 15. Tätigkeitsbericht vom 26. November 2002, LT-Drucks. 15/4659, Nr. 7.2).

Der zweite Antrag, der beim Regierungspräsidium Darmstadt einging, betraf ebenfalls die Übermittlung von Personal- und zusätzlich von Kundendaten eines deutschen Unternehmens an die Konzernzentrale. Die Daten sollten zentral auf einem Server in den USA gespeichert werden, die US-Muttergesellschaft sollte jedoch keine eigenen Entscheidungs-

/Verfügungsbefugnisse bzgl. der Daten erhalten, sondern nur den Server administrieren etc., d.h. als Auftragsverarbeiter fungieren.
Um ausreichende Garantien für die Persönlichkeitsrechte der betroffenen Mitarbeiter und Kunden zu schaffen, sollte ein Vertrag mit der US-Mutter geschlossen werden, der sich zwar an dem entsprechenden Standardvertrag der EU vom 27. Dezember 2001 orientierte, aber doch viele Abweichungen enthielt. Auf Grund intensiver Erörterungen mit der Aufsichtsbehörde wurde der Vertrag geändert und damit weiter an den Standardvertrag der EU angepasst. Nach Abstimmung in der Arbeitsgruppe "Internationaler Datenverkehr" des Düsseldorfer Kreises konnte die Aufsichtsbehörde schließlich die Genehmigung erteilen. Dies war die erste Genehmigung dieser Art im Bundesgebiet. Der von der Aufsichtsbehörde entworfene und mit der Arbeitsgruppe abgestimmte Genehmigungsbescheid kann als Musterbescheid im Bundesgebiet Verwendung finden.

Da die EU-Kommission und die anderen EU-Staaten ein Veto-Recht haben, leitete die Aufsichtsbehörde den Genehmigungsbescheid an das Bundesinnenministerium (BMI) weiter, welches das erforderliche Notifizierungsverfahren einleitete. Bedenken wurden seitens der EU nicht erhoben.

Gegenstand des dritten Antrages war ebenfalls eine Übermittlung von Personaldaten an eine Konzernzentrale in den USA, welche als Auftragsverarbeiter fungierte. Auch hier wurde ein Vertragsentwurf vorgelegt, der auf Grund der Hinweise der Aufsichtsbehörde und der Abstimmung im Düsseldorfer Kreis geändert wurde. Die Genehmigung (die zweite im Bundesgebiet) konnte Anfang 2003 erteilt und an das BMI weitergeleitet werden. Bei Redaktionsschluss dieses Berichtes lagen keine Einwände seitens der EU vor. Es kann somit davon ausgegangen werden, dass beide Genehmigungsbescheide bestandskräftig werden.

Weitere Einzelheiten der Genehmigungserteilung sind unter Nr. 8 dargestellt.

4. Überprüfung von Verhaltensregeln nach § 38a BDSG

Art. 27 EG-Datenschutzrichtlinie (EG-DSRL) verpflichtet die Mitgliedstaaten, die Erstellung von branchen- und berufsspezifischen Verhaltensregeln zum Datenschutz durch Berufsverbände und andere Vereinigungen zu fördern. Daher weist § 38a BDSG den Aufsichtsbehörden die Aufgabe zu, solche Verhaltensregeln zum Datenschutz auf ihre Vereinbarkeit mit dem geltenden Datenschutzrecht zu überprüfen und ggfs. ein entsprechendes "Unbedenklichkeitsattest" zu erteilen (siehe bereits 15. Tätigkeitsbericht vom 26. November 2002, LT-Drucks. 15/4659, Ziff. 1). Die Aufsichtsbehörde kann eine förmliche Entscheidung in diesem Sinne jedoch nur treffen, wenn der Berufsverband oder die sonstige Vereinigung, welche die Verhaltensregeln erstellt, diese vorlegt und die Entscheidung beantragt.

Im Berichtsjahr legte ein im Rhein-Main-Gebiet ansässiger Sportverband dem Regierungspräsidium Darmstadt eine Verhaltensregel zur Bewertung vor.
Diese erfüllte jedoch nicht vollständig die rechtlichen Anforderungen an Verhaltensregeln i.S.d. § 38a BDSG.

Nach Auffassung der Aufsichtsbehörde genügt es nicht, den Wortlaut der einschlägigen datenschutzrechtlichen Regelungen wiederzugeben. Vielmehr muss ein "Mehrwert" gegeben sein, d.h. die Verhaltensregel muss die abstrakten gesetzlichen Regelungen branchenspezifisch bzw. kontextbezogen konkretisieren, so dass typische Anwendungsfälle in dem betreffenden Bereich erläutert sind. Die von dem Verband vorgelegte Verhaltensregel war jedoch in einigen Teilen nicht hinreichend konkret. Sie blieb auch inhaltlich z. T. hinter dem Merkblatt für die Datenverarbeitung im Verein zurück, welches vom Innenministerium Baden-Württemberg und von einigen anderen Aufsichtsbehörden nach der Gesetzesnovelle neu herausgegebenen wurde.
Die Abstimmung mit den anderen Aufsichtsbehörden im Bundesgebiet ergab deshalb, dass der Bedarf bzw. Sinn der vorgelegten Verhaltensregel als zweifelhaft beurteilt wurde. Daher zog der Verband seinen Antrag gemäß § 38a BDSG zurück. Nach gewisser Überarbeitung machte der Verband seine "Verbandsregelung" gleichwohl seinen Mitgliedern bekannt. Hiergegen war nichts einzuwenden.

Der vom Deutschen Direktmarketingverband vorgelegte Leitfaden zu den Auswirkungen der BDSG-Novelle auf das Direktmarketing (s. 15. Tätigkeitsbericht vom 26. November 2002, LT-Drucks. 15/4659, Nr. 15) erfüllt zwar - ungeachtet der inhaltlichen Kritik der Aufsichtsbehörden in einigen Punkten - grundsätzlich die "Mehrwert"-Anforderungen, da er viele praxisnahe Erläuterungen und Beispiele enthält, aber der Deutsche Direktmarketingverband gab zu erkennen, dass er den Leitfaden nicht als "Verhaltensregel" i.S.d. § 38a BDSG eingeordnet wissen wolle bzw. keine förmliche Entscheidung nach § 38a BDSG wünsche (näheres hierzu siehe unter Nr. 16.1).

5. Register der meldepflichtigen Verfahren nach § 4d BDSG

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

Im Melderegister waren 84 Verfahren von 82 verantwortlichen Stellen eingetragen.
Wie sich aus diesen Zahlen ergibt, haben nur zwei verantwortliche Stellen mehr als ein Verfahren gemeldet.

Davon werden in 41 gemeldeten Verfahren geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung gespeichert (Adresshändler , Handels- und Wirtschaftsauskunfteien, meldepflichtig nach § 4d Abs. 4 Nr. 1 BDSG), 53 der eingetragenen Verfahren dienen dem Zwecke der anonymisierten Übermittlung (Markt- und Meinungsforschung, meldepflichtig nach § 4d Abs. 4 Nr. 2 BDSG).

Beim Ausfüllen der Meldeformulare waren die Unternehmen offensichtlich vor einige Probleme gestellt. Insbesondere die Angaben zur Beurteilung der Angemessenheit der Datensicherheit im Sinne des §9 BDSG waren unzureichend. Mit der Novellierung des BDSG wurden diese Angaben erstmals erforderlich. Die Aufsichtsbehörden begrüßen ausdrücklich die Aufnahme dieser Informationen in den Meldebogen, fordert dies doch von den Unternehmen, die gesamte innerbetriebliche Organisation im Bezug auf Sicherheitsmaßnahmen zu durchdenken.

Immer noch melden sich Dienstleistungsunternehmen bei den Aufsichtsbehörden und beantragen die Aufnahme in das Melderegister, obwohl die Auftragsdatenverarbeiter nach der Neureglung des Datenschutzrechts gar nicht mehr meldepflichtig sind.

6. Anlassunabhängige Überprüfungen

Im Berichtsjahr wurden 16 anlassunabhängige Kontrollen durchgeführt.

Diese betrafen folgende Branchen/Bereiche:

- Arbeitsvermittler	4
- Public-Relations-Unternehmen (PR)	4
- Datenträger- und Aktenvernichtungsunternehmen	3
- Rechenzentren/Dienstleister	2
- Automobilbranche	2
- Handels- und Wirtschaftsauskunftei	1

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

- Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten nicht erfüllt,
- Mängel in den Bereichen der Datensicherheit, z.B. fehlende Zugriffsregelungen, Versenden von E-Mails mit Anhängen mit vertraulichen Daten ohne Verschlüsselung,
- fehlende Weisungen gemäß § 11 BDSG.

Die Prüfungsschwerpunkte wurden im Berichtsjahr deshalb bei den Arbeitsvermittlern und PR-Unternehmen gesetzt, weil verschiedene Eingaben von Betroffenen über Arbeitsvermittler vorlagen und Presseberichte über ein PR-

Unternehmen die Aufsichtsbehörde veranlassten, sich mit dieser Branche zu beschäftigen.
Anlassabhängige Prüfungen bei einzelnen Unternehmen ließen es zweckmäßig erscheinen, dass die Aufsichtsbehörde zusätzlich jeweils vier "Vergleichsprüfungen" bei Unternehmen der gleichen Branche durchführte. Auf diese Weise konnte sich die Aufsichtsbehörde auch einen Überblick über die Besonderheiten der jeweiligen Branche verschaffen. Letztlich dient dies auch der Gleichbehandlung.

Bei den Arbeitsvermittlern stellte sich heraus, dass diese auf sehr unterschiedliche Art und Weise tätig sind. Eine Einrichtung sieht ihren Hauptzweck in einer weitgehenden Betreuung der Arbeitslosen; diese sollen u.a. lernen, wie eine Bewerbung auszusehen hat und wie ein Vorstellungsgespräch zu führen ist. Andere legen den Schwerpunkt auf Fortbildungsmaßnahmen der Arbeitslosen, wieder andere haben ihren Schwerpunkt in der Vermittlung. Außerdem gibt es Arbeitsvermittler als so genannte Head-Hunter, die sowohl Berater der Unternehmen als auch der Arbeitsplatzsuchenden - hauptsächlich solcher Personen, die ihren Arbeitsplatz wechseln wollen - sind.

Bei allen, außer der letzten Gruppe, musste festgestellt werden, dass Maßnahmen zum Datenschutz und zur Datensicherheit so gut wie nicht beachtet wurden. Auch die Arbeitsämter haben bei der Übermittlung der Arbeitslosendaten und der Zuwendung der Gelder an Arbeitsvermittler nicht darauf geachtet, dass diese die gesetzlichen Vorschriften einhalten. So war z.B. versäumt worden, die Organisation innerhalb der Schulungsaktivitäten so zu gestalten, dass Bewerberdaten und Lebensläufe nicht von Mitschülern auf dem Server eingesehen werden konnten. Ebenso gab es Mängel in der Bestellung eines betrieblichen Datenschutzbeauftragten bzw. bei der Ausübung der Tätigkeit der Datenschutzbeauftragten.

Bei den Aufsichtsbehörden verfestigte sich der zuvor bereits durch die Beschwerden gewonnene Eindruck, dass bei einem angespannten Arbeitsmarkt und in Zeiten der Umstrukturierung der staatlichen Arbeitsverwaltung der Schutz von Persönlichkeitsrechten von Arbeitssuchenden bei einigen datenverarbeitenden Stellen dieser Branche auf der Strecke bleibt.

Durch die Prüfungen konnte jedoch u.a. erreicht werden, dass persönliche Daten der Arbeitssuchenden künftig auf externen Datenträgern gespeichert werden und das Lehrpersonal überprüft, ob die erforderlichen Datenlöschungen vorgenommen wurden. Auch wurden auf Anregung der Aufsichtsbehörden Datenschutzbeauftragte bestellt bzw. deren Tätigkeit intensiviert. In diesen Bereichen werden in den kommenden Jahren weitere Prüfungen durchzuführen sein.

Bei den PR-Unternehmen konnte festgestellt werden, dass alle in der Hauptsache mit allgemein zugänglichen Daten arbeiten. Werden nicht-öffentliche Quellen genutzt, dann geschieht dies in der Regel mit Zustimmung der Betroffenen, die z.B. dem Unternehmen Lebensläufe zur Verfügung stellen, damit diese veröffentlicht werden.
Diese Unternehmen gingen jedoch alle von der irrigen Vorstellung aus, dass Daten aus allgemein zugänglichen Quellen nicht den Gesetzesvorschriften unterliegen würden. Sie mussten darüber belehrt werden, dass - auch wenn z.B. ein prominenter Politiker in der Öffentlichkeit eine bestimmte Zigarrenmarke bevorzugt und für diese in der Öffentlichkeit Werbung betreibt, in dem er die Zigarre in die Fernsehkameras hält - es sich gleichwohl um die Verarbeitung personenbezogener Daten handelt, wenn das PR-Unternehmen derartige Daten mittels EDV verarbeitet.
Wenngleich für die Verarbeitung von Daten aus allgemein zugänglichen Quellen gewisse Erleichterungen gelten, sind sie doch nicht von der Geltung des BDSG ausgenommen.

Auch die Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten war den Unternehmen schlichtweg fremd. Die Aufsichtsbehörde nutzte die Chance, an einen Dachverband dieser Branche heranzutreten und erhofft sich aus der Beratung des Verbands einen Multiplikationseffekt im Hinblick auf die übrigen Unternehmen, die diesem Verband angehören. Auch hier sind in den kommenden Jahren weitere Überprüfungen vor Ort durchzuführen; die Entwicklung bleibt zu beobachten.

Neben den dargestellten 16 "reinen" anlassunabhängigen Prüfungen wurden auch die 18 Überprüfungen aus konkretem Anlass (s.o. Nr. 1.4) überwiegend dazu genutzt, um die Datenverarbeitung der verantwortlichen Stellen umfassender zu prüfen. Die Prüfungen wurden also nicht nur auf den konkreten Beschwerdegegenstand beschränkt.
Hier musste häufig festgestellt werden, dass u.a. die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten nicht beachtet wurde, dass Datensicherheitsmängel bestanden und Weisungen gemäß § 11 BDSG fehlten. Zusätzlich wurden bei diesen Überprüfungen vor Ort häufig Videoüberwachungssysteme entdeckt, bei denen die datenschutzrechtlichen Anforderungen nicht beachtet wurden. In drei Fällen der Videoüberwachung von öffentlich zugänglichen Bereichen musste festgestellt werden, dass die Maßnahme weder zur Wahrnehmung des Hausrechtes noch zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich war. In anderen Fällen lagen zwar die Voraussetzungen des § 6b Abs. 1 BDSG vor, aber die Kennzeichnungspflicht des § 6b Abs. 2 BDSG wurde missachtet.

Auf Grund der Zunahme der Beschwerden und Eingaben hat sich die Gewichtung der anlassunabhängigen Prüfungen verschoben. Insgesamt kann die Zahl der Überprüfungen vor Ort mit der Entwicklung der Eingaben nicht Schritt halten. Dies führt bedauerlicherweise teilweise dazu, dass der Wahrheitsgehalt der schriftlichen Antworten der Unternehmen rückläufig ist.

Eine Überprüfung vor Ort ist Garant dafür, dass der Datenschutz in den Unternehmen nicht nur in der Theorie existiert, sondern auch in die Praxis umgesetzt wird. Zusätzlich kann durch Überprüfungen vor Ort auch die Tätigkeit des betrieblichen Datenschutzbeauftragten unterstützt werden.

7. Ordnungswidrigkeitenverfahren

Im Berichtsjahr wurden von den Aufsichtsbehörden sieben neue Verfahren nach dem Gesetz über Ordnungswidrigkeiten (OWiG) eingeleitet.

In zwei dieser Verfahren, die gemäß §§ 43 Abs. 1 Nr. 10, 38 Abs. 3 Satz 1 BDSG wegen der Nichterteilung von Auskünften an die Aufsichtsbehörde gegen die jeweiligen Geschäftsführer eines Medizingeräteherstellers und eines Reisebüros eingeleitet wurden, erbrachten die Anhörungen der Betroffenen neue entlastende Erkenntnisse zum Sachverhalt. Die Verfahren wurden daher gemäß § 47 Abs. 1 OWiG im Rahmen der pflichtgemäßen Ermessensausübung eingestellt.

Erstmals wurde gemäß § 43 Abs. 1 Nr. 3 BDSG ein Bußgeld wegen Verstoßes gegen die neue Bestimmung des § 28 Abs. 4 Satz 2 BDSG verhängt. Die Werbetreibenden haben nach dieser Vorschrift die Pflicht, bei jeder adressierten Werbung auf das Recht der Betroffenen hinzuweisen, dass diese der werblichen Nutzung ihrer Daten widersprechen können. Obwohl ein Verstoß gegen diese Regelung des BDSG bußgeldbewehrt ist und die Dachverbände der Direktmarketingbranche entsprechende Empfehlungen ausgesprochen haben, wird diese gesetzliche Verpflichtung von den Unternehmen der Werbewirtschaft immer noch in den wenigsten Fällen beachtet (siehe auch Nr. 16.1 und 16.2). Die Datenschutzaufsichtsbehörde hat daher im Berichtsjahr gegen einen Anbieter von Seminaren und Schulungen, der seine Veranstaltungen mit personalisierten Schreiben ohne den erforderlichen Hinweis auf das Widerspruchsrecht bewirbt, ein Bußgeld in Höhe von 1000,- Euro festgesetzt. Der Bußgeldbescheid hat inzwischen Rechtskraft erlangt. Das Unternehmen bringt den gesetzlich geforderten Hinweis nunmehr in geeigneter Form auf seinen Werbemailings an.

Ein weiteres Verfahren nach dem OWiG betraf eine Stelle, die personenbezogene Daten zum Zweck der Übermittlung speichert und seine Verfahren bei der Aufsichtsbehörde melden muss. Da nach mehrfacher Erinnerung an die Abgabe der neuen Registermeldung keine Reaktion des Unternehmens erfolgte, wurde gegen den Adresshändler ein Bußgeld in Höhe von 750,- Euro verhängt, das noch im Berichtszeitraum rechtskräftig wurde.

Drei Bußgeldverfahren mit einer Bußgeldsumme i.H.v. 1000,- Euro wurden zur Durchsetzung des Auskunftsanspruches der Aufsichtsbehörde i.S.d. § 38 Abs. 3 Satz 1 BDSG durchgeführt, nachdem Mahnungen, die Fragen der Aufsichtsbehörde zu beantworten, erfolglos geblieben waren.

In vielen anderen Fällen, in denen die Aufsichtsbehörden durch Beschwerden von Bürgerinnen und Bürgern auf Missstände bei der Verarbeitung ihrer Daten bei verarbeitenden Stellen aufmerksam gemacht wurden, konnten die Regierungspräsidien auf die Einleitung von Bußgeldverfahren verzichten. Auch wenn dabei deutlich wurde, dass die Grundbegriffe des Datenschutzrechts in einigen Betrieben weitgehend unbekannt sind und immer noch zu wenige Unternehmen ihre datenschutzrechtlichen Pflichten kennen und erfüllen, zeigten sich fast alle Unternehmen nach den Hinweisen der Datenschutzaufsichtsbehörden einsichtig und bemühten sich umgehend, bestehende datenschutzrechtliche Defizite zu beseitigen.

Ausgesuchte Probleme und Einzelfälle

8. Aspekte Internationaler Datenverarbeitungen

8.1 Abweichungen von den EU-Standardverträgen

Bei den im Berichtsjahr bearbeiteten Genehmigungsanträgen (s.o.) und bei zahlreichen entsprechenden Beratungsanfragen stellte sich die Frage, inwieweit beim Drittstaatentransfer Abweichungen von den EU-Standardverträgen gerechtfertigt sind.

Insbesondere die so genannte Drittbegünstigungsklausel, die sowohl in Klausel 3 des Standardvertrages vom 15. Juni 2001 als auch in Klausel 3 des Standardvertrages vom 27. Dezember 2001 enthalten ist, wird von den Unternehmen i.d.R. als überflüssig empfunden. Sie meinen, es reiche aus, wenn überhaupt geregelt ist, dass den Betroffenen Auskunft zu geben ist, dass die Daten ggf. zu löschen oder berichtigen sind.

Verträge werden jedoch nur zwischen den Vertragsparteien, hier also zwischen dem datenexportierenden und dem datenimportierenden Unternehmen geschlossen und haben grundsätzlich nur zwischen diesen (inter partes) Wirkung.
Gegenüber Dritten entfaltet die vertragliche Regelung also grundsätzlich keine Rechtswirkungen. Das heißt, betroffene Mitarbeiter oder Kunden können sich nicht selbst auf den Vertrag berufen, wenn die Vertragspartner unwillig sind, sich an den Vertrag zu halten. Die Berufung auf das BDSG hilft jedenfalls zunächst nicht, wenn die Verarbeitung im Drittstaat erfolgt.

Dritte können jedoch, obwohl sie nicht am Vertragsabschluss beteiligt waren, durchaus von den vertragsabschließenden Parteien als Begünstigte einbezogen werden (Vertrag zugunsten Dritter).

Daher wurde die Drittbegünstigungsklausel in den Genehmigungsverfahren vom Regierungspräsidium Darmstadt in Übereinstimmung mit der Arbeitsgruppe "Internationaler Datenverkehr" des Düsseldorfer Kreises als unverzichtbar angesehen. Die Art. 29-Gruppe hat bereits im Arbeitspapier 12 und jüngst im Arbeitspapier 74 die Bedeutung der Einräumung von drittbegünstigenden Rechten hervorgehoben.
Ob der Begriff "Drittbegünstigungsklausel" explizit verwendet werden muss, bleibt zu diskutieren, er ist evtl. verzichtbar, wenn aus der Regelung eindeutig hervorgeht, dass eine drittbegünstigende Regelung gewollt ist.

Ein weiterer Diskussionspunkt waren die Rechte der Aufsichtsbehörde.
Klausel 8 (2) des Standardvertrags vom 27. Dezember 2001 sieht vor, dass die Aufsichtsbehörde befugt ist, bei dem Datenimporteur im gleichen Maße und unter denselben Bedingungen eine Prüfung vorzunehmen, die gemäß dem anwendbaren Datenschutzrecht (BDSG) auf eine Prüfung des Datenexporteurs anzuwenden wäre. Folglich wären jederzeit anlassunabhängige Kontrollen beim Datenimporteur möglich.
Gemäß Klausel 5 e) des Standardvertrages vom 27. Dezember 2001 verpflichtet sich der Datenimporteur, die Feststellungen der Aufsichtsbehörde im Hinblick auf die Verarbeitung der übermittelten Daten zu respektieren.

Vor allem US-Unternehmen sind häufig nicht bereit, diese Regelungen zu akzeptieren. Sie scheinen unangekündigte Kontrollen und überzogene Forderungen der Aufsichtsbehörde zu fürchten.

Die Zusammenarbeit mit der Aufsichtsbehörde ist jedoch unerlässlich zur Gewährleistung ausreichender Garantien. Im Erwägungsgrund 15 bzw. Er-

wägungsgrund 8 der Entscheidungen vom 15. Juni und 27. Dezember 2001 betonte die EU-Kommission, dass die Kontrollstellen eine Schlüsselrolle in dem Vertragsmechanismus einnehmen (s. auch Arbeitspapier 74 der Art. 29-Gruppe).

Nach deutschem Recht ist es eine Selbstverständlichkeit, dass Unternehmen sich gegen rechtswidrige Forderungen der Aufsichtsbehörde wehren können. Wenn etwa die Aufsichtsbehörde die Genehmigung zum Drittstaatentransfer mit der Begründung widerrufen würde, dass der Datenimporteur ihre Forderungen nicht beachtet hat, könnte beispielsweise im Rechtsstreit um die Wirksamkeit des Widerrufs der Genehmigung die Rechtmäßigkeit der Forderung geprüft werden. Die Aufsichtsbehörde hat in dem Genehmigungsverfahren entsprechende Klarstellungen akzeptiert, allerdings erscheinen diese überflüssig.

Hinsichtlich der Kontrolle beim Datenexporteur hat die Aufsichtsbehörde eine einschränkende Regelung für ausreichend erachtet, welche dem Erwägungsgrund 8 der Entscheidung der EU-Kommission vom 27. Dezember 2001 entspricht. Danach ist es ausreichend, wenn die Aufsichtsbehörde in den Fällen eine Prüfung beim Datenimporteur vornehmen kann, in denen der Datenexporteur es ablehnt oder nicht in der Lage ist, dem Datenimporteur angemessene Anweisungen zu geben. Ob diese Abweichung akzeptiert werden kann, wird in jedem Genehmigungsverfahren freilich neu zu bewerten sein.

Aber schon angesichts der Kostenfrage müssen die Datenimporteure in den Drittstaaten nicht befürchten, mit ständigen Kontrollen der Aufsichtsbehörde konfrontiert zu sein. Von daher sollten die Unternehmen sehr genau überlegen, ob die Durchsetzung derartiger - praktisch relativ unerheblicher - Abweichungen von den Standardverträgen es wert sind, das letztlich aufwändige Genehmigungsverfahren durchzuführen. Bei wörtlicher Verwendung entfällt die Genehmigungspflicht.

Offensichtlich sind es jedoch hauptsächlich die Haftungsregelungen in den Standardverträgen, die zu Akzeptanzproblemen führen. Die Unternehmen wollen sich vielfach nicht der Gefahr ruinöser Schadensersatzprozesse nach US-Recht aussetzen (Sammelklagen, exorbitante Schadensersatzsummen). Die Aufsichtsbehörde hat daher in den entschiedenen Genehmigungsverfahren klarstellende Regelungen akzeptiert, wonach sowohl formell (Gerichtsstand, Prozessrecht) als auch materiell (§ 7 BDSG und BGB als Anspruchsgrundlagen) ausschließlich deutsches Recht gilt. Betroffene dürfen durch die Datenübermittlung nicht schlechter gestellt werden, als wenn die Verarbeitung komplett in Deutschland erfolgen würde, es besteht aber kein Anspruch, sie durch Anwendbarkeit von US-Recht besser zu stellen.

Es wäre wünschenswert, wenn die EU-Kommission bzw. die Art. 29-Gruppe eine entsprechende Klarstellung in die Standardverträge aufnehmen würde.

8.2 Bestimmungen in den Genehmigungsbescheiden nach § 4c Abs. 2 BDSG

Die von der Aufsichtsbehörde erteilten Genehmigungsbescheide enthielten u.a. folgende Bestimmungen:

Da Amtssprache Deutsch ist, ist in jedem Fall die vom Antragsteller vorzulegende deutsche Vertragsfassung bzw. -übersetzung maßgeblich. In weltweit tätigen Konzernen werden die Verträge oft ausschließlich oder zusätzlich in englischer Fassung unterzeichnet. Die Verantwortung für die Richtigkeit der Übersetzung liegt somit beim Datenexporteur und Antragsteller.

Auf Grund des durch Art. 26 Abs. 3 EG-DSRL erforderlichen Notifizierungsverfahrens enthält der Bescheid einen Widerrufsvorbehalt für den Fall, dass die EU-Kommission selbst oder ein anderer Mitgliedstaat der EU "Widerspruch" gegen die erteilte Genehmigung einlegen und die EU-Kommission daraufhin einen Widerruf oder eine Änderung der Genehmigung fordern sollte.

Außerdem wurden auf Grund Art. 4 der Entscheidung der EU-Kommission vom 27. Dezember 2001 weitere Widerrufsvorbehalte für folgende Fälle aufgenommen:

- Wenn feststeht, dass der Datenempfänger rechtlichen Anforderungen unterliegt, die mit demokratischen und rechtsstaatlichen Prinzipien nicht vereinbar sind und sich wahrscheinlich sehr nachteilig auf die vereinbarten Garantien auswirken, oder
- wenn die Aufsichtsbehörde festgestellt hat, dass der Datenexporteur oder der Datenimporteur die Vertragsklauseln nicht einhält, oder
- wenn eine hohe Wahrscheinlichkeit besteht, dass die Vertragsklauseln (künftig) nicht eingehalten werden und die Fortsetzung der Übermittlung den betroffenen Personen einen schwerwiegenden Schaden zufügen würde.

Darüber hinaus wurde geregelt, dass die Genehmigung nur gilt, wenn der Vertrag tatsächlich abgeschlossen wird und solange dieser Bestand hat.

8.3 Einschaltung eines Unterauftragnehmers im Drittstaat

Wenn ein Unternehmen seine Datenverarbeitung ganz oder teilweise an einen Datenverarbeitungsdienstleister in einem Drittstaat auslagern will, kann es das an sich erforderliche zeitaufwändige Genehmigungsverfahren gemäß § 4c Abs. 2 BDSG vermeiden, wenn es den EU-Standardvertrag vom 27. Dezember 2001 wortwörtlich verwendet (s. bereits oben Nr. 3 und 8.1 sowie 15. Tätigkeitsbericht, LT-Drucks. 15/4659, Nr. 7.2).

Nicht selten kommt es vor, dass der Datenverarbeitungsdienstleister im Drittstaat (Auftragsverarbeiter) seinerseits die Datenverarbeitung ganz oder teilweise an einen Unterauftragnehmer im Drittstaat auslagert.

Da der EU-Standardvertrag vom 27. Dezember 2001 dies nicht vorsieht und hierzu keine Regelungen trifft, stellt sich die Frage, ob die Beauftragung eines Unterauftragnehmers in einem Drittstaat überhaupt zulässig ist oder ob es hierfür doch individueller vertraglicher Regelungen und damit eines Genehmigungsverfahrens gemäß § 4c Abs. 2 BDSG bedarf.

Der Standardvertrag vom 15. Juni 2001 enthält - im Gegensatz zum Standardvertrag vom 27. Dezember 2001 - in Anlage 2 Nr. 6 sowie in Anlage 3 Nr. 3 ausdrücklich Regelungen dazu, unter welchen Voraussetzungen der Datenempfänger im Drittstaat die personenbezogenen Daten an einen Dritten weiter übermitteln darf und sieht hier drei Alternativen vor:

- Die Weiterübermittlung darf erfolgen, wenn Datenexporteur und Datenimporteur dem Beitritt eines weiteren, für die Verarbeitung Verantwortlichen zu den Klauseln, der dadurch zu einer Partei dieser Klauseln wird und dieselben Verpflichtungen wie der Datenimporteur eingeht, zugestimmt haben (Anlage 2 Nr. 6b; Anlage 3 Nr. 3b).
- Die betroffenen Personen haben der Weiterübermittlung eindeutig zugestimmt, falls besondere Arten personenbezogener Daten betroffen sind (Anlage 2 Nr. 6a, 1. Alternative; Anlage 3 Nr. 3a, 1. Alternative).
- Bei sonstigen personenbezogenen Daten: Die betroffenen Personen haben nach vorheriger umfassender Information die Möglichkeit erhalten, sich gegen die Weiterübermittlung auszusprechen (Anlage 2 Nr. 6a, 2. Alternative; Anlage 3 Nr. 3a, 2. Alternative).

Dieser Standardvertrag vom 15. Juni 2001 betrifft die Übermittlung an eine Stelle im Drittstaat, die nicht nur als weisungsgebundener Auftragsverarbeiter, sondern als verantwortliche Stelle mit eigenen Entscheidungsbefugnissen agiert (s. bereits 15. Tätigkeitsbericht, LT-Drucks. 15/4659, Nr. 7.2).

Welche Schlüsse aus dem Nicht-Vorhandensein entsprechender Regelungen im Standardvertrag vom 27. Dezember 2001 zu ziehen sind, ist zunächst fraglich.
Einerseits legt dies die Vermutung nahe, dass die EU-Kommission bei Verwendung des Standardvertrages vom 27. Dezember 2001 eine Datenweitergabe im Drittstaat gerade ausschließen wollte.
Andererseits könnte man folgern, dass die Weitergabe an einen bloßen (Unter-) Auftragsverarbeiter, der sich den Weisungen des Datenempfängers

unterwirft, möglich sein muss, wenn schon der Standardvertrag vom 15. Juni 2001 die Weiterübermittlung an sonstige Dritte zulässt.

Aus Sinn und Zweck ergibt sich Folgendes:
Die Einschaltung eines Unterauftragnehmers im Drittstaat kann nur zulässig sein, wenn der Auftraggeber hierzu ausdrücklich sein Einverständnis erklärt hat, und zwar nicht pauschal, sondern in Bezug auf den konkreten Unterauftragnehmer im Drittstaat, denn andernfalls würde der Auftraggeber seine Pflicht zur sorgfältigen Auswahl des Auftragsverarbeiters nicht erfüllen. Die Entscheidung über die Auswahl muss im Europäischen Binnenmarkt verbleiben.
Darüber hinaus kommt es maßgeblich darauf an, dass gewährleistet ist, dass der Betroffene seine Rechte bezüglich der beim Unterauftragnehmer erfolgenden Datenverarbeitung geltend machen kann.

Dies kann am besten durch einen Vertrag zwischen Auftraggeber und Unterauftragnehmer erfolgen, das heißt, diese schließen entweder separat den Standardvertrag vom 27. Dezember 2001 oder der Unterauftragnehmer wird von vornherein als Datenimporteur und damit als Vertragspartner in den Standardvertrag mit dem (Haupt-)Auftragsverarbeiter einbezogen. Rechtlich gleichwertig ist es, wenn der Unterauftragnehmer mit ausdrücklicher Zustimmung des Auftraggebers dem Standardvertrag beitritt und damit zur Vertragspartei wird und somit denselben Verpflichtungen wie der Auftragnehmer unterliegt. Auf diese Weise ist sichergestellt, dass Betroffene ihre Rechte geltend machen können und die Kontrollrechte des Auftraggebers und der Aufsichtsbehörde nicht ins Leere gehen, sondern auch gegenüber dem Unterauftragnehmer gelten.
Diese Auffassung wurde in der Arbeitsgruppe "Internationaler Datenverkehr" des Düsseldorfer Kreises abgestimmt.

9. Datenverarbeitung bei Banken

9.1 Kreditkartenzusendung ohne Kreditkartenvertrag

Der Wettbewerb im Bankenbereich wird immer härter, was u.a. dazu führt, dass die Banken kreative Marketingmaßnahmen durchführen, bei denen die Belange des Datenschutzes nicht immer hinreichend bedacht werden (s. bereits 15. Tätigkeitsbericht vom 26. November 2002 - LT-Drucks. 15/4659, S. 32, Nr. 9.1). Im Berichtsjahr versendete eine Bank an zahlungskräftige Kunden eine einsatzfähige Kreditkarte, ohne je einen Kreditkartenvertrag mit diesen Kunden abgeschlossen zu haben. Mit der ersten Zahlungstransaktion sollte der Kunde - quasi konkludent - den Kreditkartenvertrag abschließen. Wie eine derartige Konstruktion vertragsrechtlich zu bewerten ist, liegt nicht in der Zuständigkeit der Datenschutzaufsichtsbehörde. Datenschutzrechtlich kritisch ist jedoch, dass Personen Blankokreditkarten erhalten ohne irgendeine Form der vorherigen Benachrichtigung. Wenn die Briefsendung in falsche Hände gerät, sind Transaktionen zu Lasten des Betroffenen möglich und eine Entdeckung der Missbräuche ist erst mit den Monatsabrechnungen zu erwarten. Abgesehen von der schuldrechtlichen Problematik führt dies im Missbrauchsfall zu einer falschen Speicherung personenbezogener Daten und der Registrierung des Betroffenen - zumindest mit Kartennummer - in einer Missbrauchsdatei. Es bleibt dann nur zu hoffen, dass zwischen Täter und Opfer angemessen unterschieden wird. Die geschilderten Abläufe sind mit den in § 9 BDSG nebst Anlage beschriebenen technischen und organisatorischen Maßnahmen nicht zu vereinbaren.
Die Vorgehensweise ist daher sowohl unter Sicherheitsaspekten als auch wegen der potentiell möglichen Gefährdung schutzwürdiger Belange der Betroffenen nicht akzeptabel.

Im konkreten Fall kam ein weiteres Problem hinzu. Ein Dienstleistungsunternehmen ("Processor") war mit der weiteren Abwicklung des Kreditkartengeschäftes betraut. Dies hatte zur Folge, dass das Dienstleistungsunternehmen - ohne jede Vertragsgrundlage mit dem Betroffenen - personenbezogene Daten über den Kunden erhielt. In diesem Zusammenhang ist umstritten, ob der Dienstleistungsvertrag mit dem Processor eine Funktionsübertragung oder eine Dienstleistung nach § 11 BDSG darstellt.
Aus Sicht der Aufsichtsbehörde ist spätestens dann, wenn der Processor eigene Entscheidungsspielräume hat, z.B. Genehmigung von Limit-Überschreitungen, Bearbeitung von Reklamationen, Beitreibung von Außenständen, von einer Funktionsübertragung und damit einer Übermittlung an

einen Dritten im datenschutzrechtlichen Sinne auszugehen. Ohne vorherige vertragliche Regelung mit dem Kunden ist diese unzulässig. Die zwischen der Bank und dem Processor getroffenen vertraglichen Regelungen sprechen nach Auffassung der Aufsichtsbehörde eher für eine Funktionsübertragung. Wenn vertraglich eingeräumte Befugnisse faktisch vom Processor nicht ausgeübt werden - so die Darlegung der Bank - dann ist der Vertrag entsprechend zu ändern.

Die Klärung des Falles ist insoweit noch nicht abgeschlossen, u.a. weil die Aufsichtsbehörde eines anderen Bundeslands um Stellungnahme gebeten wurde, da der Konzern, zu dem die Bank gehört, dort ihren Sitz hat.

9.2 Nutzung des Verwendungszwecks

Durch Marketingideen kann auch die Gefahr entstehen, dass die Kunden - entgegen ihren Interessen - ausgeforscht werden.

Die professionelle Neugier der Marketingabteilung muss insbesondere vor den Angaben zum Verwendungszweck aus dem Zahlungsverkehr halt machen.

In einem Falle wurden Mietzahlungen, das heißt die entsprechende Auswertung des Verwendungszwecks aus Überweisungen bzw. Daueraufträgen, zum Anlass genommen, den betreffenden Kunden Angebote für Immobilienfinanzierungen zuzusenden. Das inhaltlich unqualifizierte Angebot konnte nicht kommentiert werden, jedoch verletzt eine systematische Auswertung des Verwendungszwecks regelmäßig die schutzwürdigen Interessen des Betroffenen. Derartige Auswertungen waren auch in der Vergangenheit unzulässig und wurden von den Aufsichtsbehörden regelmäßig beanstandet. Erfreulicherweise haben die betroffenen Banken jeweils ihr Fehlverhalten eingesehen und die Auswertung des Verwendungszwecks eingestellt, auch im konkreten Fall.

Der Phantasie der Marketingabteilungen - Kindergeldzahlungen führen zu Sparangeboten, Mietzahlungen zu Immobilienfinanzierungen usw. - sind offensichtlich keine Grenzen gesetzt. Der Gesetzgeber hat mit § 28 Abs. 1 und Abs. 2 bzw. Abs. 5 BDSG und der dort festgelegten Zweckbindung eindeutige Grenzen gezogen. Wie bereits unter Nr. 9.7 des 15. Tätigkeitsberichtes (LT-Drucks.15/4659, S. 34) ausgeführt, ist die Bank bzgl. der Angaben zum Verwendungszweck nur Bote für die Überbringung dieser Angaben. Die schutzwürdigen Belange der betroffenen Kunden stehen einer anderweitigen Nutzung dieser Daten entgegen. Hierauf muss immer wieder hingewiesen werden.

Eine nicht bestimmungsgemäße Nutzung und Verarbeitung der Angaben über den Verwendungszweck kann gemäß § 43 Abs. 2 Nr.1 bzw. Abs.1 Nr. 4 BDSG zumindest mit einem Bußgeld geahndet werden, unter Umständen käme eine Strafbarkeit gemäß § 44 BDSG in Betracht. Die Aufsichtsbehörden werden bei entsprechenden klaren, insbesonders bei wiederholten Verstößen, künftig von ihren neuen rechtlichen Möglichkeiten Gebrauch machen.

9.3 Probleme beim Ausscheiden von Mitarbeitern

In der jetzigen wirtschaftlichen Lage ist damit zu rechnen, dass weiterhin zahlreiche Bankmitarbeiter entlassen werden müssen bzw. Arbeitsverhältnisse einvernehmlich aufgelöst werden.

In einem Fall hatte ein leitender Mitarbeiter offensichtlich mindestens die Kundenadressen von zahlungskräftigen Kunden mitgenommen und diese vom neuen Arbeitgeber aus beworben. Die betroffene Bank bestand auf einer sofortigen Datenlöschung beim Wettbewerber, als sie davon erfuhr. Für die Aufsichtsbehörde, die auf Grund der Beschwerde eines betroffenen Kunden Kenntnis erhielt, machte dies jedoch weitere Recherchen nahezu unmöglich. Aus Sicht der Aufsichtsbehörde hätten die unbefugt genutzten Kundendaten beim Wettbewerber gesichert und dem Eigentümer (der betroffenen Bank) übergeben werden müssen. Auf diese Weise hätte sich die Dimension der Arbeitsvertrags- und der Datenschutzverletzungen abschätzen lassen.

Bei leitenden Bankmitarbeitern ist es sehr schwer - wenn nicht gar im Einzelfall unmöglich - die Nutzung der Kundendaten des früheren Arbeitgebers zu unterbinden. Wenn Daten für die Tätigkeit des Mitarbeiters zur Verfügung stehen müssen, hat dieser auch die potentielle Missbrauchsmöglichkeit.

In diesem Zusammenhang sollte sich eine Bank sehr gründlich überlegen, ob sie - schon im Eigeninteresse - wirklich allen Mitarbeitern außerhalb der Kundenregion den Zugriff auf alle Daten ermöglicht. Wie unter Nr. 9.8 des 15. Tätigkeitsberichtes der Landesregierung (LT-Drucks. 15/4659, S. 35) dargestellt, ist es ohnehin aus Datenschutzgründen geboten, den Zugriff auf Kundendaten regional und sachlich zu beschränken. Das Eigeninteresse an einem restriktiven Kunden-Datenzugriff dürfte für die Bank noch größer sein als die Datenschutzerfordernisse bzw. der geschilderte Fall zeigt, dass die Beachtung der Datenschutzerfordernisse auch den Eigeninteressen der Banken dient.

Im konkreten Fall empfahl die Aufsichtsbehörde außerdem, in den Kundendatenbestand mehrere Kontrolladressen zu integrieren. Mit diesen Kontrolladressen lassen sich Schwachstellen - zumindest nachträglich - erkennen. Vom unbefugten Nutzer dieser Kontrolladressen führt dann u.U. auch eine Spur zu einem ausgeschiedenen Mitarbeiter oder einem externen Serviceunternehmen. Nur mit hieb- und stichfesten Kontrolladressen lassen sich Missbräuche nachweisen und zivil- und datenschutzrechtlich ahnden. Die Kontrolladressen sollten von einer neutralen Instanz - z.B. der Revisionsabteilung - in den Kundenbestand integriert werden.

Zusätzlich kann es hilfreich sein, auch bei den Mitarbeiteradressen Kontrolladressen einzufügen, weil so auch eine unbefugte Nutzung der Mitarbeiterdaten nachgewiesen werden kann.

9.4 Abfrage von Auskunftei-Daten zu anderen als den angegebenen Zwecken

Die Möglichkeit, Bonitätsauskünfte über Dritte einholen zu können, scheint immer wieder auch zu Missbrauch zu verleiten, obwohl die gesetzliche Verpflichtung besteht, bei einer Auskunftseinholung das berechtigte Interesse hieran zu dokumentieren (§ 29 Abs. 2 Satz 2 und 3 BDSG).
Ein Mitarbeiter eines Kreditinstitutes forderte von einer Wirtschaftsauskunftei Bonitätsauskünfte über ein einzelkaufmännisch geführtes Immobilienunternehmen an. Im Rahmen der Nachforschungen durch die Aufsichtsbehörde konnte nicht abschließend geklärt werden, ob dem ein eigenes berechtigtes Interesse des Kreditinstitutes zugrunde lag oder ob der Mitarbeiter diesen Zugang lediglich für seine privaten Interessen nutzte. Er stand nämlich zuvor schon wegen eines privaten Immobiliengeschäfts mit dem betroffenen Unternehmen in Verhandlungen.
Dabei spielte eine Rolle, dass das von dem Mitarbeiter geltend gemachte Anfrageinteresse "Anbahnung einer Geschäftsverbindung" dem Sachverhalt nach eher fraglich war und das Vorliegen dieses Interesses beim Kreditinstitut nicht eindeutig belegt werden konnte.
Das Kreditinstitut stellte sich jedoch auf den Standpunkt, dass die Einholung einer Auskunft durch den Mitarbeiter selbst dann rechtmäßig gewesen wäre, wenn er diese nur für seine privaten Kaufinteressen hätte nutzen wollen.
Dem war entgegen zu halten, dass Bonitätsauskünfte in der Tat von jedermann eingeholt werden können, es dafür jedoch erforderlich bleibt, dass die tatsächlichen Interessen benannt und keine unzutreffenden Gründe vorgeschoben werden. Die Einholung einer Bonitätsauskunft unter Ausnutzung eines Arbeitgeberanschlusses, bei der Arbeitgeberinteressen vorgeschoben werden, jedoch ein privater Anlass zugrunde liegt, ist als datenschutzrechtlich unzulässig anzusehen.
Möchte ein Arbeitgeber seinen Mitarbeitern die günstigen Konditionen für solche Auskünfte zugänglich machen, bedarf es entsprechender Vereinbarungen mit der Auskunftei und detaillierter Regelungen gegenüber den Mitarbeitern, die auch die Nennung des tatsächlichen privaten Anfrageinteresses beinhalten. Soweit der Arbeitgeber keine solche Regelung trifft, ist es seine Pflicht, verdeckte Anfragen für private Zwecke zu untersagen und für die Einhaltung dieses Verbots Sorge zu tragen.
Eine Reihe von Beschwerden und Anfragen, welche Banken betrafen, standen im Zusammenhang mit der SCHUFA. Entsprechende Einzelfälle werden daher nachfolgend unter Nr. 10 dargestellt.

10. Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA)

10.1 Zustandekommen des SCHUFA-Scores

In Anknüpfung an Nr. 10.2 des 15. Tätigkeitsberichtes (LT-Drucks. 15/4659, S. 37) wird über den aktuellen Sachstand berichtet:

Die SCHUFA legte dem Regierungspräsidium Darmstadt im Berichtsjahr einen Aufsatz vor, der von den Verfassern der von der SCHUFA in Auftrag gegebenen Studie zur Wissenschaftlichkeit des Scoring-Verfahrens erstellt und auch veröffentlicht wurde (www.risknews.de). Außerdem erklärte sich die SCHUFA bereit, die Verfasser mit der Erstellung einer Kurzfassung der Studie in allgemeinverständlicher Form zu beauftragen und diese vorzulegen.
Die SCHUFA betonte, sowohl die Bundesbank als auch das Bundesaufsichtsamt für Finanzen hätten das auf dem logistischen Regressionsmodell basierende SCHUFA-Score-Verfahren positiv bewertet.

Wenngleich die Bewertung der Wissenschaftlichkeit des Verfahrens nicht zu den Kernaufgaben und -kompetenzen der Aufsichtsbehörde gehört, ist diese doch von Bedeutung für die Aufsichtsbehörde, denn sie ist für die Beurteilung erheblich, ob schutzwürdige Belange der betroffenen Bankkunden etc. entgegenstehen.

Neben der reinen Wissenschaftlichkeit ist nach Auffassung der Aufsichtsbehörde aber auch eine wertende Betrachtung geboten. Daher hielt sie die Einbeziehung der Selbstauskünfte in die Berechnung des Score-Wertes nicht für gerechtfertigt, selbst wenn es rein mathematisch zutreffend sein mag, dass ein gewisser Zusammenhang zwischen der Häufigkeit von Selbstauskünften und dem Kreditausfallrisiko besteht. Die SCHUFA hat nun ihre Zusage, die Selbstauskünfte aus der Score-Berechnung herauszunehmen, eingehalten. Die hierfür erforderliche Umstellung der Verfahren war Mitte 2002 abgeschlossen.

Die Aufsichtsbehörde verlangte weitergehende Auskunft bzgl. der tatsächlich genutzten Faktoren des Scorings. Daraufhin erklärte die SCHUFA, dass grundsätzlich alle gespeicherten Daten in die Score-Berechnung einfließen können.
Nicht genutzt werden jedoch Selbstauskünfte, Adresse, Geburtsort und bestrittene Daten.

Die Ausübung sonstiger datenschutzrechtlicher Rechte des Betroffenen, z.B. Berichtigung, Sperrung, kann bereits deshalb nicht in den Scoring-Wert einfließen, weil derartige Angelegenheiten zwar von der SCHUFA abgehandelt werden, wenn der Betroffene die Rechte geltend macht, aber die Tatsache der Geltendmachung der Rechte als solche nicht in dem SCHUFA-Datensatz des Betroffenen gespeichert wird. Die im Jahresbericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2002, Nr. 4.6.2 erhobene Forderung ist damit erfüllt.

Das SCHUFA-Scoring enthält - entgegen teilweise von Kritikern geäußerten Behauptungen - keine soziodemographischen Komponenten. Es wird also beispielsweise nicht ermittelt und nicht berücksichtigt, ob die Adresse dem sozialen Wohnungsbau zuzuordnen ist.

Ebenso wenig fließt die Nationalität einer Person in die Score-Berechnung ein. Diese wird ohnehin nicht als Merkmal gespeichert, über den Geburtsort wären jedoch unter Umständen gewisse Rückschlüsse auf die Nationalität der Person möglich. Indem der Geburtsort nicht verwendet wird, ist dies aber ausgeschlossen.

Die Aufsichtsbehörde hat für das Jahr 2003 eine Prüfung des Score-Verfahrens vor Ort bei der SCHUFA vorgesehen.

10.2 Auskunft über den Score-Wert und sonstige SCHUFA -Daten

Über die Praxis der Beauskunftung des Score-Wertes durch die SCHUFA wurde unter Nr. 10.3 des 15. Tätigkeitsberichts (LT-Drucks. 15/4659, S. 38) berichtet. Hier haben sich keine Änderungen ergeben, d.h. die SCHUFA

beauskunftet zwar den tagesaktuellen, nicht aber den übermittelten Score. Die Aufsichtsbehörde wird sich weiter dafür einsetzen, dass spätestens mit der Einführung einer neuen Software die übermittelten Score-Werte dem Betroffenen auf Wunsch mitgeteilt werden.

Bis dies umgesetzt wird, ist es im Interesse der Transparenz für die Betroffenen umso bedeutsamer, dass die Empfänger des Score-Wertes, also die SCHUFA-Vertragspartner, ihre gesetzlichen Auskunftspflichten erfüllen. Der übermittelte Score-Wert ist nach Auffassung der Aufsichtsbehörden ein personenbezogenes Datum, das - ebenso wie sonstige übermittelte SCHUFA-Daten - offensichtlich aus der automatisierten Verarbeitung der SCHUFA entnommen wurde. Unabhängig davon, in welcher Form der Score-Wert beim Vertragspartner gespeichert wird, ist er damit zu beauskunften (§ 27 Abs. 2 BDSG i.V.m. § 34 Abs. 1 BDSG).
Nach § 27 Abs. 2 BDSG ist es unerheblich, dass der Score-Wert nicht aus der eigenen automatisierten Verarbeitung des Vertragspartners, sondern aus derjenigen der SCHUFA stammt. Für die Anwendbarkeit des BDSG reicht es, dass er jedenfalls offensichtlich aus "einer" automatisierten Verarbeitung entnommen wurde (Simitis u.a., BDSG/Simitis, § 27, Rdnr. 31, 32; Gola/Schomerus, BDSG, § 28 Rdnr. 15).
Leider werden aber gleichwohl immer wieder von Banken Auskünfte an den Betroffenen über seine SCHUFA-Daten verweigert. Hierbei wird i.d.R. auf Nr. 3.10 des SCHUFA-Vertrages hingewiesen, der es den Banken angeblich untersagt, derartige Auskünfte auf Basis der vorliegenden SCHUFA-Auskunft zu erteilen. Diese Regelung besagt, dass Vertragspartner "sofern sich aus den Vorschriften des BDSG oder entsprechenden landesrechtlichen Regelungen nichts anderes ergibt, den Auskunftsinhalt gegenüber dem Betroffenen nur offen zu legen [berechtigt sind], wenn der Inhalt der Auskunft von den Angaben des Betroffenen abweicht."
Die Aufsichtsbehörde erörterte die Thematik mit der SCHUFA und es bestand hierbei Einigkeit, dass es zwar notwendig und gerechtfertigt ist, dass Vertragspartner die Anschlusskennung der Bank vertraulich behandeln. Diese Vertraulichkeit muss auch nach den technischen und organisatorischen Maßnahmen gemäß § 9 BDSG gefordert werden. Im übrigen aber muss die Bank gemäß § 34 BDSG vollständig Auskunft - auch über den Score - erteilen.

Diese Vorgehensweise ist nicht nur datenschutzrechtlich zwingend erforderlich, sie ist auch für alle Beteiligten sinnvoll, weil nur so eventuell falsche bzw. falsch zugeordnete Daten für den Betroffenen zeitnah offenkundig und kurzfristig bereinigt werden können.
Offensichtlich besteht bei einigen Banken die Befürchtung, in zeitaufwändige Diskussionen über die SCHUFA-Daten verwickelt zu werden, was mit der Verweigerung der Auskunft vermieden würde. Die Daten lassen sich jedoch überhaupt nur sehr begrenzt diskutieren, da die einmeldenden Unternehmen der Bank nicht bekannt sind. Es sollte deshalb bei Unklarheiten auf die Unmöglichkeit einer näheren Erörterung hingewiesen, das SCHUFA-Merkblatt übergeben, das Erfordernis einer SCHUFA Selbstauskunft mit **allen Daten** genannt und an die SCHUFA zur Klärung der Sachverhalte verwiesen werden.
Verursacher falscher Daten sind i.d.R. die Anschlusspartner der SCHUFA; hier können im Streitfall die jeweils regional zuständigen Datenschutzaufsichtsbehörden angesprochen werden.

Damit die SCHUFA-Vertragspartner künftig ihrer Auskunftsverpflichtung nachkommen, sollte auch die SCHUFA für eine Klarstellung sorgen. Die Aufsichtsbehörde forderte daher die SCHUFA auf, z.B. in der technischen Anleitung für das SCHUFA-Verfahren eine solche Klarstellung aufzunehmen.

10.3 Personenverwechslungen

Personenverwechslungen können für die Betroffenen sehr gravierende Auswirkungen haben. Seit der Umstrukturierung der SCHUFA ist das Regierungspräsidium Darmstadt verstärkt mit der Bearbeitung entsprechender Eingaben befasst.

Zu unterscheiden ist zwischen den Auskunftsverfahren der SCHUFA und den bloßen Anschriftenermittlungsverfahren.

Beim Anschriftenermittlungsverfahren erteilt ein Unternehmen (Gläubiger) über einen Schuldner, der unter Hinterlassung von Verbindlichkeiten mit unbekannter Adresse verzogen ist, einen Auftrag zur Anschriftenermittlung. Grundsätzlich hat der Gläubiger hierfür auch das Geburtsdatum des Schuldners anzugeben.
Wird der SCHUFA eine Anschrift bekannt, die den gesuchten Schuldner betreffen könnte, erhält der Auftraggeber darüber unaufgefordert eine Mitteilung. Die SCHUFA weist darauf hin, dass sie keine Gewähr für die Existenz und Richtigkeit übernehmen kann, da sie die gemeldete Anschrift von dritter Stelle erhalten habe. Dem Auftraggeber obliege daher die genaue Identitätsprüfung. Das Ergebnis der Identitätsprüfung ist der SCHUFA unverzüglich auf dem hierfür vorgesehenen Formular bekannt zu geben. Eine Postanfrage zur Anschriftenermittlung reicht nach den Vorgaben der SCHUFA nicht aus. Vielmehr ist die Identitätsprüfung ggf. durch Inaugenscheinnahme oder Unterschriftenvergleich sicherzustellen.

Die praktischen Auswirkungen des Verfahrens werden von der Aufsichtsbehörde kritisch beobachtet. Wenngleich hier keine Bonitätsdaten übermittelt werden, ist es jedenfalls geboten, auch bei der bloßen Anschriftenermittlung Verwechslungen möglichst bereits seitens der SCHUFA auszuschließen.

Stets erfolgt zunächst ein automatisierter Datenabgleich. Wenn hierbei eine eindeutige Zuordnung nicht möglich ist, erfolgt eine manuelle Bearbeitung durch eine Sachbearbeiterin oder einen Sachbearbeiter der SCHUFA.

In einem Beschwerdefall waren zwei Datensätze mit gleichem Namen und Geburtsdatum im SCHUFA-Datenbestand vorhanden. Als eine Suchanfrage einging, entschloss sich die Sachbearbeiterin, eine der beiden gespeicherten Adressen, die sie offensichtlich für die zutreffende hielt, im Hinblick auf den Suchantrag als "mögliche Anschrift" mitzuteilen.
Sie hätte jedoch diese Mitteilung zumindest mit dem Hinweis versehen müssen, dass zwei Adressen mit gleichem Namen und Geburtsdatum vorliegen. Damit hätte das anfragende Unternehmen eine Warnung erhalten, dass es die Identitätsprüfung mit besonderer Sorgfalt durchzuführen hat.

In einem anderen Fall war es bei zwei Personen gleichen Namens und Geburtsdatums in der Vergangenheit bereits zu einer Verwechslung gekommen. Die SCHUFA hatte daher in beide Datensätze einen wechselbezüglichen Nichtidentitätshinweis als internen Bearbeitungshinweis aufgenommen. Als dann jedoch eine Suchanfrage eines Inkassounternehmens bzgl. der einen Person, zu der Negativdaten gespeichert waren, einging, da diese unbekannt verzogen war, und kurz danach eine Auskunftsanfrage zu der Person gleichen Namens und Geburtsdatums, aber mit einer "dritten" Adresse, wurde diese dritte Adresse dem Inkassounternehmen als "mögliche" neue Adresse des Schuldners mitgeteilt.

Der Nichtidentitätshinweis hätte die Sachbearbeiterin jedoch veranlassen müssen, zumindest auf die nahe liegende Gefahr einer Personenverwechslung hinzuweisen. Tatsächlich stellte sich auch heraus, dass die dritte Adresse die neue Adresse des "guten" Schuldners war und nicht die des gesuchten "schlechten" Schuldners. In einem solchen Fall wäre aber auch ein entsprechender Hinweis auf die Verwechslungsgefahr unzureichend gewesen. Durch eine Frage nach der Voranschrift der Person mit der dritten Adresse hätte sich die Verwechslung vermeiden lassen.

Das "manuelle" Verfahren ist zwar eine zu begrüßende und unerlässliche Vorsichtsmaßnahme der SCHUFA, um Verwechslungen zu vermeiden. In beiden Fällen verfehlte sie jedoch ihr Ziel.

In beiden Fällen hatten auch die Vertragspartner, denen die Adressen mitgeteilt wurden, keine ausreichende Identitätsprüfung vorgenommen, sondern den Betroffenen unmittelbar mit Zwangsvollstreckungsmaßnahmen gedroht. Die SCHUFA rügte dies ausdrücklich. Gegenüber der Aufsichtsbehörde teilte sie mit, dass das Anschriftenermittlungsverfahren an einem SCHUFA-Standort zentralisiert wird. Hiermit soll zugleich die Kontrolle des Rücklaufs der Formulare mit dem Ergebnis der Identitätsprüfung verbessert werden.

Im eigentlichen Beauskunftungsverfahren, in dem Negativdaten und ggf weitere Daten bermittelt werden, sind besonders strenge Anforderungen an die Identitätsprüfung zu stellen.

Ohne Bedeutung ist, dass im Innenverhältnis zwischen SCHUFA und dem Vertragspartner auf Grund vertraglicher Vereinbarung dieser auch hier zur Prüfung der Personenidentität verpflichtet ist. Die SCHUFA ist als verantwortliche Stelle i.S.d. § 3 Abs. 7 BDSG selbst verpflichtet, nur richtige personenbezogene Daten zu verarbeiten. (s. bereits 1. Tätigkeitsbericht, LT-Drucks. 12/3069, Nr. 7.2.4, Simitis, BDSG/Mallmann, § 29, Rdnr. 124).

Nicht akzeptabel war es daher, dass die SCHUFA in dem oben geschilderten zweiten Fall bei einer Anfrage unter der dritten Adresse einfach die komplette Auskunft über den unbekannt verzogenen schlechten Schuldner übermittelte. Auch hier hätte bei der Anfrage unbedingt zunächst nach der Voranschrift gefragt werden müssen, um zu klären, welche der beiden gespeicherten Datensätze mit gleichem Namen und Geburtsdatum der neuen Adresse zuzuordnen ist.
In diesem Fall kam es darüber hinaus zu einem weiteren Fehler der SCHUFA.
Bei einer Auskunftsanfrage bzgl. des gespeicherten "guten" Schuldners wurde einfach zusätzlich der Datensatz des "schlechten" Schuldners übermittelt, d.h. der Nichtidentitätsnachweis wurde bei der Sachbearbeitung völlig ignoriert.

In einem anderen Fall führte ebenfalls ein eindeutiger Fehler seitens der SCHUFA zu einer Verwechslung.
Als ein Versandhändler, bei dem eine Betroffene erstmals eine Bestellung vornahm und Lieferung auf Rechnung wünschte, bei der SCHUFA unter der Angabe der Adresse und des Geburtsdatums anfragte, übermittelte die SCHUFA die Negativdaten einer anderen Frau gleichen Namens, obwohl hier eine andere Adresse und ein anderer Geburtsort gespeichert war. Zu der Versandhandelskundin war zum Zeitpunkt der Anfrage noch kein Datensatz im Datenbestand der SCHUFA gespeichert.
Die mit der Beauskunftung befasste Mitarbeiterin der SCHUFA entschied sich aufgrund des
übereinstimmenden Namens und der Übereinstimmung des Wohnortes, nur Straße und Hausnummer waren anders, sowie des ähnlichen Alters zu einer Datenübermittlung.
Die SCHUFA räumte gegenüber der Aufsichtsbehörde ein, dass hier eine Beauskunftung nicht hätte erfolgen dürfen, sondern zuvor die Identität hätte geklärt werden müssen. Aufgrund der telefonischen Reklamation der Verbraucherin bei einer Geschäftsstelle der SCHUFA war der Versandhändler noch am selben Tag von der Geschäftsstelle über die fehlerhafte Beauskunftung informiert worden.

In anderen Fällen waren z.T. auch Fehler der einmeldenden Bank ursächlich für Personenverwechslungen.

Es wäre reine Spekulation, wollte man angesichts der bekannt gewordenen Verwechslungsfälle auf die Dimension des Problems schließen. Ob es sich nur um "die Spitze des Eisbergs" handelt oder um eine, angesichts der Vielzahl der Auskünfte, welche die SCHUFA erteilt, doch geringe Verwechslungsquote, ist nicht festzustellen.

Fehler lassen sich sicher nie ganz ausschließen. Zu berücksichtigen ist auch, dass die Schuldnerverzeichnisverordnung die Veröffentlichung von eidesstattlichen Versicherungen etc. in den bei den Amtsgerichten geführten Schuldnerverzeichnissen auch zulässt, wenn Geburtsdatum und -ort fehlen. Gleichwohl wäre es nicht gerechtfertigt, die Verwechslungen einfach als unvermeidbar oder "Mitarbeiterfehler" hinzunehmen.

Die SCHUFA wird daher sämtliche ihr bekannten Verwechslungsfälle strukturiert aufarbeiten, um zu klären, inwieweit Verbesserungen notwendig und möglich sind. Auf dieser Basis wird sie überarbeitete Arbeitsanweisungen erstellen und der Aufsichtsbehörde vorlegen.

Sofortmaßnahmen wurden bereits ergriffen.
Die SCHUFA fragt verstärkt nach der Voranschrift. Die Vertragspartner sollen von vorn herein mehr Identifikationsdaten - vor allem Geburtsort, -datum und Voranschrift erfassen. Die Zahl der Verwechslungen kann damit erheblich reduziert werden.

Die Aufsichtsbehörde wird zu gegebener Zeit prüfen, ob die ergriffenen Maßnahmen insgesamt ausreichend sind.

10.4 Zusammenarbeit der SCHUFA mit eBay

Das Internet-Auktionshaus eBay verlangt eine namentliche Registrierung mit Adressenangabe von denjenigen, die sich an den Versteigerungsverfahren beteiligen wollen, da eine Vielzahl von Scheinbietern das Verfahren gefährdet.
Um die Echtheit der Angaben zu prüfen, vereinbarte eBay im Berichtsjahr eine Zusammenarbeit mit der SCHUFA. eBay erfragt bei der SCHUFA, ob die Identitätsangaben des Kunden zutreffend bzw. bekannt sind. Die SCHUFA antwortet nur mit "Ja" oder "Nein", sie übermittelt keine weiteren Daten. Auch dann, wenn es nahe liegt, dass nur ein versehentlicher oder absichtlicher Schreibfehler des eBay-Kunden vorliegt, übermittelt die SCHUFA nicht die wahren Daten.

Das Verfahren wurde auch vom Innenministerium Brandenburg geprüft, da dieses für eBay zuständig ist und in Übereinstimmung mit dem Regierungspräsidium Darmstadt und dem Hessischen Ministerium des Innern und für Sport als zulässig bewertet.

10.5 Wohnungsunternehmen als Vertragspartner der SCHUFA

Aufgrund eines Urteils des Bundesgerichtshofes vom 19. September 1985 zur damaligen Fassung der SCHUFA-Klausel (BGHZ 95, 362 ff) wurde das SCHUFA-Auskunftsverfahren neu organisiert und der Kreis der SCHUFA-Vertragspartner erheblich eingeschränkt. So erhielten u.a. Wohnungsvermieter keine Auskünfte mehr.
Es zeigte sich jedoch, dass gewerbliche Vermieter von Mietinteressenten regelmäßig die Vorlage einer SCHUFA-Selbstauskunft verlangten. Auf diese Weise erhielten Vermieter einen lückenlosen Überblick über die bei der SCHUFA gespeicherten Daten, also weit mehr Daten als selbst die A-Vertragspartner der SCHUFA, wie die Banken, erhalten. Da die Datenschutzaufsichtsbehörden nach dem BDSG keine Möglichkeit hatten, dieses Verfahren zu untersagen, wurde als datenschutzfreundlichere Alternative mit der SCHUFA vereinbart, die Wohnungsunternehmen wieder als Vertragspartner aufzunehmen. (Roßnagel/Duhr, Kapitel 7.5, Rdnr. 5.6).
Zunächst wurde hierzu in Hamburg ein Pilot-Projekt durchgeführt, bei dem die Vermieter Daten über nicht vertragsmäßiges Verhalten und Vollstreckungsmaßnahmen erhielten. Seit Einführung des Verfahrens war ein deutlicher Rückgang bei der Erteilung von Eigenauskünften für Mietinteressenten festzustellen (Roßnagel/Duhr a.a.O.).
Bei der Einführung des bundesweiten Anschlusses der gewerblichen Wohnungswirtschaft im Jahr 2001 wurde allerdings von der SCHUFA eine über den Inhalt der im Pilot-Projekt vereinbarten Klausel hinausgehende SCHUFA-Klausel zugrunde gelegt, was von den Datenschutzbehörden kritisiert wurde (Roßnagel/Duhr).
So sah die Klausel der SCHUFA vor, dass den Wohnungsunternehmen auch die Summe der monatlichen Belastungen der Mietinteressenten mitgeteilt werden sollten.

Damit würden die Wohnungsunternehmen mehr Daten erhalten als echte B-Partner (z.B. Versandhäuser), denn diese erhalten nur reine Negativdaten. Die Summe der monatlichen Belastungen stellt jedoch eine summarische Darstellung von Positivdaten (Höhe der ordnungsgemäß bedienten Kredite) dar, so dass im Grunde eine Zwischenform zwischen A- und B-Vertragspartnerschaft begründet worden wäre. Dies gab die SCHUFA jedoch auf, d.h. die neue Fassung der Klauseln für die Wohnungswirtschaft sieht keine Beauskunftung der Summe der monatlichen Belastungen vor.

Die Klausel sieht auch vor, dass die Vermieter Negativdaten melden, es geht jedoch nach wie vor nicht eindeutig hervor, was die Vermieter konkret zu melden haben. Die Formulierung "… wird der Vermieter der SCHUFA auch Daten aufgrund nichtvertragsgemäßen Verhaltens (z.B. Forderungsbetrag nach rechtmäßiger Kündigung gemäß § 543 Abs. 2 BGB) übermitteln…" würde es auch zulassen, dass sonstiges, nicht vertragsgemäßes Verhalten gemeldet wird.
Auf entsprechende Kritik der Aufsichtsbehörde versicherte die SCHUFA, dass nur Forderungsbeträge zu melden seien und ggfs. darauf folgende ge-

richtliche Titel und Vollstreckungsmaßnahmen, die sich aufgrund einer fristlosen Kündigung wegen unbestrittenen Mietrückstands mit zwei Monatsmieten gemäß § 543 Abs. 2 BGB ergeben. Die Klausel wurde im Berichtsjahr nicht entsprechend abgeändert, die Änderung wurde jedoch zugesagt.

Bei der Beauskunftung eines solchen Forderungsbetrages ist für den Empfänger nicht ersichtlich, dass die Forderung aus einem Mietverhältnis stammt, denn die Forderung wird grundsätzlich lediglich mit dem neutralen Merkmal "SD" (= Saldo) beauskunftet. Dieser Punkt wurde durch Umformulierung der Klausel klargestellt, denn Merkmale über die Aufnahme des Mietverhältnisses ("Mietkonto") werden danach nicht beauskunftet. Allerdings sollen andere Vermieter die Information erhalten, dass die Forderung aus einem Mietverhältnis stammt.

Abgesehen von der Problematik der Formulierung der SCHUFA-Klausel für Vermieter bestehen zwischen den Aufsichtsbehörden im Bundesgebiet unterschiedliche Ansichten darüber, ob Vermieter vollwertige B-Vertragspartner werden sollen oder ob eine Teilnahme am SCHUFA-System von vornherein nur in einer geschlossenen Benutzergruppe von Vermietern möglich sein soll. Die Vermieter erhielten dann nur die von anderen Vermietern gemeldeten Negativdaten und zusätzlich evtl. alle Schuldnerverzeichnisdaten (eidesstattliche Versicherung, Haftbefehl), da sich die Vermieter diese ohnehin bei den Amtsgerichten oder über andere Auskunfteien beschaffen könnten.

Wenngleich seit der Umstrukturierung der SCHUFA an sich nur das Regierungspräsidium Darmstadt für die SCHUFA zuständig ist, müssen Grundsatzfragen dieser Art bundesweit abgestimmt werden, da die Vertragspartner der SCHUFA in allen Bundesländern ansässig sind. Die weitere Abstimmung der Aufsichtsbehörden wird in der Arbeitsgruppe "SCHUFA/ Auskunfteien" des Düsseldorfer Kreises erfolgen. Dabei wird zu berücksichtigen sein, dass Konkurrenten der SCHUFA ebenfalls mit Vermietern zusammenarbeiten.

An dieser Stelle sei daher nur angemerkt, dass sowohl das Hessische Ministerium des Innern und für Sport als auch das Regierungspräsidium Darmstadt darum bemüht sind, eine Lösung herbeizuführen, die möglichst von allen Aufsichtsbehörden im Bundesgebiet mitgetragen wird.

Die Haltung der SCHUFA ist aus unternehmerischer Sicht verständlich. Außerdem ist zweifelhaft, ob durch eine geschlossene Benutzergruppe für Vermieter, das heißt ohne Negativdaten von anderen SCHUFA-Anschlusspartnern, das Problem der Selbstauskünfte gelöst werden kann.

11. Teledienste, Neue Medien, Internet-Provider

11.1 Speicherung der IP-Nummer durch Access-Provider

Das Regierungspräsidium Darmstadt hatte im Berichtsjahr aufgrund einer hohen Anzahl eingehender Anfragen und Beschwerden von betroffenen Internet-Nutzern die datenschutzrechtlich äußerst problematische Entscheidung zu treffen, ob die bei nahezu allen deutschen Internet-Zugangsanbietern seit Jahren praktizierte Protokollierung und Speicherung der an die Kunden vergebenen dynamischen IP-Nummer zulässig ist oder ob diese Daten künftig umgehend gelöscht werden müssen.

Da es sich bei dem von den Beschwerden betroffenen südhessischen Unternehmen um den größten Internet-Anbieter Deutschlands mit ca. 10 Millionen Vertragskunden handelte, war zu erwarten, dass die Entscheidung richtungsweisend für die gängigen Speicher- und Protokollierungspraktiken von Internet-Providern in anderen Bundesländern sein könnte, auch wenn es sich bei der datenschutzrechtlichen Beurteilung der Protokollierung des Providers um eine unternehmensspezifische Einzelfallentscheidung handelt.

Die IP-Nummer hat eine zentrale Bedeutung für die Funktion des Internet. Wenn ein Kunde sich in das Internet einwählt, erhält er eine IP-Nummer aus dem Bestand des Providers, mit der er sich im Internet gegenüber anderen Internet-Teilnehmern und Serverbetreibern anonym bewegen kann. Kein Internet-Dienst kommt ohne die Verwendung dieser Nummer, die als Kommunikationsadresse im Internet dient, aus. Ein Verbindungsaufbau ohne IP-Nummer ist nicht möglich, ohne IP-Nummer kann auch nicht im Internet

"gemailt", "gesurft", "gechattet", Dateien ausgetauscht oder anders kommuniziert werden. Diese IP-Adressen werden als "dynamisch" bezeichnet, weil sie dem Kunden nur für die Dauer einer Verbindung zugeteilt und nach dem Ende wieder freigegeben und einem anderen Kunden zugeteilt werden. Grund für die Verwendung dieses Verfahrens ist die mit der Verbreitung des Internet verbundene Verknappung verfügbarer IP-Adressen. Das Verfahren ist aus datenschutzrechtlicher Perspektive zu begrüßen, da durch den ständigen Wechsel der IP-Nummer eines Nutzers gegenüber anderen Internetnutzern und Diensteanbietern eine pseudonyme, wenn nicht sogar weitgehend anonyme Nutzung von Internet-Diensten im Sinne des § 4 Abs. 6 Teledienstedatenschutzgesetz (TDDSG) gewährleistet werden kann. Bei Zugangsprovidern wird befristet die Information gespeichert, welchem Kunde für welchen Zeitraum eine bestimmte IP-Nummer aus dem IP-Adress-Bestand des Providers zugeteilt war. Außer dem Zugangsprovider und dem Kunden selbst kann niemand eine entsprechende Zuordnung einer dynamisch vergebenen IP-Nummer zu einer Person vornehmen.

Die seit Jahren geführte Diskussion sowohl zwischen den Aufsichtsbehörden untereinander als auch mit den Unternehmen der Internet-Branche, ob es sich bei der dynamisch vergeben IP-Nummer überhaupt um ein personenbezogenes Datum im Sinne des § 3 Abs. 1 BDSG handelt, hat sich inzwischen beruhigt. In der datenschutzrechtlichen Fachwelt hat sich die Auffassung durchgesetzt, dass nicht nur für die Internet-Zugangsprovider sondern auch für viele Anbieter von Diensten und Inhalten im WWW die dynamisch vergebene IP-Nummer personenbeziehbar sein kann und alle an Personen vergebene IP-Adressen aus diesem Grund in den Anwendungsbereich datenschutzrechtlicher Vorschriften fallen.

In der Fachwelt heftig umstritten war und ist jedoch immer noch, ob die IP-Nummer nach dem Telekommunikationsgesetz (TKG) oder dem Recht der Tele- und Mediendienste (TDDSG, Mediendienste-Staatsvertrag MDStV) zu beurteilen ist. Für die Abgrenzung von Tele- und Telekommunikationsdiensten wird überwiegend das so genannte "Schichtenmodell" verwendet. Es unterscheidet die Ebene des Datentransports (Telekommunikation - TKG) von den Ebenen der Interaktion zwischen Nutzer und Anbieter (Teledienst /Mediendienst - TDDSG/MDStV) und den Inhalten der Kommunikation (BDSG). Die Antwort auf die Frage, ob ein Datum nun der Transport- oder eher der Dienstebene zuzurechnen ist, entscheidet gleichzeitig über die aufsichtsbehördliche Zuständigkeit von Bund und Ländern, da nach dem TKG für die Datenschutzaufsicht bei der Telekommunikation gemäß § 91 Abs. 4 TKG der Bundesbeauftragte für den Datenschutz und für die Aufsicht über Tele- und Mediendienste die Aufsichtsbehörden der Länder nach dem BDSG zuständig sind.

Der Gesetzgeber hat in § 2 Abs. 2 Nr. 3 Teledienstegesetz (TDG) das "Angebot zur Nutzung des Internet" und damit die Tätigkeit der Zugangsprovider als Teledienst eingeordnet. Auch die Bundesregierung geht im Evaluierungsbericht zum Informations- und Kommunikationsdienste-Gesetz (IuKDG, BT-Drs. 14/1191 S. 7f) ausdrücklich davon aus, dass es sich bei der "Vergabe der IP-Adresse" um ein Diensteangebot des Zugangs-Providers nach dem TDG handelt. Dennoch wird in der Fachwelt die gegenteilige Position vertreten, dass der reine Zugang zum Internet und die Vergabe der IP-Nummer durch den Einwahl-Server des Providers mehr zu den Steuerungsprozessen der Telekommunikation nach § 3 Nr. 16 TKG gehört, da dabei noch kein Teledienst erbracht wird und der Internet-Zugang sowie die IP-Nummern-Vergabe daher nach dem Telekommunikationsgesetz zu bewerten sind. Gemäß § 2 Abs. 1 TDG wird ein Teledienst immer mittels Telekommunikation erbracht, d. h. die Nutzung eines Teledienstes setzt zwingend Telekommunikation voraus. Gleichzeitig schließt § 2 Abs. 4 Nr. 1 TDG die Anwendung des TDG auf Telekommunikationsdienste im Sinne des TKG aus.

Zwischen den Datenschutzaufsichtsbehörden der Bundesländer und dem Bundesbeauftragten für den Datenschutz wurden die aufgrund der erheblichen Abgrenzungsprobleme zwischen Transportschicht und Diensteschicht entstehenden Zuständigkeitsfragen in der Vergangenheit immer in der Weise gelöst, dass die vor Ort für das inhaltliche Angebot und die Dienste eines Providers zuständige Aufsichtsbehörde sich auch mit Fragen des Internet-Zugangs befasste und bei Bedarf den Bundesbeauftragen für den Datenschutz über den jeweiligen Sachverhalt in Kenntnis setzte. Die Datenschutzauf-

sichtsbehörden der Länder und der Bundesbeauftragte für den Datenschutz haben sich darauf verständigt, dass im Sinne einer kontinuierlichen Rechtsanwendung diese Praxis der Zuständigkeitsverteilung auf die Aufsichtsbehörden der Länder und der praktischen Zusammenarbeit bis zum Inkrafttreten des neuen "Elektronische Medien Datenschutzgesetzes (EMDSG)" oder der anstehenden Novellierung des TKG, durch welche die Zuständigkeiten ggf. auf den Bundesbeauftragten für den Datenschutz übergehen werden, beibehalten bleibt.

Das Regierungspräsidium Darmstadt hatte den Bundesbeauftragten für den Datenschutz aus diesen Gründen bereits vor Jahren anlässlich der Bearbeitung einer Betroffeneneingabe davon in Kenntnis gesetzt, dass der Provider die seinen Kunden zugeteilte IP-Adresse über die Nutzungsdauer hinaus zu Zwecken der Abrechung gemäß § 6 Abs. 4 TDDSG speichert und die Datenschutzaufsichtsbehörde dies akzeptiert und nicht beabsichtigt, eine Beanstandung auszusprechen. Eine Reaktion des Bundesbeauftragten für den Datenschutz, der die Entwicklung des Datenschutzes bei Telediensten gemäß § 8 TDDSG beobachtet, blieb damals aus. Vom Bundesbeauftragten für den Datenschutz wurde weder die sachliche Zuständigkeit noch die damals geäußerte Rechtsauffassung der Aufsichtsbehörde in Frage gestellt oder kritisiert.

Zu Beginn des Berichtsjahres wandten sich nun mehrere Kunden des Providers an das Regierungspräsidium Darmstadt mit der Aufforderung, diese seit langem praktizierte Speicherung der vergebenen dynamischen IP-Nummer durch den Zugangsprovider aktuell datenschutzrechtlich zu überprüfen und diesem die Protokollierung zu untersagen. Zur Begründung wurde auf den von Online-Zeit und Übertragungsvolumen unabhängigen Pauschaltarif des Unternehmens für den Internetzugang über eine DSL-Netzwerkverbindung - so genannte "DSL-Flatrate" -, hingewiesen und damit argumentiert, dass im Gegensatz zu einem normalen zeitabhängigen Tarif bei einem Pauschaltarif immer der gleiche Betrag an den Provider zu entrichten sei und daher keine Abrechnungserforderlichkeit im Sinne des § 6 Abs. 4 TDDSG für die Aufbewahrung der einzelnen Protokolldatensätze mit den für bestimmte Zeiträume vergebenen IP-Adressen gegeben sein könne. Im Laufe der Zeit gingen immer mehr Eingaben von Betroffenen mit der selben oder einer ähnlichen Fragestellung bezüglich der Speicherpraxis des Providers bei der Aufsichtsbehörde ein. Noch während die Aufsichtsbehörde den Sachverhalt bei dem Unternehmen überprüfte, wurde das Thema in der überregionalen Presse und den Online-Medien aufgegriffen und teilweise sehr emotional in öffentlichen Internet-Foren diskutiert.

Weshalb die datenschutzrechtliche Beurteilung von IP-Adressen und die lediglich in Datenschutz-Fachzirkeln diskutierte aber in der Datenverarbeitungswelt wenig beachtete Frage plötzlich die Aufsichtsbehörde beschäftigte und ein enormes Medienecho hervorrief, liegt auf der Hand: Zeit- und volumenabhängige Pauschaltarife (so genannte "Flatrates") wurden immer erschwinglicher und populärer. Durch diese kostengünstige Möglichkeit eines Breitbandzugangs (DSL) können nun viel intensiver und länger Internet-Dienste genutzt und eine wesentlich größere Menge Daten aus dem Internet heruntergeladen werden, als dies noch vor einigen Jahren der Fall war. Bei vielen jungen Internet-Surfern steht deswegen die Nutzung von Internet-Tauschbörsen zum kostenlosen Herunterladen von umfangreichen Film- und Musikdateien im Vordergrund der Internetnutzung. Aufgrund der verstärkten Aktivitäten von Organisationen der Lizenz- und Rechteinhaber an Musik- und Filmtiteln steigen bei diesen Nutzern die Bedenken, dass sie durch das Herunterladen von lizenzrechtlich geschützter Musik und Filmen von Internet-Tauschbörsen gegen geltendes Recht verstoßen haben und sich strafbar bzw. schadensersatzpflichtig gemacht haben könnten.

Im vorliegenden Sachverhalt wurde der Provider mit der Bitte einer internationalen Rechteinhabervereinigung konfrontiert, die IP-Nummern aus seinem Adressbestand und dazugehörige Uhrzeiten von urheberrechtlich unzulässigen Nutzeraktivitäten auf internationalen P2P-Tauschbörsenplattformen im WWW vorlegten. Die Rechteinhaber baten das Unternehmen darum, seine betroffenen Kunden darauf hinzuweisen, dass das Anbieten und Herunterladen urheberrechtlich geschützter Musik- und Filmtitel unzulässig ist und die Rechteinhaber künftig versuchen werden, dies juristisch verfolgen und ahnden zu lassen. Der Provider reagierte auf die Aufforderung, indem er mit Hilfe der IP-Nummern-Protokolle die betroffenen Vertragskunden identifizierte und eine Ermahnung an diese versandte, was die Ängste der Betroffe-

nen vor einer Herausgabe ihrer Daten noch weiter steigerte und zu der geschilderten Welle von Beschwerdeeingängen und Anfragen bei der Aufsichtsbehörde führte. In keinem dieser Tauschbörsenfälle hat jedoch nach Erkenntnissen der Datenschutzaufsichtsbehörde eine Übermittlung der Daten eines IP-Nummern-Inhabers an die Rechteinhaber oder andere Stellen stattgefunden. Laut Presseberichten haben übrigens außerhalb Hessens ansässige Provider im Jahr 2003 ähnliche Abmahnungen durchgeführt.

Vor der Entscheidung über die Zulässigkeit der IP-Nummern-Speicherung wurde dem Unternehmen Gelegenheit gegeben, zur Sache Stellung zu nehmen. Der Provider legte daraufhin ein ausführliches Rechtsgutachten vor, das intensiv und kritisch mit dem Unternehmen besprochen wurde und wegen der grundsätzlichen Bedeutung des Falles auch den obersten Datenschutzaufsichtsbehörden der anderen Bundesländer und dem Bundesbeauftragten für den Datenschutz zur Kenntnis gegeben wurde. In einem Gesprächskreis der für den Datenschutz im nicht-öffentlichen Bereich zuständigen obersten Datenschutzaufsichtsbehörden der Bundesländer und des Bundesbeauftragten für den Datenschutz wurde die Fragestellung mehrfach eingehend diskutiert, leider ohne dass dabei eine vollkommene Übereinstimmung der beteiligten Dienststellen erzielt werden konnte. Aus einigen anderen Bundesländern gab es Einwände gegen die im folgenden dargelegte und begründete Rechtsauffassung des Regierungspräsidiums Darmstadt; die Mehrheit der Bundesländer äußerte sich nicht entgegengesetzt.

a) Die Speicherung der dynamischen IP-Nummer durch Internet-Zugangsanbieter zu Abrechnungszwecken nach § 6 Abs. 1 und 4 TDDSG

Die Aufsichtsbehörde ist nach gründlicher Abwägung der vorgetragenen Argumente zu der Rechtsauffassung gelangt, dass die durch einen Zugangs-Provider vergebene dynamische IP-Nummer nicht nur als Nutzungsdatum gemäß § 6 Abs. 1 TDDSG anzusehen ist, sondern auch als erforderliches Abrechnungsdatum im Sinne des § 6 Abs. 4 TDDSG beurteilt werden kann und somit auch über das Ende des Nutzungsvorganges hinaus gespeichert werden darf. Nach § 6 Abs. 1 TDDSG darf ein Diensteanbieter personenbezogene Daten der Nutzer (Nutzungsdaten) verarbeiten, soweit dies erforderlich ist, um die Inanspruchnahme von Telediensten zu ermöglichen oder abzurechnen. Daten, die für die Zwecke der Abrechnung erforderlich sind (Abrechnungsdaten), dürfen nach § 6 Abs. 4 TDDSG auch über das Ende des Nutzungsvorganges hinaus verarbeitet und genutzt werden.

Welche Datenarten unter die Kategorie "Abrechnungsdaten" fallen, kann nicht verallgemeinert werden.
Die Aufzählung der Datenarten in § 6 Abs. 6 TDDSG stellt zumindest keine gesetzliche Definition der "Abrechungsdaten" dar, sondern soll den Nutzer vor der Erstellung von Nutzungsprofilen schützen. Daher kann aus § 6 Abs. 6 TDDSG auch nicht geschlossen werden, dass die dort nicht erwähnte IP-Adresse nicht als Abrechungsdatum bewertet werden kann. Unter den Begriff der "Abrechnungsdaten" des § 6 Abs. 4 TDDSG fallen alle bei dem Provider anfallenden Nutzungsdaten, die für die Zwecke der Abrechnung mit dem Nutzer erforderlich sind. Der Gesetzgeber hat bei der Formulierung hier im Hinblick auf die verschiedenen möglichen abrechnungsrelevanten Verwendungen bewusst die Mehrzahl "Zwecke" gewählt. Mit der Vorschrift des § 6 Abs. 4 TDDSG sind also nicht nur die Datenarten erfasst, die der Kunde auf seiner Rechnung erhält oder mit denen z.B. die konkrete Höhe einer Rechnung ermittelt wird. Die Regelung des § 6 Abs. 4 TDDSG umfasst ebenso die Datenarten, die für den Access-Provider notwendig sind, um im Zweifelsfall die kostenpflichtige Erbringung einer Leistung wirklich korrekt und durchsetzbar nachweisen zu können. Bei der zentralen Frage des Vorliegens der gesetzlich bestimmten "Erforderlichkeit" sind also alle Belange der Abrechnung zu berücksichtigen, wozu auf jeden Fall die Fehlersicherheit und Revisionsfähigkeit eines Abrechnungssystems und damit korrespondierend ebenso die Nachweisbarkeit und die Durchsetzbarkeit einer auf die Abrechnung folgenden Forderung gehören. Diese Ziele sind ohne eine Speicherung der dynamisch vergebenen IP-Nummer nicht ohne wesentliche Qualitätseinbußen zu erreichen.

Die Art des Zuganges (analog, ISDN, GSM oder DSL) lässt im Übrigen noch keine Rückschlüsse auf das vom Kunden gewählte Tarifmodell zu. Die Information, welcher der vielen unterschiedlichen Tarife anzuwenden ist,

steht dem Einwahl-Server bei der Prüfung der Berechtigung des Kunden und bei der Vergabe der dynamischen IP-Nummer gar nicht zur Verfügung. Erst im Rahmen des deutlich später erfolgenden kaufmännischen Buchungsvorganges wird bei der Verarbeitung der in den Logfiles angefallenen Daten nach den unterschiedlichen Tarifmodellen differenziert. So können z.B. innerhalb des DSL-Flat-Tarifes eines Kunden auch Verbindungen über ISDN, Modem oder GSM aufgebaut werden, die dann nicht mehr pauschal, sondern zeitabhängig verrechnet werden. Da der Tarif DSL-Flat bei dem Provider nur für Hauptbenutzer gilt, werden die Verbindungen vorhandener Anschluss-Mitbenutzer des Flatrate-Kunden ebenfalls in Abhängigkeit von der jeweiligen Onlinezeit berechnet, ebenso wie das Abrufen kostenpflichtiger Inhalte auch für Flatrate-Kunden zusätzliche Kosten und Gebühren verursacht, die über die vergebene IP-Nummer abgerechnet werden.

Mit Hilfe der vergebenen und dokumentierten IP-Nummern bei "Flatrates" kann auch eine von Kunden behauptete Leistungsstörung widerlegt, bzw. der Umfang einer vorhandenen Leistungsstörung mit den zu bestimmten Zeiten vergebenen IP-Nummern umrissen werden. Sollten Kunden also mit Hinweis auf Leistungsstörungen beabsichtigen, die zu entrichtende Pauschale anteilig zu kürzen, kann das Unternehmen nur mit der Dokumentation über die zu dieser Zeit vom Einwahl-Server vergebenen IP-Nummern den Gegenbeweis antreten, ohne dass hierfür gleich die Inhalte der Nutzungen protokolliert werden müssten.

Die Speicherung der IP-Nummer dient also unabhängig vom gewählten Tarif der Kontrolle der Verfügbarkeit, Fehlersicherheit und Revisionsfähigkeit des Abrechnungssystems und ist aus diesem Grund zulässig nach § 6 Abs. 4 TDDSG

b) Die Speicherung der dynamischen IP-Nummer durch Anbieter von Internet-Zugängen als Maßnahme zur Datensicherheit nach § 9 BDSG

Die Speicherung der IP-Nummer durch den Zugangsprovider ist zudem zur Gewährleistung der Datensicherheit nach § 9 BDSG i. V. m. § 1 Abs. 2 TDDSG notwendig.

Aus der Tatsache, dass der Gesetzgeber im TDDSG die Datensicherheit, die Datensicherung, die Datenschutzkontrolle und den ordnungsgemäßen Betrieb einer Datenverarbeitungsanlage nicht erwähnt oder nur ansatzweise in Detailregelungen (§ 4 Abs. 4 Nr. 3 u. 4 TDDSG) streift, darf nicht geschlossen werden, dass das TDDSG an diesen Punkten eine Schwächung oder gar Nichtanwendbarkeit dieser grundlegenden Datenschutz-Vorschriften beabsichtigt, wozu eine umgehende Löschung der IP-Nummer faktisch führen würde. Es wäre auch geradezu widersprüchlich, wenn in dem an technischen, rechtlichen und tatsächlichen Unsicherheiten kaum noch zu überbietenden Regelungsgegenstand "Internet" mit den vielfältigen Sicherheitsdefiziten des aktuellen IPv4-Standards, auf die Anwendung von Kontroll-, Sicherungs- und Sicherheitsvorschriften verzichtet würde, die aber für andere, ungefährdetere Datenverarbeiter der "Offline-Welt" sehr wohl gelten und dort eingehalten werden müssen.

Beim TDDSG handelt es sich unstreitig um eine spezialgesetzliche Regelung im Sinne des § 1 Abs. 3 Satz 1 BDSG, die dem BDSG vorgeht. Wenn ein Tatbestand in einem Spezialgesetz keine Erwähnung findet, wird das BDSG dort aber auch nicht verdrängt. Mit der Subsidiaritätsregel des § 1 Abs. 2 TDDSG wird zudem klargestellt, dass eine Rechtsvorschrift wie § 9 BDSG auch im Anwendungsbereich des TDDSG, nämlich bei Telediensten zur Geltung kommt.

Die Speicherung und Verarbeitung der vergebenen dynamischen IP-Adresse durch einen Internet-Zugangsprovider stellt insoweit ein geeignetes Mittel zur Erreichung der Sicherheits- und Schutzziele des § 9 BDSG dar. Sie ist insbesondere zur Einrichtung einer wirksamen Zugriffskontrolle nach Nr. 3 und Eingabekontrolle nach Nr. 5 der Anlage zu § 9 BDSG, aber auch für die oft zeit- und personalaufwändige Analyse vergangener Angriffe und anderer Unregelmäßigkeiten (Portscans, Trojaneraktivitäten, DoS-Angriffe, Hacker-Attacken usw.) zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung unabdingbar notwendig, da Angreifer bei ihren Aktivitäten ihre IP-Adresse im Server- oder Firewall-Logfile des "Opfers" hinterlassen und

ein Angreifer dann nur anhand dieser Zusatzinformation (Zeitpunkt und IP-Adresse) von seinem Access-Provider ermittelt werden kann.

Der betroffene Provider ist als größter und bekanntester deutscher Zugangsanbieter auch den meisten Angriffsversuchen sowohl von außen als auch durch eigene Kunden ausgesetzt. Die hohe Schutzwürdigkeit der gefährdeten Daten auf den Datenverarbeitungsanlagen des Providers und vor allem auch der Daten seiner ca. 10 Millionen an das offene und unsichere Internet angeschlossenen Kunden steht außer Frage. Aus § 9 BDSG muss daher auch ein hoher einzuhaltender Sicherheitsstandard abgeleitet werden, der die Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Rechtsverbindlichkeit einer Datenverarbeitung gewährleisten kann. Ein ebenso geeignetes oder gar effektiveres Instrumentarium, das ohne die bei dem Internet-Zugangsprovider dokumentierte Information über die für einen bestimmten Zeitraum vergebene IP-Nummer ähnlich wirksam wäre, ist nicht zu erkennen.

In Diskussionen darüber, wie Sicherheitsziele nach § 9 BDSG auch ohne die gespeicherte IP-Adresse erreicht werden könnten, wird - auch mit Hinweis auf § 6 Abs. 8 TDDSG - immer wieder das Argument vorgetragen, eine solche Speicherung sei lediglich für die Zukunft bei konkret dokumentierten Missbrauchssituationen zulässig. Diese Argumentation greift jedoch nicht bei Internet-Zugangsanbietern, sondern allenfalls bei WWW-Inhalteanbietern, denn sie verkennt, dass es bei sofortiger Löschung der vergebenen IP-Adressen aus den Protokollen des Zugangsanbieters diesem im nachhinein nie mehr möglich wäre festzustellen, welcher seiner Kunden denn nun die konkrete Missbrauchssituation verursacht hatte. Alle rechtlich zulässigen Möglichkeiten, bei konkretem Verdacht eine in die Zukunft gerichtete Protokollierung vorzunehmen, würden somit bei einer sofortigen Löschung der IP-Adresse beim Internet-Zugangsanbieter zwangsläufig immer ins Leere laufen, wenn - wie so oft - lediglich die IP-Nummer und ein bestimmter Zeitpunkt als Anhaltspunkt für Nachforschungen zur Verfügung steht.

Nach gründlicher Abwägung aller rechtlichen und tatsächlichen Gegebenheiten kann in der Speicherung der IP-Nummer keine unverhältnismäßige Beeinträchtigung von Persönlichkeitsrechten der Nutzer erkannt werden, da die beim Zugangsprovider vergebene und protokollierte IP-Nummer nur irgendeine Nutzung des Internet dokumentiert und mit den beim Access-Provider über die Dauer der jeweiligen Online-Sitzung hinaus gespeicherten Daten ohne weitere Informationen kein Persönlichkeitsprofil gebildet werden kann. Die Daten darüber, welcher Natur eine Nutzung war, das heißt welche Seiten "angesurft" und welche Angebote bzw. Dienste konkret im weltweiten Internet genutzt wurden, wird von Internet-Zugangsprovidern nicht über die Dauer der Sitzung hinaus gespeichert, sondern umgehend gemäß § 4 Abs. 4 Nr. 2 TDDSG i.V.m. § 6 Abs. 4 TDDSG gelöscht.

Der Hessische Datenschutzbeauftragte gelangt in einem Rechtsgutachten, das für die Datenschutzbeauftragten der hessischen Hochschulen erstellt wurde, ebenfalls zu der Auffassung, dass eine Aufbewahrung bestimmter Nutzungsdaten, die zu Zwecken der Datensicherung und Datenschutzkontrolle gespeichert werden, zulässig ist (28. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Nr. 9.1.1.2, Nr. 9.1.2).

Die in den Gesprächen mit dem Unternehmen und den Aufsichtsbehörden der Bundesländer zu diesem Problemkreis aufgetretenen Fragen wurden mit dem Provider intensiv weiterdiskutiert. Das Unternehmen hat ein Berechtigungskonzept vorgelegt, aus dem hervorgeht, dass lediglich ein kleiner, eingegrenzter Personenkreis in dem Unternehmen in der Lage ist, den Zusammenhang zwischen der dynamischen IP-Adresse und einem Kunden herzustellen. Dabei wird bei jedem Zugriff auf die gespeicherten Daten geprüft, ob der Zugriff datenschutzrechtlich zulässig ist. Die Aufsichtsbehörde konnte erreichen, dass der Provider die Unterrichtung der Kunden über die Datenverarbeitung verbesserte und zudem sicherstellte, dass jeder Kunde Auskunft über die zu seinen Bestandsdaten gespeicherten IP-Nummern erhalten kann. Die Gespräche über die zulässige Höchstfrist der Datenspeicherung waren bei Redaktionsschluss für diesen Bericht noch nicht abgeschlossen.

Im Hinblick auf die beabsichtigten Gesetzesnovellen bleibt zu hoffen, dass auch eindeutigere Aussagen zur Zulässigkeit von Datenspeicherungen für Datensicherheitszwecke gemacht werden.
Es wäre im Ergebnis nicht sachgerecht, wenn die Zulässigkeit von Datensicherheitsmaßnahmen davon abhinge, ob die hierfür benötigten Daten auch für Abrechnungszwecke erforderlich sind, wie derzeit vielfach vertreten wird. Der Hessische Datenschutzbeauftragte hingegen ist in dem oben zitierten Gutachten zu dem sachgerechten Ergebnis gelangt, dass auch bei kostenlosem Internet-Zugang eine Speicherung der IP-Nummern der Nutzer zu Datensicherheitszwecken gerechtfertigt ist. Wenngleich diese Frage im konkreten Fall nicht entscheidend war, da - wie ausgeführt - nach Auffassung der Aufsichtsbehörde auch eine Abrechnungsrelevanz besteht, wobei die Unterscheidung der Zwecke insoweit nicht trennscharf ist, als man die Fehlersicherheit des Abrechnungssystems auch als Unterfall der Datensicherheit ansehen könnte, wäre eine klare Regelung wünschenswert.

Eine klare Regelung sollte auch zu der Frage getroffen werden, ob Datenspeicherungen erfolgen dürfen, um die Sicherheit des Internet als kommunikatives Gesamtgeflecht zu schützen. In der Tat kann man argumentieren, dass dies über den herkömmlichen Ansatz des § 9 BDSG hinaus geht, der dem Schutz der eigenen Datenverarbeitung dient.
Aber den Gegebenheiten des Internet wird eine derart isolierte Betrachtungsweise nicht gerecht. Bereits jetzt ist es üblich, dass Provider ihre Nutzer auffordern, Angriffe auf fremde Systeme einzustellen, wenn bekannt wird, dass sie bei anderen Providern massive Datensicherheitsprobleme hervorrufen. Könnte der Provider die Verursacher nicht anhand der IP-Nummer identifizieren, bliebe für den anderen Provider oft nur die Möglichkeit, den gesamten Adressbereich des Providers zu sperren, dessen Kunde den Angriff verursacht hat. Dies würde bedeuten, dass alle Kunden des "verursachenden" Providers von der Nutzung anderer Internet-Angebote ausgeschlossen würden. Auch wenn der Provider im konkreten Fall darlegen konnte, dass sein eigenes Access-System bereits durch eigene Nutzer erheblich bedroht wird, wäre eine explizite Regelung wünschenswert.

11.2 Die Nutzung von E-Mail-Adressen zu Werbezwecken

Zur datenschutzrechtlich zulässigen werblichen Nutzung von E-Mail-Adressen, also zur legalen Zusendung von Werbe-E-Mails oder auch Newsletter-Mitteilungen, benötigt die für die E-Mail-Versendung verantwortliche Stelle die ausdrückliche informierte Einwilligung des betroffenen Inhabers der E-Mail-Adresse (zur Flut der unverlangten E-Mail-Werbung siehe auch 15. Tätigkeitsbericht, LT-Drucks. 15/4659, Nr. 8.8). Im Gegensatz zur "Offline-Welt", in der das "Opt-Out-Prinzip" (Widerspruchsrecht) gegen personalisierte Briefwerbung gilt, muss der Versender in der "Online-Welt" nach dem "Opt-In-Prinzip" verfahren. Es muss also bereits vor der ersten werblichen Nutzung einer E-Mail-Adresse eine entsprechende Willenserklärung des Betroffenen vorliegen, die den Transparenz-Anforderungen des § 4 Abs. 2 und 3 TDDSG genügt. Die Einwilligung des Inhabers der Adresse muss durch eine bewusste und eindeutige Handlung des Nutzers erfolgen, sie muss protokolliert werden sowie jederzeit als Nachweis abrufbar und auch widerrufbar sein.

Diese datenschutzrechtlichen Anforderungen an zulässige E-Mail-Werbung wurde von den führenden Verbänden der deutschen Online-Wirtschaft und der Direktmarketing-Branche (ECO e.V., DDV, DMMV) bereits weitgehend in Richtlinien und Empfehlungen an ihre Mitglieder ("erwünschtes E-Mail-Marketing", "Permission-Marketing") umgesetzt. Die Verbände empfehlen hier das sogenannte "Double-Opt-In"-Verfahren, bei dem an den WWW-Surfer nach Eingabe seiner E-Mail-Adresse auf einer WWW-Seite eine Bestätigungs-E-Mail versandt wird, die vom Inhaber der Adresse nochmals zurückgesandt werden muss, damit die Einwilligung als erteilt, der Newsletter als bestellt gilt. Diese Methode ist besonders datenschutzfreundlich, da auf diese Weise recht einfach gewährleistet werden kann, dass die E-Mail-Adresse authentisch ist und nicht von einem unberechtigten Dritten missbräuchlich im WWW angegeben wurde. Dieses "Double-Opt-In"-Verfahren wird inzwischen von vielen marktüblichen Newsletter-Programmen und CRM-Tools (Customer-Relationship-Management) automatisiert unterstützt, und wird, neben einigen Sonderlösungen und solange sich noch kein Verfahren zur sicheren elektronischen Signatur am Markt durchgesetzt hat, zur Zeit als rechtssichere und gleichzeitig für die Unter-

nehmen und Diensteanbieter praktikable Methode zur Einholung einer Online-Einwilligung von den Datenschutzaufsichtsbehörden anerkannt.

Eine Einwilligung ist allerdings nur erforderlich, soweit die E-Mail nicht zur Begründung, inhaltlichen Ausgestaltung oder Änderung eines Vertragsverhältnisses im Sinne des § 5 TDDSG dient, was bei der Zusendung von Reklame- und Werbe-E-Mails in der Regel auch nicht zutrifft.

Im Berichtsjahr gingen nun einige Eingaben von Kunden eines südhessischen Internet-Anbieters bei der Aufsichtsbehörde ein, in denen diese sich darüber beschwerten, dass ihnen der Provider Werbe-E-Mails zusenden würde, ohne dass hierfür eine Einwilligung nach den o.a. Vorschriften gegeben worden wäre. Der Provider bezog in seiner Stellungnahme zu diesen Vorgängen die an das Wettbewerbsrecht angelehnte Position, dass er für diese Nutzungen der E-Mail-Adressen keine Einwilligungen seiner betroffenen Kunden benötige, da es sich bei der E-Mail-Versendung um eine "Information im Rahmen eines bestehenden Vertragsverhältnisses" handeln würde.

Bei der Einzelfallprüfung der versandten E-Mails stellte die Aufsichtsbehörde fest, dass einige der E-Mails einen eindeutig werblichen Charakter hatten. Entweder wurden sogar schon im Betreff der E-Mail reklameartig neue Waren angepriesen, die in einem bei dem Provider gehosteten Online-Shop erstanden werden konnten oder es wurde im E-Mail-Text sogar für andere Unternehmen geworben, ohne dass irgendwelche vertragsrelevante Mitteilungen zu finden waren. Nach Auffassung der Aufsichtsbehörde dienten diese E-Mails ganz eindeutig nicht der "inhaltlichen Ausgestaltung eines Vertragsverhältnisses", für die § 5 TDDSG als Rechtsgrundlage für die Nutzung der E-Mail-Adressen in Frage kommen könnte. Und selbst wenn diesen Reklame-E-Mails - wie es das Unternehmen beanspruchte - der Status von "Informationen im Rahmen eines bestehenden Vertragsverhältnisses" nach der Terminologie des Wettbewerbsrechts hätte zugebilligt werden können, würde dies den höheren datenschutzrechtlichen Ansprüchen an eine zulässige Nutzung der E-Mail-Adressen nicht genügen. Zudem hat der Gesetzgeber für das in der Online-Welt geltende TDDSG die werbliche Nutzung von personenbezogenen Daten gerade an eine Einwilligung gebunden. Dieser wichtige Grundsatz würde durch den Versuch, § 5 TDDSG als Rechtsgrundlage für die werbliche Nutzung in Anspruch zu nehmen, geradezu konterkariert.

Die Aufsichtsbehörde machte gegenüber dem Provider deutlich, dass E-Mails, die ohne Einwilligung an eigene Vertragskunden versendet werden, und die daher der inhaltlichen Ausgestaltung eines Vertragsverhältnisses dienen müssen, nicht überwiegend Werbebotschaften und konkrete reklameartige Waren- oder Dienstleistungsangebote enthalten dürfen. Selbstverständlich kann die Werbung für weitere Unternehmen erst recht nichts mit dem bestehenden Vertragsverhältnis zu tun haben und ist deshalb ebenfalls nicht von § 5 TDDSG abgedeckt. Allenfalls Mitteilungen über Änderungen der Tarife, der AGB, neue Dienste, Updates der für die Nutzung der Dienste benötigten Software etc. können ohne Einwilligung der Betroffenen auf Grundlage des § 5 TDDSG per E-Mail versandt werden. Es liegt in der Natur der Sache, dass sich nicht immer eindeutig klären lassen wird, wo denn nun die Nutzung von E-Mail-Adressen der Kunden zur "inhaltlichen Ausgestaltung eines Vertragsverhältnisses" endet und wo die "Nutzung zu Werbezwecken" beginnt. In den bearbeiteten Beschwerdefällen konnte es aber keinen Zweifel an dem eindeutig reklameartigen Charakter der E-Mails geben. Auf die Beanstandung durch die Datenschutzaufsichtsbehörde hat der Provider durch eine entsprechende Umstellung beim Versand von E-Mails an die Kunden reagiert. Die seither versendeten Kundeninformationen sind immer auch vertragsrelevant im Sinne des § 5 TDDSG. Die Zusendung von Werbung und Newsletter-Mitteilungen per E-Mail muss nun ausdrücklich von den Betroffenen angefordert werden.

Die Aufsichtsbehörde weist die Versender von E-Mail-Werbung in diesem Zusammenhang regelmäßig auch darauf hin, dass Empfänger zunehmend gereizt auf alles reagieren, was nach unaufgeforderter E-Mail aussieht, weil unbekannte und unseriöse E-Mail-Massenversender seit einiger Zeit die E-Mail-Postfächer der Internet-Nutzer mit ihren suspekten Werbebotschaften, dem so genannten "Spam" fluten. E-Mails kommen nur dann gut an, wenn sie erwünscht sind. Unangeforderte E-Mail-Werbung verärgert die potentiel-

len Kunden, beschädigt den Ruf des Unternehmens oder seiner Produkte und verursacht letztlich nicht unerhebliche Kosten.

11.3 Die Nutzung von E-Mail-Adressen zur Parteiwerbung

Durch eine Betroffeneneingabe wurde die Aufsichtsbehörde darauf aufmerksam gemacht, dass auch politische Parteien die neuen Medien inzwischen für ihre Zwecke nutzen. Im vorliegenden Fall wurde anlässlich einer hessischen Wahl von einem Abgeordneten ein Wahlaufruf per E-Mail versandt, gegen den sich ein Betroffener mit dem Hinweis auf die nicht erteilte Einwilligung wandte, insbesondere weil der Absender auf die Bitte, seine Adresse von der E-Mail-Adressenliste zu löschen, nicht reagierte.

Die Versendung von E-Mails und so genannten "E-Cards" (elektronische Grußkarten) durch politische Parteien war bereits mehrfach Gegenstand von Verfahren vor den Zivilgerichten (LG München, 05.11.02, Az.: 33 O 17030/02, LG Berlin, 20.09.02, Az.: 15 O 560/02, AG Rostock, 28.01.03, Az.: 43 C 68/02). In den Urteilen wurde u.a. klargestellt, dass politische Parteien bei der Nutzung von E-Mail-Adressen kein Privileg gegenüber anderen Versendern genießen und dass das direkte Versenden von E-Mails ohne ausdrückliche Einwilligung des Adressen-Inhabers neben anderen Beeinträchtigungen immer auch eine Verletzung von Persönlichkeitsrechten darstellt.

Die Aufsichtsbehörde empfahl dem Versender dringend, künftig eine Nutzung von E-Mail-Adressen zum Versand von politischer Werbung oder von Aufrufen nur bei Vorliegen der Einwilligung der Betroffenen vorzunehmen. Der Versender sagte zu, diese Form der Wahlwerbung künftig nicht mehr durchzuführen. Im Übrigen habe man im Beschwerdefall lediglich versehentlich nicht geantwortet. Andere Beschwerdeführer hätten sowohl eine Auskunft über die Datenherkunft gemäß § 34 Abs. 1 BDSG als auch eine Löschungsbestätigung erhalten. Die zum Wahlaufruf und zur Wahlwerbung benutzten E-Mail-Adressen wurden zwischenzeitlich ohnehin gelöscht, da es negative Rückmeldungen aus der Bevölkerung zu der E-Mail-Kampagne gab und man erkannt habe, dass sich diese Werbeform für Wahlaufrufe und zur Wahlwerbung nicht eignet.

11.4 Keine Privilegien bei der werblichen Nutzung von "geschäftlichen" E-Mail-Adressen

Ein im Adresshandel tätiges Unternehmen wollte sein Geschäftsfeld um den Handel mit "geschäftlichen" E-Mail-Adressen erweitern und bat die Aufsichtsbehörde um datenschutzrechtliche Bewertung. Die Anwälte des Unternehmens vertraten die Auffassung, dass es für die werbliche Nutzung sogenannter "geschäftlicher" E-Mail-Adressen keiner Einwilligung der Adresseninhaber bedürfe. Unter "geschäftlichen" E-Mail-Adressen verstanden sie solche, die Arbeitnehmern und Geschäftsführern vom Arbeitgeber im Rahmen der beruflichen Tätigkeit zur Verfügung gestellt werden. Der Adresshändler wollte diese E-Mail-Adressen aus öffentlichen Quellen und im Internet zusammensuchen. Es lag weder eine Einwilligung vor, noch wurde den Betroffenen Gelegenheit zum Widerspruch gegen die werbliche Nutzung der E-Mail-Adresse gegeben.

Zur Begründung der angenommenen datenschutzrechtlichen Zulässigkeit des Vorhabens wurde in Anlehnung an die - in der Offline-Welt für die Briefwerbung und den Handel mit Postanschriften geltenden - Interessenabwägung des § 29 Abs. 2 S. 1 Nr. 1a und Nr. 2 i.V.m. § 28 Abs. 3 S. 1 Nr. 3 BDSG argumentiert. "Geschäftliche" E-Mail-Adressen unterlägen zudem einer geringeren Schutzwürdigkeit als "private" E-Mail-Adressen, da sie im Internet frei zugänglich seien und ohnehin der Kontaktaufnahme dienen würden. Im Übrigen sei das Persönlichkeitsrecht von Betroffenen im gewerblichen Bereich deutlich weniger schutzbedürftig als in seiner privaten Umgebung.

Die Datenschutzaufsichtsbehörde konnte dieser Rechtsauffassung allerdings nicht folgen.
E-Mail-Adressen, die in der Form "Vorname.Nachname@firma.de" oder ähnlich vom Arbeitgeber an Beschäftigte vergeben werden, sind einer natürlichen Person zugeordnet, die letztlich auch bestimmbar ist. Es handelt sich somit um ein personenbezogenes Datum im Sinne des § 3 Abs. 1 BDSG.

Die "geschäftliche" E-Mail-Adresse ist vor diesem Hintergrund datenschutzrechtlich nicht anders zu bewerten, als eine private E-Mail-Adresse. Nur wenn es sich um eine wirklich "neutrale" E-Mail-Adresse, z.B. in der Form "info@firma.de", "abteilung@firma.com", "service@firma.de" oder "kontakt@firma.com" handelt, ist grundsätzlich anzuerkennen, dass es an dem für die Anwendung datenschutzrechtlicher Vorschriften erforderlichen Personenbezug mangelt und keine Persönlichkeitsrechte einer bestimmten oder bestimmbaren natürlichen Person beeinträchtigt werden.

Da sich das Vorhaben aber nicht auf solche "neutralen" E-Mail-Adressen beschränkte, war selbst bei Anwendung des weniger strengen "Offline-Rechts" kein gesetzlicher Erlaubnistatbestand für das geplante Vorhaben des Adresshändlers im BDSG zu erkennen, da der Gesetzgeber in den einschlägigen Vorschriften der §§ 28, 29 BDSG der Beachtung schutzwürdiger Interessen der Betroffenen einen hohen Wert eingeräumt hat. Es handelt sich bei dem geplanten Vorhaben um die Verarbeitung personenbezogener Daten, deren Zweckbestimmung ausschließlich in der Übermittlung und anschließenden "Online-Nutzung" zu Werbezwecken liegt, ohne dass eine Einwilligung des Betroffenen hierfür vorhanden wäre. Da dies - im Gegensatz zur herkömmlichen Briefwerbung - nach einschlägiger Rechtsprechung offensichtlich wettbewerbswidrig nach dem UWG ist und es hierfür zusätzlich auch nach dem Recht der Teledienste einer ausdrücklichen und dokumentierten Einwilligung der Betroffenen bedarf, besteht Grund zur Annahme, dass ein schutzwürdiges Interesse der Betroffenen an dem Ausschluss der Verarbeitung im Sinne des § 28 Abs. 1 Nr. 2, 3 und Abs. 3 Nr. 3 BDSG sowie des § 29 Abs. 1 Nr. 2 und Abs. 2 Nr. 2 BDSG vorliegt, das offensichtlich die wirtschaftlichen Interessen der verantwortlichen Stelle an der Verarbeitung überwiegt.

Im Berichtsjahr gab es auf europäischer Ebene einige Fortschritte im Sinne des Daten- und Verbraucherschutzes. Während zu Beginn der Diskussion um die "Europäische Datenschutzrichtlinie für elektronische Kommunikation" (RL 2002/58/EG) bei Europarat und Europäischem Parlament unterschiedliche Haltungen zur werblichen Nutzung von E-Mail-Adressen anzutreffen waren, hat man zwischenzeitlich zu einer gemeinsamen Position gefunden, nach der die werbliche Nutzung von E-Mail-Adressen in den Mitgliedsländern in der Regel nur mit ausdrücklicher Zustimmung des Empfängers zulässig sein soll. In der zumeist wettbewerbsrechtlichen Rechtsprechung und der einschlägigen juristischen Fachliteratur hat sich inzwischen die Meinung durchgesetzt, dass die unaufgeforderte Zusendung von E-Mails entweder als "Verletzung des allgemeinen Persönlichkeitsrechts" oder als "Eingriff in den ausgeübten Gewerbebetrieb" zu bewerten und daher rechtswidrig ist. Zudem ist eine entsprechende Änderung des Gesetzes zur Bekämpfung des unlauteren Wettbewerbs (UWG) geplant, die bei Redaktionsschluss für diesen Bericht aber noch nicht umgesetzt war. Auch die großen Verbände der deutschen Online-Wirtschaft und Direktmarketing-Branche nehmen eine Unterscheidung zwischen privaten und geschäftlichen E-Mail-Adressen nicht vor, sondern propagieren das "erwünschte Online-Direktmarketing", das ausschließlich von den Wünschen der Empfänger abhängt.

11.5 Recht auf pseudonyme Inanspruchnahme von Telediensten umgesetzt

Bereits im letzten Tätigkeitsbericht wurde von den Problemen berichtet, die es einem großen Internetprovider in Südhessen bereitete, seinen Kunden die anonyme oder zumindest pseudonyme Inanspruchnahme seiner im Internet angebotenen Teledienste im Sinne des § 4 Abs. 6 TDDSG zu ermöglichen (LT-Drucks. 15/4659, Nr. 8.4).

Diese datenschutzrechtlichen Unzulänglichkeiten beruhten auf der historisch gewachsenen und programmtechnisch bedingten Verknüpfung der Adressen in den Diensten "E-Mail" und "Usenet" (Newsgroups) mit der Adressierung der eigenen Homepage im WWW sowie der dort befindlichen Anbieterkennzeichnung, also dem Impressum nach dem Teledienstegesetz (TDG) und dem Mediendienste-Staatsvertrag. Durch diese Verkoppelung konnten mehrere hunderttausend Homepage-Kunden des Providers die Dienste "E-Mail" und "Usenet" letztlich nicht pseudonym in Anspruch nehmen, da sie über die leicht auffindbare WWW-Hompage und das dort befindliche Impressum bis zur Wohnanschrift genau identifiziert werden konnten.

Hiergegen beschwerten sich auch immer wieder betroffene Nutzer bei der Aufsichtsbehörde.

Nachdem das Unternehmen nach einigem Drängen der Aufsichtsbehörde bereits im letzten Berichtsjahr zugesagt hatte, diese gegen das Pseudonymitätsgebot des § 4 Abs. 6 TDDSG verstoßende Koppelung der verschiedenen Teledienste im Rahmen größerer technischer Umstellungen in den Serverparks künftig aufzuheben, wurde diese Ankündigung zum Ende des aktuellen Berichtszeitraums auch zufriedenstellend umgesetzt. Die seit Jahren im Header jeder E-Mail und jedes Newsgroup-Beitrags vorhandene Teilnehmernummer, wird nun von dem Provider nur noch verschlüsselt und dabei immer wieder neu generiert hinzugefügt. Weiterhin wurde das System der Adressierung der Kunden-Homepages einer grundlegenden Überarbeitung und Erneuerung unterzogen. Ein Rückschluss von einer E-Mail-Adresse des Providers auf eine Anbieterkennzeichnung innerhalb einer Kunden-Homepage kann nun von den betroffenen Kundinnen und Kunden problemlos durch eine entsprechende Namenswahl für ihre jeweiligen Adressen verhindert werden.

11.6 Schutz vor E-Mail-Verwechselungen: Einführung einer Karenzzeit beim Wechsel des E-Mail-Namens

Das Medium E-Mail erfreut sich in der Bevölkerung immer größerer Beliebtheit. Viele Bürgerinnen und Bürger nehmen die umfangreichen Angebote der oftmals sogar kostenlosen E-Mail-Provider gerne an und besitzen mehrere E-Mail-Adressen, von denen Sie zielgerichtet zu unterschiedlichen Zwecken Gebrauch machen (z.B. zur Spam-Vermeidung; vgl. LT-Drucks. 15/4659, Nr. 8.8).

Im Berichtsjahr kam es nun zu mehreren Eingaben bei der Aufsichtsbehörde, in denen sich Kunden und E-Mail-Nutzer eines marktführenden Internet-Providers aus dem Rhein-Main-Gebiet darüber beschwerten, dass ihnen unter einem neu vergebenen E-Mail-Namen E-Mails zugestellt wurden, mit denen sie nichts anfangen konnten und die offensichtlich für andere Personen bestimmt waren. Dabei handelte es sich sowohl um kommerzielle Informationen und Werbe-E-Mails, als auch um private Schreiben und sogar vertrauliche Konto- und Depotmitteilungen. Die Petenten vermuteten regelmäßig, dass der ihnen zugeteilte E-Mail-Name von dem Provider doppelt vergeben worden sei und ein anderer Kunde nun ebenso die an sie selbst gerichteten E-Mails lesen könnte. Die Eingaben führten immer wieder zu Nachforschungen durch die Aufsichtsbehörde und den betrieblichen Datenschutzbeauftragten des Internet-Providers.

Dabei stellte sich in allen Fällen heraus, dass die vermeintlich "doppelt vergebenen" E-Mail-Namen erst kurz zuvor von anderen Kunden gekündigt und danach sofort wieder den Betroffenen neu zugeteilt worden waren. Die fraglichen E-Mail-Namen waren zuvor teilweise nur kurz, teilweise auch über Jahre hinweg in Benutzung und ihre ehemaligen Inhaber hatten es versäumt, ihren Kommunikationspartnern eine entsprechende Mitteilung über ihren Adressenwechsel zukommen zu lassen und Werbung, Newsletter oder sogar vertrauliche Bankmitteilungen ab- oder umzubestellen. In einigen Fällen entstand sogar der Eindruck, dass einige Nutzer ihre E-Mail-Namen ganz gezielt regelmäßig wechselten oder nur für eine bestimmte Zeit oder eine bestimmte Kommunikation benutzten und diesen dann wieder ablegten, ohne dies irgendwem mitzuteilen. Auch wenn die geschilderten Folgen dieses Verhaltens für den Adressennachfolger zwar unangenehm sind, ist es datenschutzrechtlich selbstverständlich vollkommen zulässig, seine E-Mail-Adressen häufig zu wechseln. Die Folgen dieses Verhaltens können nicht dem Provider angelastet werden, der lediglich E-Mails an gültige, einmal vergebene E-Mail-Adressen zustellt.

Dennoch verursachte die sofortige Neuvergabe von "abgelegten" E-Mail-Adressen an andere Kunden durch die anschließenden vermeintlichen Falschzustellungen von E-Mails und die darauf folgenden Beschwerden empörter und unzufriedener Kunden so viel Verwirrung und Unannehmlichkeiten, dass sich das Unternehmen entsprechend den Anregungen der Datenschutzaufsichtsbehörde bereit erklärte, bei der Vergabe von E-Mail-Adressen eine Karenzzeit einzuführen. Auf diese Weise werden die unerwünschten Nebeneffekte des Wechsels von E-Mail-Adressen abgemildert.

Zum Redaktionsschluss dieses Berichts teilte der Provider seinen Kunden mit, dass für abgelegte E-Mail-Adressen künftig eine Sperrfrist von 40 Tagen gilt, falls diese mehr als drei Tage in Benutzung waren. Auf diese Weise wird den Versendern die Möglichkeit gegeben, auf die eingehenden Fehlermeldungen wegen nicht zustellbarer E-Mails an abgelegte E-Mail-Adressen zu reagieren und ihr Adressbuch bzw. ihre E-Mail-Adressenliste um diesen Eintrag zu bereinigen. Die durch diese Maßnahme bei einem Provider mit mehreren Millionen Kunden eintretende Verkleinerung des zur Verfügung stehenden E-Mail-Adressenraums muss im Interesse der verbesserten Transparenz und Nachvollziehbarkeit des Gesamtsystems für die E-Mail-Kunden hingenommen werden.

11.7 Verschlüsselungs- und Signaturlösung mit GPG/PGP ersetzt unsicheres Verfahren bei der DENIC e.G.

Durch einen kritischen Artikel einer Computerfachzeitschrift wurde die Aufsichtsbehörde darauf aufmerksam, dass es bei der deutschen Vergabestelle für Internet-Domains der Top-Level-Domain ".de", der DENIC e.G. in Frankfurt am Main, jahrelang möglich gewesen sei, mit etwas Fachkenntnissen und ohne besonderen Aufwand die Registrierungsinformationen aller deutschen Internet-Domains zu manipulieren.

Aufgrund der extrem hohen Anzahl von täglichen Änderungen in dem Datenbestand der DENIC e. G. wird der Änderungsdienst durch die hierzu berechtigten Provider weitgehend automatisiert nach einem festgelegten Standard per E-Mail abgewickelt. Dieser programmgesteuerte Datenaustausch mittels so genannter "Robots" war lediglich mit unzureichenden Sicherheitsmerkmalen ausgestattet, die im Laufe der Jahre überdies einem immer größer werdenden Personenkreis - insbesondere bei den beteiligten Providern - zur Kenntnis gegeben werden mussten. Ein möglicher systematischer Missbrauch dieser Sicherheitslücke mit kriminellen Absichten hätte z.B. durch Abänderungen und Fälschungen der den Domains jeweils zugeordneten Nameserver-Einträge einzelne Domains "umleiten" und im Extremfall sogar die Funktionsfähigkeit des "deutschen Internets" erheblich beeinträchtigen können.

Obwohl solche Manipulationsfälle bis zu diesem Zeitpunkt nicht aufgetreten waren, wurde die DENIC e. G. von der Datenschutzaufsichtsbehörde zur Stellungnahme aufgefordert. Die DENIC e.G. wurde insbesondere auf § 9 BDSG hingewiesen. Diese Vorschrift verpflichtet verantwortliche Stellen, die personenbezogene Daten verarbeiten, geeignete technisch-organisatorische Maßnahmen zur Datensicherheit zu treffen und damit unter anderem einen ausreichenden Zugriffsschutz zu gewährleisten (Nr. 3 der Anlage zu § 9 BDSG) und die Eingabekontrolle (Nr. 5 der Anlage zu § 9 BDSG) sowie die Verfügbarkeitskontrolle (Nr. 7 der Anlage zu § 9 BDSG) sicherzustellen.

Die deutsche Domainvergabestelle reagierte umgehend auf die Veröffentlichungen und das Tätigwerden der Datenschutzaufsichtsbehörde, indem übergangsweise eine Passwortsicherung für die änderungsberechtigten Provider eingeführt wurde. Inzwischen wurde für alle Domain-Aufträge eine sichere Authentifizierung mit einem geeigneten GPG/PGP-Verfahren verbindlich eingeführt, das den Sicherheitsanforderungen des § 9 BDSG genügt.

12. Warndateien, Prangerseiten im Internet

Im Berichtsjahr wurden erneut Anfragen an die Aufsichtsbehörde gerichtet, die die Zulässigkeit von Warndateien betrafen.

Ausgangspunkt dafür war stets die Geschäftsidee, "schwarze Schafe" unter den Kunden einer bestimmten Branche bekannt zu machen, und so die angeschlossenen Kaufleute, Handwerker, Freiberufler oder sonstigen Auftragnehmer vor riskanten Geschäftsbeziehungen zu warnen bzw. eingehende Warnungen weiter zu geben.

Die Idee, subjektive Äußerungen der Angeschlossenen zur Zahlungswilligkeit bzw. Zahlungsfähigkeit von Geschäftspartnern zu übermitteln, musste von vornherein als datenschutzrechtlich unzulässig bewertet werden. Solche nicht verifizierbaren Beurteilungen greifen unzumutbar in das Persönlichkeitsrecht der Betroffenen ein.

Aber auch die Variante, bei der nur die objektive Tatsache übermittelt werden sollte, dass ein Zahlungstitel gegen einen bestimmten Geschäftspartner erstritten werden musste, ist nicht unproblematisch, weil sie an den Vorgaben des BDSG für die Auskunfteitätigkeit zu messen ist. So konnte beispielsweise die Vorstellung mancher potentieller Betreiber solcher Internet-Warndateien, nicht sie selbst, sondern die Einmeldenden seien gegenüber den Betroffenen für die Richtigkeit der veröffentlichten Daten verantwortlich, nicht akzeptiert werden, der Betreiber kann lediglich im Innenverhältnis zum Einmeldenden die Verantwortung abwälzen bzw. Regress vereinbaren. Insoweit wird auf die Ausführung im 15. Tätigkeitsbericht, LT-Drucks. 15/4659, Nr. 8.1 verwiesen.

Da der Aufwand für eine auskunfteimäßige Führung solcher Warndateien nicht gering ist, wurden die der Behörde bekannt gewordenen Geschäftsideen bislang nicht realisiert.

13. Versicherungen

13.1 Widerruf einer Schweigepflichtentbindungserklärung missachtet

Patientendaten unterliegen der ärztlichen Schweigepflicht. Wollen Versicherungen im Rahmen der Leistungsprüfung die Auskunft des behandelnden Arztes einholen, müssen sie zuvor eine Schweigepflichtentbindungserklärung einholen.

Der Widerruf einer Schweigepflichtentbindungserklärung ist unbedingt zu beachten, auch wenn dies dazu führt, dass die Versicherung daraufhin ihre Leistungsprüfung einstellt und der Versicherte dadurch u.U. nicht in den Genuss der von ihm beantragten Versicherungsleistung kommt.

Im Rahmen der Leistungsprüfung für die Auszahlung einer Berufsunfähigkeits-Zusatzrente forderte eine Versicherung vom Betroffenen eine Kopie des vollständigen Entlassungsberichts seiner Reha-Klinik. Der Betroffene übersandte die Unterlagen nur auszugsweise und berief sich darauf, dass die geschwärzten bzw. gekürzten Passagen für die Beurteilung der Leistungspflicht nicht relevant seien. Als die Versicherung wiederholt den vollständigen Bericht anmahnte, widerrief der Versicherungsnehmer auch seine zuvor erteilte Schweigepflichtentbindungserklärung gegenüber der Versicherung. Gleichwohl forderten die zuständigen Versicherungssachbearbeiter den vollständigen Reha-Entlassungsbericht nun bei der Klinik an und erhielten diesen auch.
Dies wurde von der Aufsichtsbehörde beanstandet. Das Versicherungsunternehmen musste daher die in der Leistungsprüfung eingesetzten Mitarbeiter darauf hinweisen, dass der Widerruf von Einwilligungen unverzüglich zu beachten ist und im Zweifel eine Rückfrage beim Betroffenen erfolgen muss, um den tatsächlichen Willen des Betroffenen und die evtl. eintretenden Konsequenzen für ihn abzuklären.

13.2 Unzulässige Datenübermittlung für Werbezwecke

Ein anderes Versicherungsunternehmen übermittelte die Daten von Interessenten, die sich ein Angebot zur "Riesterrente" erstellen ließen, ohne deren Kenntnis an das Schwesterunternehmen, eine Krankenversicherungsgesellschaft. Diese unterbreitete den Betroffenen unaufgefordert Krankenversicherungsangebote.

Zunächst berief sich das Versicherungsunternehmen darauf, dass die Datenübermittlung allein auf Initiative einiger Außendienstmitarbeiter erfolgt sei, räumte dann jedoch ein, dass die Vertriebsgesellschaft Initiator gewesen sei und dass von Anfang an geplant war, die Interessenten nach dem aktuellen Krankenversicherer zu befragen, um ihnen dann ein konzerneigenes Krankenversicherungsangebot zu unterbreiten.
Offensichtlich war man sich der datenschutzrechtlichen Problematik dieses Vorgehens bewusst, weil die Krankenversicherungsangebote von den Versicherungsvertretern nur persönlich übergeben und nicht mit der Post verschickt werden sollten.

Das Versicherungsunternehmen musste die Aktion stoppen und die betroffenen Vertriebsstellen anweisen, die Daten ausschließlich im Rahmen der Zweckbestimmung zu nutzen.

13.3 Preisgabe von Daten an Nachbarn

Im Rahmen der Bearbeitung einer Eingabe musste festgestellt werden, dass eine bisher bei den Versicherungen als "üblich" beschriebene Vorgehensweise zumindest zu Problemen führen kann.

Bei Recherchen im Schadensfall gehen Versicherungsmitarbeiter vor Ort und befragen u.a. beteiligte Personen bzw. die Nachbarschaft. Im Rahmen dieser Befragungen sind im Beschwerdefall den Nachbarn auch Daten bekannt gemacht worden, deren Mitteilung aus Sicht der Aufsichtsbehörde für die Bearbeitung des Falles nicht erforderlich war. Konkret ging es um einen Unwetterschaden an einem Baum und einer Garage. Um die Angaben des Versicherungsnehmers zu überprüfen, erfolgte die Befragung des Nachbarn. Datenerhebungen bei Dritten sind im Hinblick auf den Grundsatz der Direkterhebung in § 4 Abs. 2 BDSG grundsätzlich problematisch. Da die Angaben des Versicherungsnehmers jedoch anders nicht zuverlässig zu verifizieren waren, war die Nachbarschaftsbefragung hier zur Erfüllung des Geschäftszweckes gemäß § 4 Abs. 2 Nr. 2a BDSG an sich zulässig. Dabei wurden dem Nachbarn aber Daten über die abgeschlossene Versicherung und die vom Versicherungsnehmer angegebene Schadenshöhe offenbart. Diese Übermittlung war nicht erforderlich. Aus Sicht der Aufsichtsbehörde lassen sich derartige Befragungen auch anders gestalten und könnten sogar zu einem objektiveren Ergebnis führen, zumal auch davon auszugehen ist, dass ein Nachbar den Schaden an einem Baum oder an einer Garage sicher nicht fachlich beziffern kann. Es reicht vollkommen aus, wenn Nachbarn z.B. befragt werden, wie der Garten vor dem Schadensfall ausgesehen hat bzw. ob vor dem angegebenen Schadensfall eine Garage fertiggestellt war oder nicht.

Die Außendienstmitarbeiter der Versicherung erscheinen vor Ort nicht mehr wie vor 20 Jahren mit Block und Bleistift, sondern der Laptop gehört zur Grundausstattung eines Außendienstmitarbeiters. Auf Grund der Vielzahl der zu bearbeitenden Fälle holt sich der Außendienstmitarbeiter vor Ort dann die benötigten Daten aus seinem Laptop. In derartigen Fällen ist es nun nicht erforderlich, dass die befragten Personen sich die Datensätze auf dem Gerät anschauen können, sondern der Außendienstmitarbeiter ist dahingehend zu schulen, dass er sich entweder die Daten alleine anschaut bzw. dass er nur die Daten aus dem Laptop zur Verfügung hat, die auch zur Aufgabenerfüllung unerlässlich sind. In diesem Zusammenhang war auch nochmals darauf hinzuweisen, dass eine Schulung bzw. Sensibilisierung solcher Mitarbeitergruppen ein ständiges Thema im Unternehmen sein sollte.

14. Arbeitnehmerdatenschutz

14.1 Unzureichender Schutz von Arbeitnehmerdaten im Zusammenhang mit einer Betriebsratswahl

"Name, Adresse, Gehalt - Daten aller Mitarbeiter verkauft", mit dieser Überschrift berichtete eine überregionale Zeitung über einen unglaublichen Vorfall.

Ein ehemaliger Mitarbeiter eines Unternehmens aus dem Rhein-Main-Gebiet stand im Verdacht, seine Funktion als Wahlhelfer für die Betriebsratswahl missbraucht und Personaldaten über alle 10.000 Mitarbeiter an eine Versicherung bzw. einen derer Mitarbeiter veräußert zu haben.

Das betroffene Unternehmen hatte bereits einige Zeit vor dieser Zeitungsmeldung entsprechende Hinweise erhalten. Auf Veranlassung und in Abstimmung mit der betrieblichen Datenschutzbeauftragten wurde die gesamte Angelegenheit von der Revision untersucht.
Der beschuldigte Mitarbeiter bestritt sämtliche Vorwürfe. Aufgrund anderweitiger beruflicher Beschäftigung hatte er sich zuvor schon auf eigenen Wunsch beurlauben lassen und kündigte dann von sich aus das Arbeitsverhältnis fristlos.
Das Unternehmen erstattete schließlich Strafanzeige gegen den ehemaligen Mitarbeiter. Vor seiner Tätigkeit als Wahlhelfer war er noch von der be-

trieblichen Datenschutzbeauftragten auf das Datengeheimnis verpflichtet worden.

Die Versicherung beteuerte gegenüber der für sie zuständigen Aufsichtsbehörde eines anderen Bundeslandes, dass keine Hinweise auf die fraglichen Mitarbeiterlisten oder deren Nutzung im Telefonmarketing gefunden worden seien.

Es bleibt somit der Ausgang des strafrechtlichen Verfahrens gegen den Beschuldigten abzuwarten.

Dessen ungeachtet offenbarte der Fall aber jedenfalls mangelnde datenschutzrechtliche Sensibilität in der Personalverwaltung des hessischen Unternehmens und wohl auch im Wahlvorstand. Nach den Angaben des Unternehmens gegenüber der Aufsichtsbehörde wurde dem ehemaligen Mitarbeiter zur Erstellung der Wählerliste offiziell eine Mitarbeiterliste zur Verfügung gestellt, welche Personalnummer, Name, betriebliche und private Adresse sowie teilweise Angaben zur Funktion der Beschäftigten enthielten. Der Mitarbeiter war vom Wahlvorstand beauftragt worden, die Datenlisten in der Personalabteilung abzuholen und für seine Tätigkeit zu verwenden.

Die Weitergabe der privaten Adressen der Mitarbeiter an den Wahlvorstand oder einen diesem zugeteilten Wahlhelfer ist zur Durchführung der Betriebsratswahl jedoch grundsätzlich nicht erforderlich und damit unzulässig (siehe bereits 11. Tätigkeitsbericht vom 16. September 1998, LT-Drucks. 14/4159, Nr. 8.2). Die Mitteilung der "Funktion" der Mitarbeiter ist nur insoweit gerechtfertigt, als diese für die Zuordnung der leitenden Angestellten nach § 18a Betriebsverfassungsgesetz erforderlich ist.
Zumindest bzgl. der Privatadressen war zu beanstanden, dass der Zugriff Unbefugter nicht unterbunden wurde.

Außerdem räumte das Unternehmen ein, dass sich in dem Wahllokal unzureichend gesicherte Einbauschränke mit Listen der Personalabteilung befanden, da der Raum zuvor als Lagerraum benutzt und nicht vollständig geräumt worden war. Es besteht die Vermutung, dass der ehemalige Mitarbeiter hieraus Gehaltslisten entwendete.

Auf Nachfrage und Kritik der Aufsichtsbehörde versicherte das Unternehmen schließlich, dass aufgrund der Vorkommnisse die erforderlichen innerbetrieblichen Maßnahmen getroffen wurden, um in Zukunft den Schutz der Mitarbeiterdaten auch bei Betriebsratswahlen zu gewährleisten.
Die Weitergabe der privaten Adressen an den Wahlvorstand erfolgt künftig nur, wenn die Mitarbeiter die Zusendung von Briefwahlunterlagen wünschen.
Es wird lediglich der Status "Leitender Angestellter" mitgeteilt, weitere Angaben zur "Funktion" werden nicht weitergegeben.

Alle Mitarbeiterinnen und Mitarbeiter des Personalbereiches wurden schriftlich auf die gesetzlichen Bestimmungen hingewiesen, die Konsequenzen bei Zuwiderhandlungen wurden aufgezeigt. Die für die Räumlichkeiten verantwortliche Führungskraft wurde schriftlich auf ihre Pflichten hingewiesen. Für die Handhabung der Wählerlisten wurde eine genaue Verfahrensanweisung und Dokumentation erarbeitet, welche nach abschließender Abstimmung in das Qualitätssicherheitssystem übernommen werden soll.

14.2 Mitarbeiterdaten im Strudel der Insolvenz

Im Rahmen der Insolvenz eines großen Unternehmens und der als Folge der Insolvenz notwendigen Personalabbaumaßnahmen schloss der Insolvenzverwalter einen Dienstleistungsvertrag mit einer Personalentwicklungs- und Arbeitsmarktagentur. Gegenstand des Vertrages war die Übernahme der Mitarbeiter des in Insolvenz befindlichen Unternehmens in ein befristetes Arbeitsverhältnis, die Qualifizierung der Mitarbeiter sowie die Durchführung von Vermittlungsaktivitäten. Dabei sollte so genanntes "Strukturkurzarbeitergeld" gemäß § 175 SGB III in Anspruch genommen und seitens des insolventen Unternehmens eine Aufstockung auf das Strukturkurzarbeitergeld gezahlt werden.

Die betroffenen Mitarbeiter wurden daher vom Insolvenzverwalter angeschrieben und erhielten das Angebot, den Vertrag mit der Personalentwick-

lungsgesellschaft zu unterschreiben und zugleich die ordentliche betriebsbedingte Kündigung des alten Arbeitsverhältnisses zu akzeptieren. Erst nach dem Abschluss des neuen Vertrages sollten die Personaldaten übermittelt werden.
Ein Mitarbeiter, welcher den neuen Arbeitsvertrag nicht unterschrieben hatte, war sehr erstaunt und verärgert, als er gleichwohl von dem Personalentwicklungsunternehmen in einem Schreiben als neuer Mitarbeiter begrüßt und zu einem ersten Gespräch geladen wurde.

Die Überprüfung durch die Aufsichtsbehörde ergab, dass eine Liste mit sämtlichen vom Personalabbau betroffenen Mitarbeitern, also einschließlich derjenigen, welche das Übernahmeangebot abgelehnt oder nach den Regelungen des Sozialplans nicht anspruchsberechtigt waren, übermittelt wurde.
Der Insolvenzverwalter bezeichnete dies als ein bedauerliches Versehen.
Er verwies jedoch darauf, dass er in die tatsächliche Abwicklung nicht involviert gewesen sei. Der Personalleiter teilte mit, dass das damals zuständige Vorstandsmitglied von der gesamten Maßnahme nicht informiert worden sei.

Insgesamt zeigte der Fall, wie wichtig es ist, dass der betriebliche Datenschutzbeauftragte bis zuletzt, gerade auch in der Insolvenzphase, auf die Einhaltung des Datenschutzes hinwirkt.
Dessen Arbeitsverhältnis war jedoch bereits aufgelöst worden.

14.3 Totalüberwachung am Arbeitsplatz?

Mitarbeiter eines weltweit operierenden Dienstleistungsunternehmens mit Niederlassung in Frankfurt am Main wandten sich an die Aufsichtsbehörde, weil sie sich umfangreichen Überwachungsmaßnahmen durch ihren Arbeitgeber ausgesetzt sahen.
In einem anonymen Schreiben legten sie dar, dass mindestens zehn Überwachungskameras installiert worden seien. Diese seien nach Auskunft eines Operators voll steuerungsfähig (360° schwenkbar, zoomfähige Optik). Die Anbringung sei keinem Mitarbeiter mitgeteilt worden. Die Kameras seien kaum als solche zu erkennen. Auf Grund der blickdichten Abschirmung mittels eines Spezialgehäuses sei auch nicht erkennbar, was oder wen die Kameras gerade beobachten.

Außerdem würden telefonische Abhörmaßnahmen durchgeführt. Ferner sei die Einführung eines Gerätes, das vornehmlich zur Kommunikation via Internet-Telephonie dienen solle, ebenfalls mit Überwachungsmaßnahmen verbunden. Eine integrierte Leseeinheit diene zur biometrischen Merkmalserfassung von Fingerprints. Beim Log-In-Prozess werde das Passwort samt Fingerabdruck an einen Security-Server in den USA übermittelt.

Die Mitarbeiter hegten auch den Verdacht, dass eine Mitarbeiterliste ("Watchlist") mit den Namen unliebsamer Mitarbeiter, die in irgendeiner Weise kritisch aufgefallen seien, beispielsweise durch die bekannt gemachte Absicht, einen Betriebsrat zu gründen, geführt werde. Die Geschäftsführung und Personalleitung würden das Passwort solcher Mitarbeiter durch eine spezielle Funktion umgehen und könnten so simultan alle E-Mails der Mitarbeiter "mitlesen".

Zuletzt beklagten die Mitarbeiter, dass die Geschäftsführung sich beharrlich weigere, einen betrieblichen Datenschutzbeauftragten zu bestellen.

Bereits die Ankündigung der Prüfung ohne Angabe des Prüfgegenstandes durch die Aufsichtsbehörde zeigte gewisse Wirkung, denn zu Beginn der Prüfung wurde ein Mitarbeiter vorgestellt, der zum betrieblichen Datenschutzbeauftragten bestellt werden sollte und bereits über Grundkenntnisse zum Datenschutz verfügte.

Es war tatsächlich eine verdeckte Videoüberwachungsanlage installiert worden, deren Steuerung von der Europazentrale des Unternehmens in London aus durchgeführt wird. Die Geschäftsführung gab an, dass die Anlage nur außerhalb der Arbeitszeiten, von 21:30 bis 06:00 Uhr, angeschaltet sei. Sie diene ausschließlich dem Schutz vor Einbrüchen und Diebstählen, da in dem von mehreren Unternehmen genutzten Gebäude in der Vergangenheit schon mehrfach derartige Delikte vorgekommen seien. Diese Angaben erschienen insgesamt plausibel, letztlich wird jedoch nur eine Überprüfung in London

Klarheit über Umfang und Zweck der Videoüberwachung bringen. Der zukünftige betriebliche Datenschutzbeauftragte hatte sich dies bereits als erste Aufgabe vorgenommen.
Die Aufsichtsbehörde forderte außerdem, dass die Mitarbeiter umfassend informiert werden, zumal nicht auszuschließen ist, dass sich Mitarbeiter auch nach der offiziellen Arbeitszeit in den Büros aufhalten.

Anhaltspunkte für eine Telefonabhörung wurden nicht gefunden.
Zur Identifizierung und zum Nachweis der Berechtigung für die Nutzung des neuen internen Telefonsystems, dass über das eigene Standleitungsnetz abgewickelt wird, müssen die Mitarbeiter zunächst ein Passwort eingeben und danach ihren Fingerabdruck vom Gerät überprüfen lassen. Es wird aber nicht der gesamte Finger oder Daumen gescannt und verglichen, sondern lediglich ein Teilausschnitt.
Hierzu wird zunächst zu dem jeweiligen Passwort der entsprechende Ausschnitt des Fingerabdrucks in London gespeichert. Wenngleich eine dezentrale Speicherung von Biometriedaten, möglichst beim Betroffenen grundsätzlich vorzuziehen ist, wurde eine derartige Form der Identifizierung und des Berechtigungsnachweises akzeptiert, zumal eine Alternative angeboten wurde. Mitarbeitern, die diese Form der Identifizierung ablehnen, ist die Möglichkeit eingeräumt worden, mit einem Zusatzgerät, das wiederum über einen Geheimcode zugänglich ist, den Fingerprint zu ersetzen.

Die befürchtete "Watchlist" wurde trotz intensiver Prüfung der Personaldatenverarbeitung nicht gefunden.

Ebenso wenig ergaben sich Anhaltspunkte, dass eine Umgehung des gesamten Passwortsystems für die Geschäftsführung möglich sei. Hier bleibt aber - wie bei der Videoüberwachung - abzuwarten, in welcher Form der zukünftige Datenschutzbeauftragte die Berechtigungsvergabe darstellen wird.

Bemängelt werden musste das Fehlen von Verfahrensverzeichnissen. Aufzuarbeiten wird auch sein, inwieweit die US-Muttergesellschaft Zugriff auf die Personaldatenverarbeitung hat.

Insgesamt haben sich die Befürchtungen der Mitarbeiter somit zwar im wesentlichen als unbegründet erwiesen. Das Unternehmen hätte jedoch bei der Einführung neuer Techniken für Transparenz sorgen müssen und damit Vertrauen schaffen können. Es bleibt auch viel Arbeit für den Datenschutzbeauftragten. Die Aufsichtsbehörde wird weiter verfolgen, ob dieser seiner Aufgabe gerecht und der Datenschutz in dem Unternehmen ausreichend beachtet wird.

15. Medizinischer Bereich: Was geschieht mit den Patientenunterlagen, wenn Ärzte verschwinden?

Ein Zahnarzt hatte sich wegen Überschuldung ins Ausland abgesetzt, Aufenthaltsort unbekannt. Die gesamte Einrichtung nebst Patientenunterlagen (Röntgenbilder, Abrechnungsunterlagen, Gebissabdrücke etc.) verblieben in der Praxis. An den Vermieter der Praxis zahlte er bereits seit Monaten keine Miete mehr.

Der Vermieter wollte die Räume wieder vermieten und verwahrte die Unterlagen sowie das EDV-System zunächst in seinem Keller. Er war sich der Sensibilität der Daten bewusst und schrieb in seiner Not das Sozialministerium und andere Einrichtungen an und teilte mit, dass er beabsichtige, die Patientenunterlagen als Altpapier oder Hausmüll zu entsorgen, wenn keine Stelle bereit sei, die Unterlagen zu übernehmen.

Das Sozialministerium informierte ihn darüber, dass die Landesärztekammer Hessen sich bereiterklärt habe, in problematischen Fällen die Patienten- und Arztunterlagen bis zur endgültigen Klärung der Sachlage aufzubewahren.
Auf telefonische Anfrage teilte die Kammer jedoch mit, dass sie nicht zuständig sei, da ihr der Zahnarzt nicht mehr angehöre.

Eine betroffene Patientin wandte sich an die Datenschutzaufsichtsbehörde, die sich daraufhin mit Hausmeister und Vermieter in Verbindung setzte, sich von der sicheren Aufbewahrung der Unterlagen überzeugte und dann recherchierte, welche Mitarbeiter der verlassenen Praxis möglicherweise in anderen Praxen tätig sind. Schließlich wurden zwei ehemalige Mitarbeiterinnen

gefunden, die mittlerweile in einer anderen Praxis tätig waren, und sich nach einem längeren Gespräch dazu bereit erklärten, die Verwaltung der Unterlagen zu übernehmen.
Patienten, die verzweifelt nach ihren Röntgenunterlagen fragten, konnte so geholfen werden, indem die Aufsichtsbehörde an diese ehemaligen Mitarbeiterinnen verwies, welche die Unterlagen heraussuchten und aushändigten.

Endgültig gelöst wurde das Problem dadurch, dass sich ein Zahnarzt fand, der als Praxisnachfolger die Räume mietete und - auf Vermittlung der Aufsichtsbehörde - bereit war, eine Praxisangestellte des früheren Arztes zu übernehmen. Diese verwahrte die Schlüssel zu den Schränken mit den alten Unterlagen. Wenn ein Patient des verschwundenen Arztes die Praxis aufsucht, übergibt sie dem Nachfolger die Unterlagen oder händigt sie auf Wunsch dem Patienten aus. Auf diese Weise kann die ärztliche Schweigepflicht, die auch gegenüber dem Praxisnachfolger gilt, gewahrt und gleichzeitig die ärztliche Dokumentationspflicht erfüllt werden.

In einem anderen Fall entsorgte ein vor seinen Gläubigern fliehender Arzt seine Unterlagen im Papiercontainer einer Polizeiwache in Wiesbaden. Die Polizeibeamten stellten die Unterlagen sicher und baten dann die Aufsichtsbehörde, sich um die Angelegenheit zu kümmern. Die Zahnärztekammer lehnte es auf telefonische Nachfrage der Aufsichtsbehörde ab, sich der Sache anzunehmen.
Da der Aufenthaltsort des Arztes unbekannt war, stellte die Aufsichtsbehörde selbst weitgehende Recherchen an. Das Ergebnis: Ein Rechtsanwalt wurde als Vermittler zwischen Arzt und Aufsichtsbehörde eingeschaltet. Der Rechtsanwalt verbürgte sich zunächst für die fachgerechte Entsorgung der Unterlagen, diese wurden von der Polizeiwache abgeholt, der Rechtsanwalt bestätigte abschließend nochmals die fachgerechte Entsorgung der Unterlagen. In diesem Fall gelang es nicht, die ärztliche Dokumentationspflicht sicherzustellen.

Über das Grundsatzproblem wurde bereits im 13. Tätigkeitsbericht vom 30. August 2000 (LT-Drucks. 15/1539 Nr. 12.1) berichtet.

Zwischenzeitlich hat sich auch die Arbeitsgemeinschaft der Obersten Landesgesundheitsbehörden mit der Thematik befasst. Die Mehrheit der Länder hat jedoch wegen der bisher geringen Zahl von Praxisaufgaben ohne Praxisnachfolger keine Probleme gesehen. Die Mehrzahl der Länder wies überdies darauf hin, dass die jeweiligen Berufsordnungen hinreichende Regelungen zur Aufbewahrung von Unterlagen in solchen Fällen vorsähen. Im Hessischen Heilberufegesetz und in der Hessischen Berufsordnung für Ärzte ist die Frage, wie zu verfahren ist, wenn ein Arzt seiner Dokumentationspflicht nicht nachkommt, nicht ausdrücklich geregelt.
Mögen in Hessen bisher nur relativ wenige Fälle aufgetreten oder bekannt geworden sein, waren die Erfahrungen in den oben geschilderten Fällen doch sehr unbefriedigend.

16. Werbung, Reklame und Direktmarketing

16.1 Leitfaden des Deutschen Direktmarketingverbandes (DDV)

Wenngleich der DDV nicht um eine formelle Bewertung nach § 38a BDSG gebeten hatte (s. oben unter Nr. 4), gab er doch zu erkennen, dass er an einem Meinungsaustausch mit den Aufsichtsbehörden interessiert sei.

Der im Jahr 2001 erstellte Leitfaden zu den Auswirkungen der BDSG-Novelle auf das Direktmarketing sollte als Diskussionsbeitrag des DDV verstanden werden.

Da der DDV seinen Sitz in Wiesbaden hat, erarbeitete das Regierungspräsidium Darmstadt eine umfangreiche Stellungnahme. Diese wurde mit den obersten Aufsichtsbehörden im Bundesgebiet abgestimmt, weil die Fragestellungen für alle Unternehmen relevant sind, welche personenbezogene Daten für Werbezwecke verarbeiten oder nutzen, und weil der DDV selbst nicht datenverarbeitende und verantwortliche Stelle i. S. d. BDSG ist.

Insgesamt hielten die Aufsichtsbehörden eine Reihe von Änderungen für erforderlich.

Die vorgetragene Kritik wurde vom DDV zum Teil berücksichtigt und floss in die Erstellung einer zweiten überarbeiteten Auflage des Leitfadens "Best Practice Guide Nr. 3" vom September 2002 ein. Erfreulicherweise stellte der DDV auch diese Auflage wieder als offenen Diskussionsbeitrag bereit.
Leider war der DDV zunächst nicht ohne weiteres zu einem "Nachverhandeln" mit den Aufsichtsbehörden bzgl. der verbliebenen Kontroversen bereit.
Kurz vor Redaktionsschluss dieses Tätigkeitsberichts fand jedoch beim Regierungspräsidium Darmstadt ein sehr konstruktives Gespräch mit dem DDV statt. Es bleibt zu wünschen, dass der Leitfaden weiter überarbeitet wird, so dass die Aufsichtsbehörden ratsuchende Unternehmen uneingeschränkt auf die praktischen Erläuterungen im Leitfaden des DDV verweisen können.

16.2 Negative Prüferfahrungen im Bereich der Werbung

Auch diesmal hatte die Aufsichtsbehörde im Berichtszeitraum wieder zahlreiche Beschwerden von Betroffenen zu verzeichnen, die persönlich adressierte Werbung erhielten, jedoch bei der Anfrage zur Herkunft ihrer Daten oder beim Widerspruch gegen weitere Werbung beim Werbetreibenden kein Gehör fanden.

Die Aufsichtsbehörde hat diese Beschwerden aufgegriffen und das Auskunftsrecht des Betroffenen (§ 34 Abs. 1 BDSG) durchgesetzt.
In nahezu allen Fällen, in denen wegen der Nichtbeauskunftung ermittelt wurde, war auch zu rügen, dass der Hinweis auf das Widerspruchsrecht (§28 Abs. 4 S.2 BDSG) in den Werbeschreiben nicht enthalten war.

Auch in den Fällen, in denen die Aufsichtsbehörde ohne Beschwerde von außen selbst initiativ wurde und stichprobenartig Werbematerial bezüglich des Hinweises auf das Widerspruchsrecht prüfte, waren die Ergebnisse nicht besser. In der überwiegenden Mehrzahl der Fälle fehlte der Hinweis. Obwohl dieser Widerspruchshinweis bereits seit der Novellierung des BDSG im Mai 2001 gesetzlich vorgeschrieben ist, war leider festzustellen, dass sich noch immer nur wenige Werbetreibende daran halten, so dass sich die Aufsichtsbehörde gezwungen sah, Bußgelder zu verhängen (siehe hierzu auch unter Nr. 7).

Eine besondere Häufung von Beschwerden zog die Werbeaktion eines Finanzdienstleisters nach sich. In einem persönlich adressierten Werbeschreiben bot er den potentiellen Kundinnen und Kunden einen Kredit an, der auf die finanziellen Verhältnisse der oder des einzelnen zugeschnitten schien bzw. jedenfalls in einzelnen Fällen diesen Eindruck erweckte. Bei einigen Adressaten kam der Verdacht auf, hier seien personenbezogene Finanzdaten an das Geldinstitut weitergegeben worden.
Dieser Verdacht erwies sich jedoch nach Prüfung durch die Aufsichtsbehörde als unbegründet. Das Unternehmen hatte aber auf das Ersuchen der Betroffenen um Auskunft über die gespeicherten Daten unzureichend bzw. derart ungeschickt geantwortet, dass es ihm nicht gelungen war, selbst den Verdacht bei den Betroffenen auszuräumen.
Zu beanstanden war auch, dass im Werbeschreiben der Hinweis auf das Widerspruchsrecht fehlte.

16.3 Große Haushaltsbefragungen

Aus der Werbebranche sind jedoch auch positive Entwicklungen zu berichten.

In den Jahren 1997 und 1998 hatte die bundesweite Versendung von Fragebögen durch ein im Rhein-Main-Gebiet ansässiges Unternehmen, ebenso wie ähnliche Aktionen eines baden-württembergischen Unternehmens, für großes Aufsehen und eine Vielzahl von Eingaben bei den Datenschutzaufsichtsbehörden gesorgt.

Das Unternehmen wollte die Konsum- und Freizeitgewohnheiten der Bürger erfragen und die eingehenden Antworten u.a. anderen Unternehmen zur Verfügung stellen, damit diese zielgerichtete Werbung an die angegebenen Adressen versenden können.

Auf Grund starker bundesweiter Kritik aller Aufsichtsbehörden holte das Unternehmen bei den nächsten Befragungen die schriftliche Einwilligung der

Betroffenen mit Unterschrift ein und verbesserte die Aufklärung, so dass Verwechslungen mit der herkömmlichen Markt- und Meinungsforschung, bei der die Antworten ausschließlich anonymisiert bzw. statistisch verwendet werden, ausgeschlossen sind (s. Tätigkeitsberichte der Hessischen Landesregierung vom 16. September 1998, LT-Drucks. 14/4159, Nr. 7.1 und vom 27. August 1999, LT-Drucks. 15/357, Nr. 13.1).

Obwohl der Verbraucherschutzverein Berlin, der wegen der datenschutzrechtlichen Mängel der ersten Befragung gegen das Unternehmen geklagt hatte, im Rechtsstreit unterlag, hielt sich das Unternehmen weiterhin an die Forderungen der Aufsichtsbehörden.

Seither finden vor allem auf Wunsch des Unternehmens jährliche Statusgespräche beim Regierungspräsidium Darmstadt statt. Hierbei wurde in den Jahren 2001 und 2002 intensiv erörtert, welche Konsequenzen sich aus der BDSG-Novelle ergeben. Bei den jüngsten Befragungen hat das Unternehmen nun die erforderlichen Änderungen vorgenommen.

Es wurde § 4 Abs. 3 Satz 1 Nr. 3 BDSG Rechnung getragen, indem die Angaben über die potentiellen Empfänger bzw. die Kategorien von Empfängern präzisiert wurden. Da prinzipiell alle Unternehmen als Empfänger in Betracht kommen, welche entweder die Fragen selbst im Fragebogen platziert haben oder deren Waren- oder Dienstleistungsangebot zu dem sich aus dem Fragebogen ableitbaren Interessensprofil der Betroffenen passt, wurde dabei folgende offene, beispielhafte Beschreibung in der Einwilligungserklärung gewählt, um den Betroffenen die Bandbreite der potentiellen Empfänger bewusst zu machen:
"Die personenbezogene Weitergabe wird ausschließlich auf die Organisationen und Unternehmen aus den verschiedensten Branchen - z.B. Markenanbieter, Verlage, Autohersteller, Handel und Dienstleistungsunternehmen - beschränkt, die meinen erkennbaren Interessen und Wünschen entgegenkommen können. Diese Organisationen und Unternehmen dürfen mir Informationen, Angebote, Werbung und kostenlose Produktmuster … übermitteln."

Da der Begriff des "Empfängers" i.S.d. § 4 Satz 1 Abs. 3 Nr. 3 BDSG nicht nur Dritte umfasst, sondern auch Auftragsdatenverarbeiter, trotz der Verwendung des Begriffes "Übermittlung" im einschränkenden zweiten Halbsatz, werden Betroffene nun darüber informiert, dass die Daten auch "von externen Datenverarbeitern wie z.B. Datenerfassern und Internetdienste-Anbietern" - letzteres ist nur für die Online-Befragungen relevant - verarbeitet werden.

Bereits die direkt adressierte Versendung des Fragebogens ist eine "Ansprache zum Zweck der Werbung" i.S.d. § 28 Abs. 4 Satz 2 BDSG. Daher muss der Betroffene die Möglichkeit haben, der Verwendung seiner Daten für diese Zwecke zu widersprechen, und muss hierüber unterrichtet werden. Dies ist zu unterscheiden von der Einholung der Einwilligung in die Verwendung der Daten, die der Betroffene beim Ausfüllen des Fragebogens preisgibt. Für die direkt adressierte Versendung des Fragebogens verwendet das Unternehmen z.T. auch Fremdadressen von anderen Adresshändlern oder Listbrokern.

In den neuesten Fragebögen ist daher die Information enthalten:
"Sollten Sie kein Interesse am Erhalt eines Fragebogens haben, genügt ein formloses Schreiben an die unten angegebene Adresse von ….". Diese Unterrichtung ist mit der Information über die jederzeitige Widerruflichkeit der Einwilligung verknüpft.

In den jüngsten Befragungen sind auch Fragen enthalten, die mit der Gesundheit in Zusammenhang stehen ("Kaufen Sie Kontaktlinsenpflegemittel?"), also mit besonderen Arten personenbezogener Daten i.S.d. § 3 Abs. 9 BDSG. Die besonderen Anforderungen des § 4a Abs. 3 BDSG wurden berücksichtigt, indem diese Fragen besonders gekennzeichnet wurden und in der Einwilligungserklärung nochmals gesondert mit "Ja" oder "Nein" anzugeben ist, ob sich die Einwilligung auch auf diese Fragen beziehen soll.

Das Unternehmen hat bei der Überarbeitung der Datenschutzhinweise am Anfang des Fragebogens auch eine weitere Ergänzung vorgenommen.

Dies betrifft die Fälle, in denen Betroffene zwar den Fragebogen ausfüllen, aber dann ohne Unterschrift und damit ohne schriftliche Einwilligung zurücksenden. Die Daten werden dann nicht personenbezogen übermittelt und der Name wird von vornherein nicht erfasst und gespeichert, aber Postleitzahl, Ort, Straße und Hausnummer werden gespeichert - getrennt von den sonstigen Angaben -, um die Daten für anonyme Auswertungen, beispielsweise Bedarfssituation für ein neues Autohaus in einem Stadtteil, verwenden und den entsprechenden Gebietszuschnitt ggf. verändern zu können.

Da bei den Daten der Adressen nach Auffassung der Aufsichtsbehörde eine gewisse Personenbeziehbarkeit vorhanden ist, wurde nun folgende Information aufgenommen: "Fehlt die Einwilligung, wird die Adresse getrennt von Ihren Angaben gespeichert und vor unberechtigtem Zugriff geschützt. Sie wird dann ausschließlich im Rahmen statistischer Marktforschung genutzt."

Beschwerden gegen die Haushaltsbefragungen gehen bei der Aufsichtsbehörde kaum noch ein.
Die datenschutzfreundliche Gestaltung dürfte dazu beigetragen haben, dass das Unternehmen das Vertrauen der Verbraucher gewinnen konnte. Der Dialog mit dem Unternehmen wird gleichwohl fortgeführt. Themen gibt es nach wie vor.

Wiesbaden, 9. Dezember 2003

Der Hessische Ministerpräsident: **Koch**

Der Hessische Minister des Innern und für Sport: **Bouffier**