15. Wahlperiode

Drucksache **15/4659**

# HESSISCHER LANDTAG

26. 11. 2002

## Vorlage
## der Landesregierung

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

Vorgelegt mit der Stellungnahme zum Dreißigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten - Drucks. 15/3705 - nach § 30 Abs. 2 des Hessischen Datenschutzgesetzes in der Fassung vom 7. Januar 1999.

Eingegangen am 26. November 2002 · Ausgegeben am 17. Dezember 2002

Druck: Druck- und Verlagshaus Chmielorz GmbH · 65205 Wiesbaden · Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

**Zusammenfassung**

**1. Neue Gesetze - neue Aufgaben**

Die Regierungspräsidien sind zuständige Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich. Deren Aufgaben und Befugnisse wurden durch die am 23. Mai 2001 in Kraft getretene Novelle des Bundesdatenschutzgesetzes erweitert.

Nach § 38 Abs. 1 Satz 1 BDSG kontrollieren die Aufsichtsbehörden die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln, einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5 BDSG.

Diese Neuregelung bedeutet, dass den Aufsichtsbehörden nun eine generelle anlassunabhängige Kontrolle obliegt. Eine solche Dauer- bzw. Initiativkontrolle mit anlassunabhängigen Überprüfungen war vom Gesetzgeber bislang nur für bestimmte Bereiche vorgesehen (Auskunfteien, Adresshandelsunternehmen, Markt- und Meinungsforschungsinstitute, Servicerechenzentren und sonstige Auftragsdatenverarbeiter (§ 38 Abs. 2 BDSG a.F.) sowie für Tele- und Mediendiensteanbieter gemäß Teledienstedatenschutzgesetz und Mediendienstestaatsvertrag). In allen anderen Bereichen oblag den Behörden nur eine Anlassaufsicht, sodass sie Prüfungen nur vornehmen konnten, wenn Beschwerden oder sonstige konkrete Anhaltspunkte auf Datenschutzverstöße vorlagen (§ 38 Abs. 1 BDSG a.F.).

Auch künftig werden die Aufsichtsbehörden vorrangig in den Fällen tätig sein, in denen konkrete Anhaltspunkte auf Datenschutzverstöße vorliegen, denn hierbei kann sich das Ermessen auf Null reduzieren, währenddessen bezüglich der Initiativkontrolle ein weiterer Spielraum besteht.

Die Bezugnahme in § 38 Abs. 1 Satz 1 BDSG auf das Recht der Mitgliedstaaten bedeutet, dass die Aufsichtsbehörden nach Maßgabe des § 1 Abs. 5 BDSG gegebenenfalls das Recht anderer Mitgliedstaaten der Europäischen Union (EU) oder des Abkommens über den Europäischen Wirtschaftsraum (EWR) als Prüfmaßstab für die Beurteilung der Zulässigkeit einer Datenverarbeitung im Inland zugrunde zu legen haben. Dies wird nur in enger Abstimmung mit den Datenschutzaufsichtsbehörden der anderen Mitgliedstaaten zu bewältigen sein.

Die Aufsichtsbehörden haben außerdem die Aufgabe erhalten, auch bei materiellen Verstößen gegen datenschutzrechtliche Vorschriften Bußgeldbescheide zu erlassen (§ 43 Abs. 1 Nr. 3, 4, 6 und 7, Abs. 2 BDSG). Bisher konnten Bußgelder nur bei einigen formellen Verstößen verhängt werden.
Die Aufsichtsbehörden haben nun bei besonders schweren Verstößen ein Strafantragsrecht (§ 44 BDSG). Mit diesen erweiterten Sanktionsmöglichkeiten, die - wie die meisten Änderungen - aufgrund entsprechender Vorgaben der EG-Datenschutzrichtlinie (EG-DSRL) aufgenommen wurden, werden die Aufsichtsbehörden ihren Rechtsauffassungen und Forderungen mehr Nachdruck verleihen können.

Des Weiteren haben die Aufsichtsbehörden nunmehr nach § 4c Abs. 2 BDSG die Aufgabe, Datenübermittlungen in Staaten außerhalb der EU und des EWR (bei Vorliegen der Voraussetzungen des § 4c Abs. 2 BDSG) zu genehmigen, wenn in dem Drittstaat kein angemessenes Datenschutzniveau besteht und die gesetzlichen Ausnahmetatbestände des § 4c Abs. 1 BDSG nicht erfüllt sind. Jede Genehmigung muss dem Bund mitgeteilt werden, welcher dann die EU-Kommission und die anderen Mitgliedstaaten informiert. Diese können Widerspruch gegen die Genehmigung erheben. (Zu den vielfältigen Fragen im Zusammenhang mit der Auslandsdatenverarbeitung siehe Nr. 7.)

§ 38a BDSG weist den Aufsichtsbehörden die Aufgabe zu, Verhaltensregeln zum Datenschutz, die von Berufsverbänden und anderen Vereinigungen erstellt und den Aufsichtsbehörden vorgelegt werden, auf ihre Vereinbarkeit mit dem geltenden Datenschutzrecht zu überprüfen. Entsprechend der Intention der EG-DSRL soll damit die Erstellung von "Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen" angeregt wer-

den, weil diese der branchenspezifischen und kontextbezogenen Konkretisierung des Gesetzeswortlauts dienen und damit zur stärkeren Beachtung der gesetzlichen Anforderungen beitragen (siehe Nr. 15).

Auch die sonstigen Änderungen des BDSG wirken sich natürlich auf die Aufgaben der Aufsichtsbehörden aus, z.B. die Erweiterung des Geltungsbereiches des BDSG, die Regelungen für Videoüberwachungen, die erhöhten Anforderungen bei der Datenerhebung, die Verpflichtung der betrieblichen Datenschutzbeauftragten, sich in Zweifelsfällen im Zusammenhang mit der Vorabkontrolle an die Aufsichtsbehörde zu wenden.

Das Regierungspräsidium Darmstadt ist durch die oben genannten gesetzlichen Änderungen im Verhältnis zu anderen Aufsichtsbehörden faktisch besonders betroffen, da in der Wirtschaftsregion Rhein-Main viele große Unternehmen, Konzerne und Verbände ihren Sitz haben.

Ferner bewirkt die Neuorganisation der SCHUFA einen Aufgabenzuwachs beim Regierungspräsidium Darmstadt und beim Hessischen Ministerium des Innern und für Sport (siehe Nr. 10.1).

## 2. Das Melderegister

### 2.1 Das Register der meldepflichtigen Stellen nach § 32 BDSG a.F.

Die Aufsichtsbehörden führten seither nach § 38 Abs. 2 BDSG a.F. das Register der Stellen, die personenbezogene Daten geschäftsmäßig zum Zweck der personenbezogenen oder der anonymisierten Übermittlung speichern oder im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen. Diese Stellen unterlagen nach § 32 BDSG a.F. der Meldepflicht bei der Datenschutzaufsichtsbehörde.

Am 21. Mai 2001 waren 854 meldepflichtige Unternehmen im Register der Aufsichtsbehörden eingetragen. Der Melderegisterbestand blieb damit gegenüber dem Vorjahr nahezu unverändert.

Den größten Anteil hieran hatten mit 711 Registereinträgen die nach § 32 Abs. 1 Nr. 3 BDSG a.F. gemeldeten Unternehmen, die im Auftrag als Dienstleistungsunternehmen weisungsgebunden im Sinne des § 11 BDSG personenbezogene Daten verarbeiten oder nutzen. Hierbei handelt es sich z.B. um Konzern- und Dienstleistungsrechenzentren sowie um Datenerfassungsbetriebe, Schreibserviceunternehmen, Mikroverfilmer, Datenträgervernichter sowie Lettershops und ähnliche Unternehmen aus dem Bereich des Direktmarketings.

Mit 79 Meldungen hatten die nach § 32 Abs. 1 Nr. 2 BDSG a.F. meldepflichtigen Unternehmen der Markt- und Meinungsforschung, die personenbezogene Daten zum Zwecke der anonymisierten Übermittlung (§ 30 BDSG) speichern, den zweitgrößten Anteil am Melderegisterbestand.

Den geringsten Anteil hatten mit 64 Registereinträgen die nach § 32 Abs. 1 Nr. 1 BDSG a.F. gemeldeten Unternehmen, die, wie z.B. Adresshändler oder auch Wirtschaftsauskunfteien, personenbezogene Daten zum Zwecke der Übermittlung im Sinne des § 29 BDSG speichern.

### 2.2 Die Neuregelung der Meldepflicht nach § 4d BDSG

Das neue BDSG brachte einige grundlegende Veränderungen für das Melderegister der Aufsichtsbehörden mit sich. Nach der Neuregelung der Meldepflicht sind nun nach § 4d Abs. 1 BDSG die Verfahren automatisierter Verarbeitungen vor ihrer Inbetriebnahme von den verantwortlichen Stellen den Aufsichtsbehörden zu melden. Der Gesetzgeber hat dabei allerdings in § 4d Abs. 2 BDSG weitreichende Ausnahmen vorgesehen. Ausnahmslos meldepflichtig sind nach § 4d Abs. 4 BDSG lediglich automatisierte Verfahren, in denen von verantwortlichen Stellen personenbezogene Daten zum Zweck der Übermittlung oder der anonymisierten Übermittlung verarbeitet werden.
Alle anderen Verfahren von Stellen, die einen betrieblichen Datenschutzbeauftragten bestellt haben oder die Voraussetzungen des § 4d Abs. 3 BDSG erfüllen, sind von der Pflicht befreit, ihre Verarbeitungsverfahren bei den Aufsichtsbehörden zu melden.

Diese gesetzlichen Veränderungen dürften sich in der Praxis der Datenschutzaufsichtsbehörden wahrscheinlich so auswirken, dass letztlich fast nur noch die Verfahren des Adresshandels, der Auskunfteien, der SCHUFA und ähnlicher Unternehmen, die nach § 29 BDSG (Erhebung und Speicherung zum Zweck der Übermittlung) arbeiten, sowie der Unternehmen der Markt- und Meinungsforschung, die Verarbeitungsverfahren nach § 30 BDSG betreiben, im Register gemeldet sein werden.

Die bereits mit dem letztjährigen Tätigkeitsbericht vorgelegten Meldeformulare sowie Hilfen und Merkblätter zur Meldepflicht, die auf dem Workshop der Datenschutzaufsichtsbehörden der Länder in Darmstadt entstanden sind, wurden nochmals in intensiver Abstimmung mit den Datenschutzaufsichtsbehörden der Länder überarbeitet und sind inzwischen im Internet unter der WWW-Seite des Regierungspräsidiums Darmstadt abrufbar (www.rpda.de/dezernate/datenschutz).

Die EDV-Dienstleistungsunternehmen und Auftragsdatenverarbeiter, die mehr als 80 v.H. des Registerbestands ausmachten, wurden schriftlich darauf hingewiesen, dass die ehemals meldepflichtige Tätigkeit nach dem neuen BDSG nicht mehr bei der Aufsichtsbehörde gemeldet werden muss. Alle ca. 710 gemeldeten Auftrags- und Konzernrechenzentren, Datenbankverwalter, Call-Center, Datenerfassungsbetriebe und Buchungshelfer, Mikroverfilmungsunternehmen und Auftrags-Belegerfasser, Datenträgervernichter, Lettershops und Mailingbetriebe ohne eigenen Adressbestand wurden danach aus dem Register gelöscht.

Die "Befreiung" von der Meldepflicht wurde allerdings nicht überall positiv aufgenommen. Einige Datenschutzbeauftragte von ehemals meldepflichtigen Unternehmen aus dem Rhein-Main-Gebiet befürchteten, dass der Kontakt mit der Aufsichtsbehörde ohne die Meldepflicht nun an Intensität verlieren wird. Viele Unternehmen - insbesondere aus der Branche der Datenträger- und Aktenvernichtung - betrachteten die seitherige Meldung bei der Aufsichtsbehörde zudem nicht als Belastung, sondern als werbewirksames Gütesiegel. Es wurde sogar befürchtet, dass sich diese Gesetzesänderung geschäftsschädigend auswirken könne.
In einem Fall wurde die Aufsichtsbehörde von einem Unternehmen sogar intensiv bedrängt, die Datenverarbeitungsverfahren trotz der Gesetzesänderung in das Verfahrensverzeichnis aufzunehmen. Dieses Dienstleistungsunternehmen für die Bank- und Finanzbranche befürchtete, seine lukrativen Aufträge bei Frankfurter Großbanken zu verlieren, wenn es nicht mehr beim Regierungspräsidium Darmstadt gemeldet ist.

In den vielen Gesprächen mit den meldepflichtigen Stellen zeichneten sich auch bereits einige Probleme und Auslegungsfragen zu den zu meldenden Angaben ab.
Viele Unternehmen übersehen, dass jedes Verfahren einzeln je nach Verarbeitungszweck der Aufsichtsbehörde gemeldet werden muss bzw. separate Anhänge zum Meldeformular auszufüllen sind. Verantwortliche nicht öffentliche Stellen, die Daten zu verschiedenen meldepflichtigen Zwecken verarbeiten, müssen daher auch separate Angaben zu den jeweiligen Verarbeitungsverfahren machen.

Ein bedeutender Fortschritt für die Datenverarbeitungspraxis ist es in den Augen der Aufsichtsbehörden, dass die Unternehmen bei der Verfahrensmeldung nach § 4e Nr. 9 BDSG der Dienststelle nun auch Angaben zu den getroffenen Sicherheitsmaßnahmen im Sinne des § 9 BDSG und Anlage hierzu machen müssen, da die Unternehmen und die betrieblichen Datenschutzbeauftragten somit gezwungen sind, die Geeignetheit und Angemessenheit ihrer Sicherheitseinrichtungen anlässlich der Meldung an die Datenschutzaufsichtsbehörden nochmals zu überprüfen. Da diese Angaben nach § 38 Abs. 2 Satz 3 BDSG nur für die Aufsichtsbehörden bestimmt sind, werden relativ detaillierte Angaben von den Unternehmen verlangt. Bei allen anderen Angaben, die nach § 38 Abs. 2 Satz 2 BDSG von jedermann eingesehen werden können, müssen auch die Interessen der Unternehmen an der Geheimhaltung interner Geschäftsinformationen berücksichtigt werden. Daher ist nach § 4e Nr. 5 und Nr. 6 BDSG die genaue Nennung der Daten bzw. der konkreten Datenempfänger nicht zwingend erforderlich. Vielmehr reicht es, wenn alternativ die entsprechenden Kategorien angegeben werden. Die Aufsichtsbehörden verlangen hier keine detaillierten Angaben, zumal der Verwaltungsaufwand für den Registeränderungsdienst bei hoher Detaildichte der

Meldeangaben für alle Beteiligten unerträglich hoch und kaum zu rechtfertigen wäre.

Für einige Verwirrung und regelmäßige Nachfragen sorgt auch die Tatsache, dass bei den zu meldenden Angaben nach § 4e BDSG der Name des betrieblichen Datenschutzbeauftragten nicht enthalten ist und diese Angabe daher auf dem Meldeformular als "freiwillige Angabe" gekennzeichnet ist, obwohl diese Funktion eine herausragende Bedeutung für den Datenschutz in den Betrieben hat und von den Datenschutzaufsichtsbehörden jederzeit nachgefragt werden kann. Die Aufsichtsbehörden erläutern stets, dass die Angabe im öffentlichen Register sinnvoll, aber nicht zwingend ist. Unberührt bleibt die Verpflichtung der Unternehmen, den Aufsichtsbehörden gegenüber auf konkrete Nachfrage im Rahmen deren Prüftätigkeit Auskunft zu erteilen.

Am 1. Januar 2002 waren 133 automatisierte Verfahren zum Register der Datenschutzaufsichtsbehörden gemeldet, wobei noch nicht alle Registereintragungen vollständig inhaltlich aktualisiert waren. Davon dienten 62 automatisierte Verarbeitungsverfahren dem Zweck der Übermittlung, 71 Verfahren dienten dem Zweck der Übermittlung in anonymisierter Form.

### 3. Bearbeitung von Datenschutzbeschwerden und sonstige Prüfungen aus konkretem Anlass

Im Berichtsjahr wurden die Aufsichtsbehörden in 358 Fällen aufgrund von Beschwerden, Eingaben oder sonstigen Hinweisen auf mögliche Datenschutzverstöße tätig.

Überwiegend handelte es sich dabei um Beschwerden betroffener Bürger, die selbst konkrete Anhaltspunkte für einen Datenschutzverstoß darlegten oder einen vermeintlichen Verstoß schilderten. Teilweise wandten sich auch Unternehmen, Vereinigungen oder Interessenverbände an die Aufsichtsbehörden, weil sie annahmen, dass bestimmte Unternehmen, Vereine etc. gegen datenschutzrechtliche Vorschriften verstoßen hätten.

Wenn sich aus Meldungen in der Presse, dem Fernsehen oder dem Internet Hinweise auf mögliche Verstöße ergaben, gingen die Aufsichtsbehörden auch diesen nach.

Die genannte Zahl betrifft nur Fälle, die eine aktenmäßige Bearbeitung erforderten.
Eingaben, die aufgrund Unzuständigkeit an die zuständige Aufsichtsbehörde in ein anderes Bundesland oder an den Bundesbeauftragten für den Datenschutz abgegeben wurden, sind in diese Statistik nicht eingeflossen, es sei denn, die Unzuständigkeit stellte sich ausnahmsweise erst im Laufe der Bearbeitung heraus. Ebenso wenig erfasst wurden telefonische Eingaben, die telefonisch abgehandelt werden konnten, z.B. durch Hinweis auf eine bereits erfolgte Überprüfung oder Nichtanwendbarkeit des BDSG. Zahlenmäßig dürften diese mindestens in der gleichen Größenordnung gelegen haben wie die aktenmäßig bearbeiteten Fälle.

Die 358 statistisch erfassten Überprüfungen von Eingaben, Beschwerden und Pressemeldungen durch die Regierungspräsidien betrafen:

- in 81 Fällen Anbieter von Telediensten (Provider von Internetzugängen und -inhalten),
- in 71 Fällen Stellen und Unternehmen der Direktmarketing- und Werbewirtschaft,
- in 44 Fällen Banken, Kreditinstitute und EDV-Dienstleister im Zahlungsverkehr,
- in 27 Fällen Handels- und Wirtschaftsauskunfteien,
- in 21 Fällen den Datenschutz in Arbeitsverhältnissen,
- in 15 Fällen Adresshändler, Adressverlage und Herausgeber öffentlicher Verzeichnisse,
- in 11 Fällen Versicherungsgesellschaften,
- in 11 Fällen das Gesundheitswesen (Apotheken, Ärzte, Krankenhäuser und Pflegeheime),

- in 10 Fällen Vereine (Sport, Soziales, Kultur) sowie deren Landes- und Bundesverbände,
- in 8 Fällen die Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA),
- in 8 Fällen Vermieter, Wohnungs- und Immobilienverwaltungsfirmen,
- in 7 Fällen die Videoüberwachung von Grundstücken, Häusern und Wohnungen,
- in 6 Fällen Unternehmen des Groß- und Einzelhandels,
- in 6 Fällen Unternehmen der Freizeit-, Touristik- und Reisebranche,
- in 5 Fällen Unternehmen der Versandhandelsbranche,
- in 4 Fällen Kreditkartenunternehmen,
- in 4 Fällen Markt- und Meinungsforschungsunternehmen,
- in 4 Fällen Inkassounternehmen,
- in 15 Fällen sonstige Stellen (Partnervermittlung, Softwarehersteller, Autovermietung, Spedition, Gen-Labor).

Fast jede dritte Beschwerde war begründet. In insgesamt 118 Fällen wurden bei den Nachforschungen der Aufsichtsbehörden unzulässige Verarbeitungen personenbezogener Daten und andere datenschutzrechtliche Verstöße festgestellt, die zu Beanstandungen der jeweiligen Verarbeitungsverfahren bei den betroffenen Stellen führten.

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

- in 39 Fällen bei werbetreibenden Stellen (inkl. Werbung per Telefax, SMS und E-Mail),
- in 33 Fällen bei Anbietern von Tele- und Mediendiensten (Access- und Content-Provider),
- in 18 Fällen bei Kreditinstituten und Banken,
- in 7 Fällen bei eingetragenen Vereinen und Dachverbänden,
- in 5 Fällen bei Adresshandelsunternehmen,
- in 4 Fällen bei Handels- und Wirtschaftsauskunfteien,
- in 3 Fällen bei Groß- und Einzelhändlern
- sowie in jeweils einem Fall bei einer Versicherung, einem Arzt, einer Apotheke, einem Videoüberwachungsanlagenbetreiber, einem Kreditkartenunternehmen, einem Markt- und Meinungsforscher, einem Versandhandelsunternehmen, einem Unternehmen der Touristikbranche und einem Arbeitgeber, der mit Personal- und Bewerberdaten unzulässig umging.

Ca. 20 v.H. der eingeleiteten Überprüfungen konnten im Berichtsjahr noch nicht abgeschlossen werden. Die Erledigung dieser Fälle wird in den nächsten Tätigkeitsbericht einfließen.

Von den noch aus den Vorjahren anhängigen Beschwerden, die in vielen Fällen äußerst vielschichtige und komplexe Verarbeitungszusammenhänge betrafen, wurden im Berichtsjahr 39 Fälle abgeschlossen. Die Beurteilung dieser in der Regel nur mit hohem Ermittlungsaufwand aufklärbaren Fälle durch die Aufsichtsbehörden ergab, dass davon 18 Eingaben begründet waren.

Die beanstandeten 18 Verstöße gegen Datenschutzbestimmungen wurden festgestellt:

- in 5 Fällen bei Vereinen und einem Dachverband,
- in 3 Fällen bei einem Adressverlag,
- in 3 Fällen bei Banken,
- in 2 Fällen im Bereich des Arbeitnehmerdatenschutzes
- sowie in jeweils einem Fall bei einer Versicherung, einem Internetprovider, einem Direktmarketingunternehmen, einer Auskunftei und einer Freizeiteinrichtung, die personenbezogene Daten unzulässig gespeichert, genutzt oder übermittelt hatten.

Bei den im Berichtsjahr insgesamt durchgeführten Prüfungen von Eingaben, Beschwerden und Hinweisen auf Datenschutzverstöße bestand in 27 Fällen Veranlassung für Überprüfungen vor Ort. Diese wurden zum Teil ohne vorherige Anmeldung und zum Teil mit vorheriger Ankündigung durchgeführt. Bei einer Anmeldung wurde der Grund bzw. der zu prüfende Teil der Datenverarbeitung nicht vorher mitgeteilt. Nur so ist sichergestellt, dass die tatsächliche Datenverarbeitung eingesehen werden kann.
Als positiv hat sich unter anderem herausgestellt, dass die Unternehmen bzw. ihre Vertreter im Rahmen der Prüfung vor Ort wesentlich offener Auskünfte erteilen und ihre Datenverarbeitung darstellen, als sie dies im schriftlichen Verfahren tun würden. Sehr selten wird vom Auskunftsverweigerungsrecht nach § 38 Abs. 3 Satz 2 BDSG Gebrauch gemacht.

## 4. Anfragen zu datenschutzrechtlichen Problemstellungen und Beratungstätigkeit

### 4.1 Statistische Auswertung der eingegangenen Anfragen

Bei den Aufsichtsbehörden gingen im Berichtsjahr 168 Beratungsersuchen von Gewerbetreibenden, Unternehmen, Vereinen und Verbänden sowie von Bürgerinnen und Bürgern und von Betriebsräten ein, die eine aktenmäßige schriftliche Bearbeitung erforderlich machten.

Damit sind die qualifizierten schriftlichen Beratungsersuchen um 50 v.H. gegenüber dem Vorjahr angestiegen. Die telefonischen Beratungen wurden bis auf wenige Ausnahmen, die schriftlich dokumentiert wurden, statistisch nicht erfasst, dürften jedoch mindestens in der gleichen Größenordnung liegen.

Moderne Datenverarbeitung und Kommunikation sind heute aus fast keinem Lebensbereich mehr wegzudenken. Entsprechend vielfältig gestalteten sich die bei den Aufsichtsbehörden eingegangenen Beratungsanfragen von Bürgerinnen und Bürgern zu fast allen Facetten des menschlichen und wirtschaftlichen Zusammenlebens. Aber auch immer mehr Unternehmen erkennen, dass die frühzeitige Zusammenarbeit mit den eigenen betrieblichen Datenschutzbeauftragten und der zuständigen Datenschutzaufsichtsbehörde oftmals eine wichtige Voraussetzung für die reibungslose Implementierung und den wirtschaftlichen Erfolg geplanter Datenverarbeitungsverfahren ist.

Im Ballungsraum Rhein/Main finden sich neben den Firmensitzen der großen nationalen und internationalen Banken und Finanzdienstleister auch die Geschäftssitze und Niederlassungen vieler weiterer vielfach ausländischer Unternehmen unterschiedlichster Dienstleistungssparten, die vom Datenschutzrecht als einem Querschnittsthema, dass fast alle Lebens- und Arbeitsbereiche betrifft, erfasst werden.

Viele dieser überwiegend auch international agierenden Unternehmen haben datenschutzrechtliche Anforderungen inzwischen in ihren Qualitätsstandards definiert und lassen die Einhaltung dieser datenschutzrechtlichen Erfordernisse von ihren betrieblichen Datenschutzbeauftragten gemeinsam mit internen Qualitätsprüfern oder der Innenrevision regelmäßig kontrollieren. Diese intensive Befassung mit datenschutzrechtlichen Fragestellungen bei der Verarbeitung und Übermittlung personenbezogener Personal- oder Kundendaten führte - insbesondere nach der Novellierung des Bundesdatenschutzgesetzes im Mai 2001 mit ihren weitreichenden Neuregelungen unter anderem zur Auslandsdatenverarbeitung - zu einem enormen Anstieg der Anfragen international auftretender Großunternehmen beim Regierungspräsidium Darmstadt.

Auch die Anzahl der Fragen im Zusammenhang mit der privaten und betrieblichen Nutzung des Internet, der datenschutzgerechten Gestaltung von Tele- und Mediendiensten sowie der Verwirklichung neuer Geschäftsideen im Internet ist erheblich angestiegen.

Ein weiterer Schwerpunkt war - wie schon in den letzten Jahren - die Beratung und Unterstützung der betrieblichen Datenschutzbeauftragten in den Unternehmen.

Insgesamt ergaben sich folgende inhaltliche Schwerpunkte:

25 Anfragen von betrieblichen Datenschutzbeauftragten im Zusammenhang mit der eigenen Aufgabenerfüllung im Betrieb (Schulungsbedarf, eigene Weiterbildung, Schulung der Mitarbeiter, Verschwiegenheit nach § 5 BDSG, Vorabkontrolle nach § 4d BDSG, Verfahrensverzeichnis nach § 4g Abs. 2 BDSG) sowie zur Auftragsdatenverarbeitung nach § 11 BDSG, der Befristung des Dienstvertrages von externen Datenschutzbeauftragten (siehe Nr. 17.1), dem Umfang des Freistellungsanspruchs und Fragen zur Zusammenarbeit mit dem Betriebsrat.

23 Anfragen von verarbeitenden Stellen oder deren betrieblichen Datenschutzbeauftragten zur Neuregelung der Meldepflicht nach § 4d BDSG. Neben der Frage vieler DV-Dienstleister, ob die Voraussetzungen zur Meldung nach der erfolgten BDSG-Novelle noch vorliegen (hier vor allem Datenträgervernichter und EDV-Dienstleister von Banken), wurden auch Fragen zum Umfang der Angaben nach § 4e BDSG, die sowohl nach § 38 Abs. 2 BDSG als auch nach § 4g Abs. 2 BDSG offen gelegt werden müssen, diskutiert (siehe Nr. 2).

19 Anfragen zur Auslandsdatenverarbeitung, insbesondere zu internationalen Personaldatenverarbeitungen von Großkonzernen und zur Zulässigkeit der Erhebung und Verarbeitung von personenbezogenen Daten von Kunden und Nutzern im Internet (WWW) durch ausländische Stellen (siehe Nr. 7).

13 Anfragen zur datenschutzgerechten Ausgestaltung von Medien- und Telediensten. Darunter Fragen zur Formulierung und Platzierung von Anbieterkennzeichnungen sowie korrekten Datenschutzhinweisen auf WWW-Seiten. Mehrere Beratungsersuchen zum genauen Text der nach dem TDDSG notwendigen Einwilligungserklärungen oder unterrichtenden Hinweise für Nutzer, aber auch technisch orientierte Fragen nach geeigneten Verschlüsselungsverfahren für Laptops, E-Mail und WWW und datenschutzrechtlich zulässigen Authentifizierungs- und Verifizierungsmechanismen beim Versand von SMS und Newsletter durch Provider.

10 Anfragen aus dem Gesundheitssektor, darunter Fragen zur Aufbewahrung von Unterlagen, zur Fernwartung von PCs mit Patientendaten und zur Zulässigkeit und Sicherheit der Datenverarbeitung und -übermittlung in und zwischen Arztpraxen sowie zur sicheren Nutzung von E-Mail und WWW-Seiten im gesundheitlichen Beratungsbereich (siehe Nr. 13).

10 Anfragen zum Umgang der Werbewirtschaft mit Adressdaten. Fragen von Bürgerinnen und Bürgern zum Adresshandel und zur Weitergabe und Nutzung von Adressdaten durch Listbroker und Lettershops.

9 Anfragen im Zusammenhang mit geplanten oder bereits existierenden WWW-Seiten, auf denen unter Veröffentlichung der jeweiligen personenbezogenen Daten, teilweise mit Foto, nach säumigen Schuldnern gesucht oder vor Personen gewarnt wird. Diese Vorhaben sollten z.T. Warn- und Prangerfunktion erfüllen, z.T. befassten sie sich auch mit dem Erteilen von Bonitätsauskünften über das Internet (siehe Nr. 8.1). Eine Anfrage betraf die Suche nach vermissten Familienangehörigen oder Bekannten (siehe Nr. 8.2).

9 Anfragen aus dem Bereich des Arbeitnehmerdatenschutzes, wobei immer noch Fragen der privaten Internetnutzung (WWW und E-Mail) im Betrieb im Vordergrund standen (siehe Nr. 8.10).

8 Anfragen von sportlich, sozial und kulturell orientierten Vereinen und Verbänden zum zulässigen Umgang mit eigenen Mitgliederdaten. Die Fragen betrafen unter anderem die Möglichkeiten der werblichen Nutzung von Mitgliederdaten sowie den Aushang bzw. die Übermittlung und Veröffentlichung von Mitgliederdaten (auch im WWW) zu unterschiedlichsten Zwecken. Ein großer deutscher Sportverband wurde bei der datenschutzgerechten Ausgestaltung der Vergabe von Eintrittskarten für eine internationale Großveranstaltung im Vorfeld intensiv beraten (siehe Nr. 14.3).

5 Anfragen zur Zulässigkeit der Videoüberwachung von Wohnanlagen durch Vermieter und Hausverwaltungen. Hier handelte es sich hauptsächlich um Fragen der Zulässigkeit und der ausreichenden Beschilderung des beobachteten Raumes nach § 6b BSDG.

Weitere Anfragen betrafen die SCHUFA, ein Projekt in der Markt- und Meinungsforschungsbranche, die Arbeit der Handels- und Wirtschaftsauskunfteien sowie die Datenverarbeitung von Banken, Versicherungen und deren Dienstleistungsunternehmen.

### 4.2 Informationsveranstaltungen

Am 27. Oktober 2001 luden die Industrie- und Handelskammer (IHK) Darmstadt, das IHK-Forum Rhein-Main und das Regierungspräsidium Darmstadt zu einer gemeinsam Informationsveranstaltung über das neue Bundesdatenschutzgesetz ein. Die Vertreterinnen und Vertreter des Regierungspräsidiums Darmstadt erläuterten die Grundzüge des Datenschutzrechts und die wesentlichen Neuregelungen. Über 70 Teilnehmer belegten das große Interesse der Wirtschaft.

Die Auswirkungen der BDSG-Novelle auf den Bankenbereich wurden in einer Informationsveranstaltung des Bundesverbandes deutscher Banken beleuchtet, an der Bedienstete der Aufsichtsbehörde beim Regierungspräsidium Darmstadt als Referenten mitwirkten.

Auf Einladung der Hessischen Landesstelle gegen die Suchtgefahren e.V.(HLS) referierten Vertreter des Regierungspräsidiums Darmstadt bei einem Kompaktseminar über die Neuerungen des Bundesdatenschutzgesetzes und deren Auswirkungen auf den Datenschutz in der Suchthilfe und stellten sich den Fragen der Seminarteilnehmer. Zu begrüßen war, dass dabei eine Vielzahl von Beratungsstellen in den Verbänden der Freien Wohlfahrtpflege und deren Mitgliedsorganisationen erreicht werden konnte, die in der HLS zusammengeschlossen sind. Aufgrund der vielfältigen Fragen zur Erhebung, Verarbeitung und Nutzung von Klientendaten wird die Aufsichtsbehörde auch weiterhin in Kontakt mit der HLS bleiben.

Auch bei anderen Informationsveranstaltungen nutzen die Vertreterinnen und Vertreter der Aufsichtsbehörde die Gelegenheit, ihre Auffassungen darzulegen und dadurch präventiv auf die Beachtung der neuen Datenschutzvorschriften hinzuwirken.

### 4.3 Versendung von Informationsmaterial und Orientierungshilfen

Die Datenschutzaufsichtsbehörde beim Regierungspräsidium Darmstadt hält auch datenschutzrechtliches Informationsmaterial für Bürgerinnen und Bürger sowie für Unternehmen und deren Datenschutzbeauftragte zu unterschiedlichsten Fragestellungen des Datenschutzrechts bereit, das auf Anfrage gerne formlos zur Verfügung gestellt wird. Im Berichtsjahr haben Interessierte von diesem Angebot in über 100 Fällen Gebrauch gemacht.

Die meisten Anforderungen von Informationsmaterial, Merkblättern und Hinweisen erfolgten durch die betrieblichen Datenschutzbeauftragten von Unternehmen. Den größten Anteil hatten hierbei Unterlagen und Hilfen zur Aufgabenerfüllung im Betrieb, gefolgt von den aufgrund der gesetzlichen Änderungen umfassend überarbeiteten Merkblättern und Hinweisen zur Meldepflicht nach § 4d BDSG.

Bei den Verbraucherinnen und Verbrauchern war kein besonderer Interessenschwerpunkt auszumachen. Die angebotenen Materialien zum Direktmarketing oder zur Datenverarbeitung im Verein wurden, genauso wie die Tipps zum Umgang mit Spam-E-Mails, unverlangter Faxwerbung oder die Auskünfte über die Arbeit der SCHUFA und der Handels- und Wirtschaftsauskunfteien, gerne von den Anfragerinnen und Anfragern angenommen.

Auch die Möglichkeit, einige Unterlagen wie z.B. Mustertexte, Antragsformulare und Merk- und Hinweisblätter über die Homepage des Datenschutzdezernates beim Regierungspräsidium Darmstadt im WWW abzurufen, findet regen Zuspruch. Im Berichtsjahr zählten die Seiten des Datenschutzdezernates in mehreren Monaten - insbesondere nach der Teilnahme an einigen öffentlichkeitswirksamen Veranstaltungen (siehe Nr. 4.2) - zu den am häufigsten abgefragten WWW-Seiten des Regierungspräsidiums Darmstadt.

## 5. Anlassunabhängige Kontrollen

Wie unter Nr. 1 dieses Berichtes ausgeführt, konnten vor dem In-Kraft-Treten der BDSG-Novelle am 23. Mai 2002 nur in bestimmten Bereichen

anlassunabhängige Kontrollen durchgeführt werden (§ 38 Abs. 2 BDSG a.F., TDDSG, Mediendienstestaatsvertrag (MDStV)).
Erst ab dem 23. Mai 2002 waren generell anlassunabhängige Kontrollen möglich.

Im Berichtsjahr wurden 15 anlassunabhängige Kontrollen durchgeführt.

Diese betrafen folgende Branchen/Bereiche:

- Dienstleistungen in Form von Auftragsdatenverarbeitung 4
- Konzerndatenverarbeiter/verbundene Unternehmen 4
- Vereinsdatenverarbeitung 2
- Adresshandel/Listbroking/Lettershop 2
- Akten- und Datenträgervernichter 2
- Markt- und Meinungsforschung 1

Die Prüfungen führten zu folgendem Ergebnis:

- Wesentliche Beanstandungen 13
- Kleinere Beanstandungen/Empfehlungen 2

Folgende wesentliche Mängel wurden am häufigsten festgestellt:

1. Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten nicht erfüllt; fehlende Fachkompetenz oder unzulängliche Aufgabenwahrnehmung des betrieblichen Datenschutzbeauftragten.
2. Keine (schriftlichen) Weisungen nach § 11 BDSG.
3. Unzureichende Regelungen der Zugriffsrechte, fehlende Passwortregelungen und sonstige Datensicherheitsmängel

Neben den dargestellten 15 "reinen" anlassunabhängigen Prüfungen wurden auch die 27 Überprüfungen aus konkretem Anlass (siehe Nr. 3) überwiegend dazu genutzt, um die Datenverarbeitung der verantwortlichen Stellen umfassender zu prüfen. Die Prüfungen wurden also nicht nur auf den konkreten Beschwerdegegenstand beschränkt.
Die festgestellten Versäumnisse und daraus entstandenen Beanstandungen entsprechen denen aus den "reinen" anlassunabhängigen Prüfungen.

Anlassunabhängige Prüfungen sind zwar wichtig für eine präventive Datenschutzaufsicht, nicht minder wichtig sind hierfür jedoch die allgemeinen Informationsveranstaltungen und die Beratung zu konkreten Fragen (siehe Nr. 4). Daher setzten die Aufsichtsbehörden ihre Prioritäten im Berichtsjahr bei der Informations- und Beratungstätigkeit.

## 6. Ordnungswidrigkeitenverfahren

Im Berichtsjahr wurden von den Regierungspräsidien zwei Verfahren nach dem Gesetz über Ordnungswidrigkeiten eingeleitet. Gegen die Geschäftsführer des Call-Centers einer Bank wurde wegen nicht rechtzeitig erfolgter Bestellung eines Datenschutzbeauftragten eine Geldbuße von je 1.500 DM verhängt. Das bereits im letzten Tätigkeitsbericht erwähnte Bußgeldverfahren gegen den Geschäftsführer eines Möbelhauses (14. Tätigkeitsbericht vom 18. September 2001, LT-Drucks. 15/2950 Nr. 19) wurde nach bis dahin zweijähriger Dauer und einem Verfahren vor dem Landgericht Darmstadt mit einem rechtskräftigen Bußgeld in Höhe von 3.000 DM abgeschlossen.

Der Bundesgesetzgeber hat mit der Novellierung des BDSG den betrieblichen Datenschutzbeauftragten in der Privatwirtschaft einige neue Aufgaben übertragen und ihre Position gestärkt. Gleichzeitig wurde die Meldepflicht von Unternehmen bzw. Verfahren deutlich eingeschränkt (siehe Nr. 2.2). Verstöße gegen die Meldepflicht nach altem Recht haben die Aufsichtsbehörden vor In-Kraft-Treten der Novelle nicht mehr sanktioniert, da in allen Fällen abzusehen war, dass die Meldepflicht entfallen wird.

Da die BDSG-Novelle die Eigenverantwortung der Unternehmen weiter in den Vordergrund stellte, werden die Aufsichtsbehörden künftig vor allem Wert darauf legen, dass alle infrage kommenden nicht öffentlichen Stellen ihrer Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten

nachkommen. Sollte sich der Bekanntheitsgrad dieser wichtigen betrieblichen Datenschutzinstitution gerade in mittleren Betrieben nicht deutlich erhöhen, wird die Datenschutzaufsichtsbehörde wegen der Nichtbestellung oder auch Untätigkeit eines betrieblichen Datenschutzbeauftragten nach § 43 Abs. 1 Nr. 2 BDSG einen Schwerpunkt bei der Einleitung künftiger Bußgeldverfahren setzen müssen.

Als weiterer künftiger Bußgeldschwerpunkt zeichnet sich schon jetzt der regelmäßige Verstoß vieler Werbetreibender aller Branchen gegen die Pflicht ab, nach § 28 Abs. 4 Satz 2 BDSG bei der adressierten Werbung die Betroffenen darauf hinzuweisen, dass sie der werblichen Nutzung ihrer Daten widersprechen können. Bis zum Zeitpunkt der Berichterstellung waren Werbeschreiben mit dem seit Mai 2001 gesetzlich vorgeschriebenen Hinweistext eher die Ausnahme, obwohl auch dieser Verstoß mit einem Bußgeld bis zu 25.000 € geahndet werden kann (siehe auch Nr. 15).

**Einzelfälle**

## 7. Aspekte internationaler Datenverarbeitungen

### 7.1 Datenweitergabe an unselbständige Zweigstelle in Drittstaaten

Die vielfältigen Beratungsanfragen, welche bei der Aufsichtsbehörde in Darmstadt zum Thema Auslandsdatenverarbeitung eingingen, betrafen unter anderem die Frage, wann überhaupt die besonderen Anforderungen der §§ 4b, 4c BDSG für Datenübermittlungen in so genannten Drittstaaten, d.h. in Staaten außerhalb der Europäischen Union und außerhalb des Europäischen Wirtschaftsraumes, gelten.

Der Bevollmächtigte eines hier ansässigen Unternehmens bat um Auskunft, ob die §§ 4b, 4c BDSG auch dann zu beachten sind, wenn personenbezogene Daten an in den USA und anderen Drittstaaten befindliche unselbstständige Zweigstellen desselben Unternehmens weitergegeben werden.

Nach dem Wortlaut der §§ 4b, 4c BDSG sind nur "Übermittlungen" erfasst. Eine "Übermittlung" liegt nach der Begriffsbestimmung in § 3 Abs. 4 Nr. 3 BDSG jedoch nur dann vor, wenn Daten an einen "Dritten" gelangen. Hierunter fallen nach § 3 Abs. 8 Satz 2 BDSG nur Personen oder Stellen außerhalb der verantwortlichen Stelle. Da hierbei auf die jeweilige gesellschaftliche Einheit abzustellen ist, stellt eine Datenweitergabe an eine rechtlich unselbständige Zweigstelle an sich keine Übermittlung dar.

Andererseits wird der "Datenimporteur" im Drittstaat in den §§ 4b, 4c BDSG nicht als "Dritter" bezeichnet, wie es sprachlich konsequent gewesen wäre, sondern nur als "Stelle". In anderen Paragraphen des BDSG hat der Gesetzgeber die redaktionellen Unschärfen durch die Novelle überwiegend beseitigt und dort, wo von "Übermittlung" die Rede ist, auch den Begriff des "Dritten" verwendet, z.B. in § 28 Abs. 4 Satz 3 und Abs. 5 Satz 1 BDSG. Die Gesetzesbegründung enthält leider keine klare Aussage, was letztlich in §§ 4b, 4c BDSG gemeint ist.

Da die §§ 4b, 4c BDSG der Umsetzung der Art. 25 und 26 der EG-DSRL dienen, ist deren Auslegung maßgeblich. In diesen Vorgaben ist zwar auch von "Übermittlung" die Rede, allerdings differenziert die EG-DSRL in ihren Begriffsbestimmungen nicht zwischen einer Weitergabe an Dritte (im BDSG = Übermittlung) und anderen Formen der Verbreitung, Bereitstellung und Bekanntgabe (Art. 2a EG-DSRL, siehe auch Dammann/Simitis, Kommentar zur EG-DSRL, 1. Aufl. 1997, Rn. 17). Der Begriff der "Übermittlung" ist somit umfassender als der entsprechende Begriff des BDSG.

Wenngleich die Richtlinie differenzierende Ausgestaltungen nicht völlig ausschließt (Art. 5 EG-DSRL, Dammann/Simitis a.a.O.), so wurde im konkreten Fall jedoch kein Spielraum gesehen. In Übereinstimmung mit den Mitgliedern des Düsseldorfer Kreises vertrat die Aufsichtsbehörde daher die Auffassung, dass die Datenweitergabe an nicht selbstständige Zweigstellen außerhalb der EU und des EWR im Lichte der EG-DSRL zu interpretieren und damit als Datenübermittlung (im Sinne der §§ 4b, 4c BDSG) zu behandeln ist.

Der Gesetzgeber sollte dies bei der geplanten umfassenden Novelle des BDSG ("2. Stufe") klarstellen - ebenso wie durch § 3 Abs. 8 Satz 3 BDSG unmissverständlich geregelt ist, dass die Datenweitergabe an Auftragnehmer außerhalb der EU und des EWR als Übermittlung einzustufen ist.

### 7.2 Bedeutung der Standardvertragsklauseln - Genehmigungs- oder Vorlagepflicht?

Wenn bei einer Datenübermittlung in Drittstaaten kein angemessenes Schutzniveau bei der Daten importierenden Stelle im Drittstaat gewährleistet ist und auch keiner der in § 4c Abs. 1 Satz 1 Nr. 1 bis 6 BDSG aufgeführten Ausnahmetatbestände greift, darf die Übermittlung nur erfolgen, wenn die Aufsichtsbehörde sie genehmigt hat (§§ 4b, 4c Abs. 2 BDSG).

Die Genehmigung darf nur erteilt werden, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist. Da sich solche Garantien laut § 4c Abs. 2 Satz 1, letzter Halbsatz BDSG insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregeln ergeben können, wurde die Aufsichtsbehörde vielfach um Beratung hinsichtlich der inhaltlichen Ausgestaltung solcher Regelungen gebeten. Wie bereits im vorletzten Tätigkeitsbericht erwähnt (13. Tätigkeitsbericht vom 30. August 2000, LT-Drucks. 15/1539 Nr. 10) hat die Arbeitsgruppe nach Art. 29 EG-DSRL ein Arbeitspapier herausgegeben, welches die wesentlichen Anforderungen definiert (WP 12).

Im Interesse der Wirtschaft, aber auch der Betroffenen, nach Vereinfachung und Vereinheitlichung hat die EU-Kommission außerdem Standardvertragsklauseln erlassen.

Die Entscheidung der EU-Kommission vom 15. Juni 2001 bezieht sich auf die "normale" Übermittlung in Drittstaaten. Da die hierfür erlassenen Klauseln für solche Übermittlungen nicht passen, bei denen im Drittstaat nur eine untergeordnete Datenverarbeitungsdienstleistung erbracht wird, also vom Charakter der Tätigkeit her (ungeachtet des § 3 Abs. 8 Satz 3 BDSG) eine Auftragsdatenverarbeitung vorliegt, wurden hierfür mit Entscheidung der EU-Kommission vom 27. Dezember 2001 spezielle Vertragsklauseln erlassen.

Die Aufsichtsbehörde hat daher in der Regel die Verwendung dieser Standardklauseln bzw. die Orientierung an den im Laufe des Berichtsjahres von der Gruppe nach Art. 29 EG-DSRL erarbeiteten Entwürfen empfohlen (zu Unternehmensregelungen siehe nachfolgend Nr. 7.3).

Wichtig ist dabei die Unterscheidung zwischen den beiden Arten von Standardvertragsklauseln.

Wenn beispielsweise sämtliche Kundendaten aller konzernangehöriger Unternehmen zentral auf einem Server bei einem konzernangehörigen Unternehmen in den USA gespeichert werden, ist maßgeblich, welche Befugnisse und Aufgaben das US-Unternehmen hat.
Soll dieses nur die Datensicherung und technische Wartung durchführen, also nur wie ein externes Rechenzentrum ohne eigene Entscheidungen und Zugriffsbefugnisse tätig werden, sind die am 27. Dezember 2001 verabschiedeten Standardklauseln geeignet.
Soll das US-Unternehmen jedoch darüber hinausgehende Aufgaben und Kompetenzen erhalten, kommen nur die am 15. Juni 2001 verabschiedeten Standardklauseln in Betracht.

Häufig fragten Bevollmächtigte von Unternehmen nach, ob auch bei Verwendung der Standardvertragsklauseln eine Genehmigungspflicht nach § 4c Abs. 2 BDSG bestehe oder ob es hier Erleichterungen gäbe. Diese Frage drängte sich geradezu auf, enthalten doch die §§ 4b, 4c BDSG keinerlei Aussage hierzu. Die Problematik wurde daher intensiv in der Arbeitsgruppe "Internationaler Datenverkehr" des Düsseldorfer Kreises erörtert.

Einerseits enthält § 4c Abs. 2 BDSG keine Ausnahme von der Genehmigungspflicht, also keine Sonderregelung für Standardvertragsklauseln.
Andererseits sind die Aufsichtsbehörden an die Entscheidung der EU-Kommission gebunden, dürfen also bei vollständiger und unveränderter Verwendung der Standardklauseln insoweit zu keiner anderen Bewertung

gelangen. Daher bedeutete ein Genehmigungserfordernis ein unnötiges bürokratisches Hindernis. Von der Sache ist es gerechtfertigt, diejenigen Unternehmen, welche sich für die Standardklauseln entscheiden, verfahrensmäßig zu privilegieren. Nur wer eine individuelle Lösung sucht, sollte dem Genehmigungserfordernis unterworfen sein.

Erwogen wurde, ob zumindest eine Vorlagepflicht besteht. Eine solche ist im BDSG nicht vorgesehen. Ob sie als "Minus" aus dem Genehmigungserfordernis des § 4c Abs. 2 BDSG ableitbar ist, erscheint fraglich.

Letztlich vertritt die Aufsichtsbehörde in Übereinstimmung mit dem Düsseldorfer Kreis die Auffassung, dass bei vollständiger, unveränderter Verwendung der Standardvertragsklauseln weder eine Genehmigungs- noch eine Vorlagepflicht besteht.

Selbstverständlich aber kann die Aufsichtsbehörde im Rahmen ihrer Aufsichtstätigkeit nach § 38 BDSG die Vorlage des Vertrages fordern. Dieser konkreten Aufforderung müssen die Unternehmen dann nachkommen (siehe auch Innenministerium Baden-Württemberg, Hinweis Nr. 40 zum Datenschutz für private Unternehmen, B.2.4).

### 7.3 Verbindliche Unternehmensregelungen

Werden personenbezogene Daten innerhalb eines internationalen Konzerns übermittelt und gelangen dadurch an Unternehmen bzw. Unternehmensteile in Drittstaaten, ist die "Vertragslösung" (individueller Vertrag/Standardvertrag - siehe Nr. 7.2) oft zu umständlich. Es müsste eine Vielzahl von Einzelverträgen geschlossen und bei der Aufnahme neuer Unternehmen in den Konzern ständig weitere Verträge geschlossen werden.

Wenn sich im Drittstaat nur rechtlich unselbstständige Zweigstellen befinden (siehe Nr. 7.1), erscheint die Vertragslösung ebenfalls nicht als passend, denn das Verhältnis zwischen Unternehmenssitz und unselbständigen Zweigstellen dürfte nicht durch Vertragsklauseln geprägt sein.

Daher sieht § 4c Abs. 2 Satz 1 letzter Halbsatz BDSG vor, dass sich "ausreichende Garantien" im Sinne des § 4c Abs. 2 BDSG nicht nur aus Vertragsklauseln, sondern auch aus "verbindlichen Unternehmensregelungen" ergeben können.

Inhaltlich müssen auch solche Regelungen den im Arbeitspapier Nr. 12 der Gruppe nach Art. 29 der EG-DSRL genannten Anforderungen genügen (siehe Nr. 7.2).
Da diese Anforderungen in den Standardverträgen konkretisiert wurden, besteht die größte Gewähr, dass verbindliche Unternehmensregelungen "ausreichende Garantien" vorweisen, wenn sie sich an den Standardverträgen bzw. den hieraus ableitbaren Standards orientieren (siehe Innenministerium Baden-Württemberg, Hinweis Nr. 40, B.2.5 und 3).

Wichtig ist, dass der Geltungsbereich bzw. der Gegenstand einer Unternehmensregelung klar definiert wird. Sollen die Regelungen nur bezüglich solcher Daten gelten, die aus Deutschland bzw. aus der EU/dem EWR stammen oder bezüglich aller personenbezogenen Daten, die im Konzern verarbeitet werden?

Zwingend erforderlich sind Regelungen rechtlich nur, soweit es sich um Daten handelt, die von hier aus in Drittstaaten ohne angemessenes Datenschutzniveau übermittelt werden, und soweit nicht bereits ein Ausnahmetatbestand nach § 4c Abs. 1 BDSG vorliegt. Wünschenswert wäre gleichwohl eine "universelle" Gültigkeit der Regelungen.
Soll die Unternehmensregelung nicht für alle personenbezogenen Daten gelten, müssen die Datenbestände unter Umständen getrennt werden.

Vielfältige Unsicherheiten bestehen hinsichtlich der konkreten rechtlichen Bedeutung bzw. Behandlung von verbindlichen Unternehmensregelungen, vor allem hinsichtlich der Genehmigungsbedürftigkeit und des Genehmigungsgegenstandes.
Da Unternehmensregeln in § 4c Abs. 2 BDSG erwähnt sind, also im Zusammenhang mit der Genehmigungspflicht, ging das Regierungspräsidium Darmstadt bei seinen Beratungen davon aus, dass selbst "universell gültige"

Unternehmensregelungen nicht von der Genehmigungspflicht entheben (ebenso: Gesetzesbegründung zu § 4c Abs. 2 BDSG und Innenministerium Baden-Württemberg, Hinweis Nr. 40, B.2.2).
Da Gegenstand von Genehmigungen nach § 4c Abs. 2 BDSG nur die einzelnen konkreten Übermittlungen sein können, kann eine verbindliche Unternehmensregelung als solche nicht genehmigt werden, wenn sie nur abstrakte Regelungen enthält, ohne die betroffenen Arten personenbezogener Daten und die Drittstaaten konkret zu bezeichnen. Eine rein abstrakte Unternehmensregelung wäre jedoch für die Prüfung eines konkreten Genehmigungsantrages heranzuziehen (Innenministerium Baden-Württemberg a.a.O.).

Bezüglich der vorgenannten Fragen sind die Diskussionen im Düsseldorfer Kreis jedoch noch nicht abgeschlossen, da die gesetzlichen Regelungen und die Vorgaben der EG-DSRL keine eindeutigen Antworten geben. Daher wies die Aufsichtsbehörde in ihren Beratungen stets darauf hin, dass sie nur den aktuellen Diskussionsstand bzw. ihre eigenen Einschätzungen wiedergeben kann.

Interessant sind in diesem Zusammenhang auch Überlegungen der EU-Kommission, ob sie selbst Unternehmensregelungen internationaler Konzerne bewerten und eine Entscheidung im Sinne des Art. 26 Abs. 4 EG-DSRL hierzu treffen könne. Für internationale Konzerne, die in vielen Staaten der EU/des EWR vertreten sind, wäre dies eine erhebliche Verfahrenserleichterung.

### 7.4 Übermittlung von Arbeitnehmerdaten in internationalen Konzernen

Viele der an das Regierungspräsidium Darmstadt herangetragenen Beratungsersuchen zum Drittstaatentransfer betrafen die Übermittlung von Mitarbeiterdaten in internationalen Konzernen.

Dabei wurde offensichtlich, dass man sich oftmals nur um die spezielle Drittstaatenproblematik Gedanken machte. Übersehen wurde, dass die §§ 4b, 4c BDSG insoweit nur zusätzliche Anforderungen stellen. Da es kein Konzernprivileg gibt, muss stets zuerst geprüft werden, ob die Übermittlung bzw. die Weitergabe von einer Konzerngesellschaft an eine andere überhaupt in Betracht kommt, maßgeblich ist insbesondere die Auslegung des § 28 BDSG. Es gelten zunächst die gleichen Anforderungen wie bei Übermittlungen innerhalb Deutschlands oder der EU und des EWR.

Diese Mindestanforderungen betreffen quasi die 1. Stufe der Prüfung, welche die Unternehmen selbst durchzuführen haben und die nicht Gegenstand eines Genehmigungsverfahrens nach § 4c Abs. 2 BDSG ist. Die Aufsichtsbehörde muss nicht, kann aber gleichwohl prüfen, ob diese allgemeinen Voraussetzungen erfüllt sind. Steht fest, dass diese nicht erfüllt sind, ist für eine Genehmigung nach § 4c Abs. 2 BDSG kein Raum mehr (vgl. Innenministerium Baden-Württemberg, Hinweis Nr. 40, B.2.5).

Bei einer Beratungsanfrage, welche die Anforderungen des § 4c Abs. 2 BDSG bezüglich der Übermittlung von Biometriedaten der deutschen Mitarbeiter an die Muttergesellschaft in den USA betraf, wies die Aufsichtsbehörde daher auf diese vorrangige Prüfung hin. Zunächst ist anhand der §§ 28, 3a BDSG zu bewerten, ob die Verarbeitung und Übermittlung von Biometriedaten als solche gerechtfertigt ist. Grundsätzlich ist eine zentrale Speicherung von Biometriedaten problematisch. Biometriedaten sind teilweise als besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG einzustufen, da sie unter Umständen Rückschlüsse auf Krankheiten ermöglichen. Sie sollten, soweit sie beispielsweise für Zugangs-/Zugriffsregelungen verwendet werden, dezentral beim Arbeitnehmer auf einer mit einem Chip versehenen Karte (smart card) gespeichert werden. Eine zentrale Speicherung wäre dann weder in Deutschland noch in den USA erforderlich. Da aus der Anfrage weder das Unternehmen noch die genaueren Umstände der Datenverarbeitung ersichtlich waren, konnte die Aufsichtsbehörde die Angelegenheit nicht weiter verfolgen.

Eine andere Anfrage betraf die Erstellung eines konzernweit verfügbaren elektronischen Telekommunikationsverzeichnisses mit Namen der Mitarbeiter, dienstlicher Anschrift, Aufgabengebiet, dienstlicher Telefon- und Faxnummer sowie dienstlicher E-Mail-Adresse. Dies ist grundsätzlich als zuläs-

sig zu bewerten, denn es entspricht der legitimen Erwartung, eine ebenso schnelle wie reibungslose konzerninterne Kommunikation herzustellen (siehe Innenministerium Baden-Württemberg, Hinweis Nr. 34; Simitis, § 28 Rn. 195 zur Weitergabe firmeneigener Telefonbücher an konzernverbundene Unternehmen). Im Einzelfall kann eine Zugriffsbeschränkung auf Teile des Verzeichnisses geboten sein, soweit dies für die konzerninterne Kommunikation genügt.

Gegenstand einer weiteren Anfrage war die Datenübermittlung an ein Konzernunternehmen in den USA, welches ein zentrales Rechenzentrum betreibt. Dieses sollte lediglich die Datensicherung vornehmen und die EDV warten, aber keine eigenen Zugriffs- und Entscheidungsbefugnisse bezüglich der gespeicherten Mitarbeiterdaten haben, sondern insoweit vollständig an die Weisungen des deutschen Unternehmens gebunden sein. Da der Datenempfänger somit quasi als Auftragsdatenverarbeiter fungiert (innerhalb Deutschlands und der EU bzw. des EWR nach Maßgabe des § 11 BDSG zulässig), ist die Übermittlung grundsätzlich möglich, sofern die speziellen Anforderungen des Drittstaatentransfers erfüllt sind (siehe Nr. 7.2 und 7.3).

In allen anderen Fällen des konzernweiten Austauschs von Mitarbeiterdaten ist die Prüfung und Abwägung nach § 28 BDSG sehr schwierig.

In diesem Zusammenhang wurde die Aufsichtsbehörde häufig nach der Bedeutung von Betriebsvereinbarungen gefragt. Aufgrund ihres normativen Charakters stellen Konzern-, Gesamt- oder Betriebsvereinbarungen zwischen Arbeitgebern und Betriebsräten oder die diesen gleichstehenden Einigungsstellensprüche formal gesehenen Rechtsvorschriften im Sinne des § 4 Abs. 1 BDSG und damit Erlaubnisnormen für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten dar. Nach der Rechtsprechung des Bundesarbeitsgerichtes (BAG) können Betriebsvereinbarungen und der Spruch der Einigungsstelle auch zuungunsten der Arbeitnehmer von den Vorschriften des BDSG abweichen. Sie müssen sich aber im Rahmen der Regelungskompetenz der Betriebspartner halten und den Grundsätzen über den Persönlichkeitsschutz des Arbeitnehmers Rechnung tragen (BAG, BB 1986, S. 2333 betreffend Telefondatenerfassung).

In der Literatur wird überwiegend die Auffassung vertreten, dass Betriebsvereinbarungen vom BDSG solange abweichen dürfen, wie sie die dort getroffenen Regelungen durch Schutzverordnungen ersetzen, die den je spezifischen Beschäftigungsbedingungen besser angepasst, allerdings mindestens ebenso weitreichend sind. Der Schutz der informationellen Selbstbestimmung könne präzisiert und ausgebaut, nicht jedoch verdrängt werden (Simitis, § 28 Rn. 47; Ruppmann, Der konzerninterne Austausch personenbezogener Daten, Dissertation, S. 120, Nomos-Verlag, 1. Aufl. 2000).

Betriebsvereinbarungen, welche den Austausch von Mitarbeiterdaten zwischen Konzernunternehmen regeln, müssen daher zumindest folgende Anforderungen erfüllen (siehe Ruppmann, a.a.O.):

- Eindeutige Fixierung der zu erhebenden Datenkategorien und der als notwendig erachteten Verarbeitungsvorgänge; nicht ausreichend ist die Umschreibung der Aufgabe, zu deren Durchführung die konzernweite Personaldatenverarbeitung für erforderlich gehalten wird.
  Als unternehmensübergreifende Zwecke für die konzernweite Datenweitergabe kämen grundsätzlich in Betracht, Auslandsabordnungen, internationale Veranstaltungen, Jubiläen, Abwicklung von Leistungen an Mitarbeiter, Adressierung von Schreiben an Mitarbeiter sowie Mitarbeiterinformationen, Zugangsregelungen und sonstige Berechtigungen (z.B. Einfahrgenehmigungen), vorgesehene Personalbewegungen/-veränderungen sowie Bewerbungen zwischen Konzerngesellschaften, Führungskräfteentwicklung und -planung, Personalberichtswesen sowie Grundsatzfragen der Personalplanung und Leistungsübersichten.
- Regelung der Rechte der Arbeitnehmer (Widerspruchsrechte, Informationsrechte bzw. Verweis auf das BDSG),
- Regelung der Zugriffsberechtigungen und der Verantwortlichkeit für die ordnungsgemäße Verarbeitung der Personaldaten,
- Regelung der Mitwirkungs- und Überwachungsrechte des Betriebsrates,
- gleichartige Datenorganisation, um die einheitliche Umsetzung der unternehmensweiten Regelungen zu gewährleisten.

Bezüglich der speziellen Problematik des Drittstaatentransfers stellt sich die Frage, ob beim Abschluss einer Betriebsvereinbarung weitergehende Anforderungen, z.B. Genehmigung nach § 4c Abs. 2 BDSG, Safe Harbor-Unterwerfung etc., entfallen (vgl. Eul/Godefroid, RDV 1998, 185 [189] unter Hinweis auf Erwägungsgrund 9 und 22 der EG-DSRL).

Dem ist aber der begrenzte Geltungsbereich von Betriebsvereinbarungen entgegenzuhalten. Jedenfalls bei ausländischen Konzernen sind die außerhalb Deutschlands ansässigen Konzernmütter und -töchter nicht per se an die Betriebsvereinbarung gebunden.
Sinn und Zweck von Unternehmensregelungen/vertraglichen Regelungen im Sinne des § 4c Abs. 2 wäre dann gerade, die Betriebsvereinbarung für alle verbindlich zu machen (siehe den im 13. Tätigkeitsbericht vom 30. August 2000, LT-Drucks. 15/1539 Nr. 10.2 dargestellten Fall).

Allenfalls dann, wenn das, was die Betriebsvereinbarung regelt, an sich bereits nach § 28 Abs. 1 Nr. 1 BDSG zulässig ist, wäre der Erlaubnistatbestand des § 4c Abs. 1 Nr. 2 BDSG gegeben. Es dürfte jedoch gerade zweifelhaft sein, ob § 28 Abs. 1 Nr. 1 BDSG erfüllt ist.

Die Problematik des konzernweiten Austauschs von Mitarbeiterdaten wird die Aufsichtsbehörden wohl auch in Zukunft beschäftigen.

Zweckmäßig wären konkrete Regelungen in dem auf Bundesebene beabsichtigten Arbeitnehmerdatenschutzgesetz.

### 7.5 Auftragsdatenverarbeitung innerhalb der EU und des EWR

Nicht nur hinsichtlich des Datentransfers in Drittstaaten bestehen rechtliche Unsicherheiten, sondern auch hinsichtlich des Datenaustauschs und der Datenverarbeitung innerhalb der EU und des EWR. Dabei geht es insbesondere um die Frage, welches nationale Recht anwendbar ist.

Es wurde beispielsweise gefragt, welches Recht gelte, wenn ein in Deutschland ansässiges Unternehmen als Auftragsdatenverarbeiter für ein in Frankreich ansässiges Unternehmen in Deutschland tätig wird.
Oder welches Recht anwendbar ist, wenn ein in den Niederlanden ansässiges Unternehmen seine Kundendaten in seiner deutschen Niederlassung verarbeiten lässt, wobei aber die deutsche Niederlassung ausschließlich als weisungsgebundenes Rechenzentrum fungiert und somit als Auftragsdatenverarbeiter tätig ist?

Nach § 1 Abs. 5 Satz 1 BDSG findet das BDSG keine Anwendung, wenn eine in einem anderen EU- oder EWR-Staat belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland.
Grundsätzlich ist also der Sitz der verantwortlichen Stelle maßgeblich, wo die Datenverarbeitung tatsächlich erfolgt, ist danach unerheblich (Sitzlandprinzip). Wenn jedoch eine inländische Niederlassung besteht, gilt das BDSG, sofern die konkrete Datenerhebung, -verarbeitung oder Nutzung von dieser ausgeht bzw. in dieser erfolgt (Territorialprinzip bzw. abgeschwächtes Sitzlandprinzip).

Der Fall der Auftragsdatenverarbeitung ist in § 1 Abs. 5 BDSG nicht gesondert geregelt. Hier sind allerdings die Wertungen der §§ 3 Abs. 8 Satz 3 und 11 BDSG zu beachten, wonach auch ein im europäischen Ausland ansässiger Auftragsdatenverarbeiter nicht als Dritter anzusehen ist, sondern der Auftraggeber für die Einhaltung der Datenschutzvorschriften verantwortlich ist. Bezüglich des umgekehrten Falles, dass ein inländischer Auftragnehmer für einen im europäischen Ausland ansässigen Auftraggeber tätig ist, kann aufgrund der Vorgaben in Art. 17 Abs. 2 und 3 sowie Art. 2e EG-DSRL davon ausgegangen werden, dass in den anderen EU- und EWR-Staaten entsprechende Vorschriften bestehen bzw. diese müssten notfalls richtlinienkonform so ausgelegt werden.

Da also der Auftraggeber verantwortliche Stelle ist, d.h. der weisungsgebundene Auftragnehmer keine eigene Verfügungs-/Entscheidungsbefugnis über die Daten hat, muss das Recht des Landes, das für den Auftraggeber gilt, maßgeblich bleiben. Dabei kann es keinen Unterschied machen, ob als Auftragnehmer ein fremdes Unternehmen oder eine eigene Niederlassung tätig

ist, entscheidend sind die Funktion und die entsprechende Ausgestaltung des Auftragsverhältnisses.

Folglich sind in den eingangs genannten Fällen nicht die §§ 4, 27 ff. BDSG anwendbar, sondern die Zulässigkeit der Datenverarbeitung als solcher beurteilt sich nach französischem bzw. niederländischem Recht.

Umgekehrt ist davon auszugehen, dass ein hier ansässiges Unternehmen sich eines britischen, französischen etc. Auftragsdatenverarbeiters bedienen kann und dabei weiterhin das BDSG bezüglich der Zulässigkeit der Verarbeitung als solcher gilt.

Bezüglich der technisch-organisatorischen Maßnahmen zur Datensicherheit allerdings ist Art. 17 Abs. 3 2. Spiegelstrich EG-DSRL zu beachten. Danach ist der Auftragsdatenverarbeiter zur Beachtung der erforderlichen technisch-organisatorischen Maßnahmen zu verpflichten, und zwar nach Maßgabe der Rechtsvorschriften des Landes, in dem er seinen Sitz hat. Damit soll bewirkt werden, dass ein Auftragsdatenverarbeiter, der für Verantwortliche in verschiedenen Mitgliedstaaten Aufträge erledigt, nicht mit den rechtlichen Anforderungen aller dieser Mitgliedstaaten konfrontiert wird, sondern sich, nicht zuletzt im Hinblick auf die erfolgte Harmonisierung, allein auf die Beachtung des entsprechend seinem Sitz anwendbaren nationalen Rechts konzentrieren kann (Dammann/Simitis, Kommentar zur EG-DSRL, Art. 17 Rn. 14).

Diese Vorgabe entspricht § 11 Abs. 4 BDSG, denn danach gilt für den Auftraggeber ausnahmslos § 9 BDSG. Eine Unterscheidung danach, ob der Auftragnehmer für inländische oder ausländische Auftraggeber tätig wird, ist nicht vorgesehen.

Im Ergebnis ist also die Frage nach dem anwendbaren Recht entsprechend der im BDSG vorgekommenen Verteilung der rechtlichen Verpflichtungen zwischen Auftraggeber und Auftragnehmer zu beantworten.

### 7.6 Anwendbarkeit deutschen Rechts auf US-Websites

Schwieriger noch als bei Datenverarbeitungen innerhalb der EU und des EWR ist die Frage nach dem anwendbaren Recht bei solchen Datenverarbeitungen zu bewerten, welche im Zusammenhang mit außereuropäischen Websites erfolgen.

Das BDSG findet nach § 1 Abs. 5 Satz 2 BDSG Anwendung, sofern eine verantwortliche Stelle, die weder in der EU noch im EWR belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Damit gilt das Territorialitätsprinzip. Maßgeblich ist also der Ort der Datenverarbeitung.

In der vernetzten Welt des Internet lässt sich jedoch oft nur sehr schwer lokalisieren, wo denn nun die maßgebliche Tätigkeit erfolgt.

Exemplarisch seien zwei von vielen Fallgestaltungen genannt, zu denen das Regierungspräsidium Darmstadt von den Unternehmen bzw. deren Bevollmächtigten um Beratung gebeten wurde.

In einem Fall handelte es sich um ein US-Unternehmen mit einer deutschen Tochtergesellschaft. Das US-Mutterunternehmen beabsichtigte, eine Website in deutscher Sprache zu errichten, um Kunden in Deutschland die Bestellung von Waren zu ermöglichen. Die Website sollte also ein elektronisches Bestellformular enthalten. Sie sollte unter einer ".de"-Domain betrieben, jedoch in den USA von einem Unternehmen gehostet werden, das auch die Server für die US-Muttergesellschaft betreibt. Demzufolge sollten die Daten in die USA unter der Kontrolle der US-Mutter verarbeitet und aufbereitet werden.
Die deutsche Tochtergesellschaft sollte die Bestellungen deutscher Kunden ausführen. Zu diesem Zweck sollte sie die Daten in den USA abrufen und in ein Bestellungssystem in Deutschland eingeben. Sodann sollten die Produkte direkt von der deutschen Tochter an die Kunden ausgeliefert werden.

In einem anderen Fall stellt ein US-Unternehmen ein Computerspiel her. Dieses wird weltweit als CD-ROM vertrieben. Der Vertrieb in Deutschland erfolgt über ein deutsches Unternehmen, welches zwar keine Tochtergesellschaft ist, aber zum selben Konzern gehört. Die CD-ROM enthält die deut-

sche Fassung des Spiels. Das Spiel kann jeder Spieler für sich allein an seinem PC spielen (offline). Er hat aber auch die Möglichkeit, sich auf der Website des US-Unternehmens zu registrieren und dann das Spiel mit und gegen andere Spieler im World Wide Web zu spielen (online). Das deutsche Unternehmen unterstützt deutsche Spieler bei technischen Problemen.

In beiden Fällen stellte sich zunächst die Frage, ob die unmittelbar im Zusammenhang mit der US-Website erfolgende Datenerhebung und –verarbeitung dem deutschen Unternehmen zuzurechnen und dieses also als Anbieter des Tele- bzw. Mediendienstes anzusehen sei. Bezüglich der im Zusammenhang mit der Auslieferung der Ware bzw. des CD-Verkaufs erfolgenden Verarbeitung in Deutschland sind die deutschen Unternehmen selbstverständlich verantwortlich.

Dies wäre zu bejahen, wenn ein Unternehmen die Akquisition neuer deutscher Kunden betreibt, an der Verwaltung der Nutzerdaten mitwirkt und die deutschsprachigen Inhalte des Dienstes redaktionell zu verantworten hat (siehe 17. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten, S. 30, 31). Gerade Letzteres verneinten die Unternehmensvertreter jedoch in den geschilderten Fällen.

Trotz des engen Zusammenwirkens mit den US-Unternehmen in einem einheitlichen wirtschaftlichen Gesamtkonzept ist es problematisch anzunehmen, dass die Datenverarbeitung im Zusammenhang mit den US-Websites im Rahmen der Tätigkeit der deutschen Unternehmen erfolge.

Bei der gebotenen richtlinienkonformen Auslegung ist Art. 4 Abs. 1c EG-DSRL zu beachten. Danach hat jeder Mitgliedstaat sein nationales Datenschutzrecht auf alle Verarbeitungen, nach Art. 2b EG-DSRL auch auf Erhebungen, Nutzungen etc., personenbezogener Daten anzuwenden, die von einem für die Verarbeitung Verantwortlichen ausgeführt werden, der nicht im Gebiet der Gemeinschaft niedergelassen ist und zum Zweck der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaates belegen sind, es sei denn, dass diese Mittel nur zum Zweck der Durchfuhr durch das Gebiet der Europäischen Gemeinschaft verwendet werden.

Ein Rückgriff auf derartige Mittel läge zweifellos vor, wenn die Website in Deutschland gehostet würde oder Einwahlknoten genutzt werden, was aber in den Beispielen nicht der Fall war.

Bei einer bloßen Datenerhebung mittels Website-Formular liegt die Schwierigkeit darin, dass die Erhebung quasi mit der Bereitstellung des Formulars im Internet beginnt und erst mit dessen Ausfüllung durch den Nutzer beendet ist. Problematisch ist auch, ob der PC des Nutzers ein "Mittel" im Sinne des Art. 4 Abs. 1c) EG-DSRL ist. Ein solches liegt grundsätzlich nur vor, wenn es von der verantwortlichen Stelle beherrscht wird.

Die Problematik wird von der Gruppe nach Art. 29 EG-DSRL bzw. zunächst von einer eigens hierfür gebildeten Untergruppe behandelt.

Bei Redaktionsschluss dieses Tätigkeitsberichts war nur insoweit Einigkeit erzielt, dass bei Verwendung von Cookies, Javascript und vergleichbarer Software sowie dem Einsatz von Viren, Würmern und Trojanischen Pferden deutsches Recht bzw. das Recht der anderen EU-/EWR-Staaten gilt. Typischerweise ist der Nutzer hier Objekt einer Datenverarbeitung, die er nicht selbst steuert.

Da in den oben genannten Beispielfällen laut Auskunft der Bevollmächtigten zumindest Cookies gesetzt werden sollten bzw. dies aufgrund der Allgemeinen Geschäftsbedingungen des US-Spieleherstellers anzunehmen war, wies die Aufsichtsbehörde die Unternehmen auch darauf hin, dass von der Geltung deutschen Datenschutzrechts auszugehen sei.

Die Unternehmen können sich dem nicht schon dadurch entziehen, indem sie lediglich einen Hinweis auf die Konfigurationsmöglichkeit des Browsers in die Website aufnehmen. Nur wenn das Angebot so gestaltet wird, dass der Nutzer die Verarbeitung insgesamt selbst steuert, gilt etwas anderes.

## 8. Neue Medien, Internet-Provider

### 8.1 Auskunftei und Prangerseiten im Internet

Mehrere Unternehmen planten das Angebot von Auskünften über das Internet und baten die Aufsichtsbehörde um Beratung zu dieser Geschäftsidee.

Die konkreten Zwecke waren unterschiedlich.
In einem Fall sollten Unternehmen vor potenziellen Kunden mit schlechter Zahlungsmoral, im anderen sollten Kunden vor betrügerischen Handwerkern gewarnt werden.

Die Anfrager schlugen selbst mehrere Varianten vor. Die Möglichkeit, Negativauskünfte jedermann über das Internet zur Verfügung zu stellen, wurde von der Aufsichtsbehörde von vornherein verworfen, da hierbei regelmäßig schutzwürdige Belange der betroffenen angeprangerten Personen verletzt worden wären (vgl. Oberlandesgericht Rostock, Urteil vom 21. März 2002 - 2 U 55/00; Jahresbericht BlnBDI für 2001, Nr. 4.6.4; Tätigkeitsbericht des ULD SH 2002, Nr. 6.27).
Wenn überhaupt, kam deshalb nur eine geschlossene Benutzergruppe - hier für Kunden der Internetauskunftei - infrage.
An die Internetauskunftei sind die gleichen Maßstäbe anzulegen, wie an eine der etablierten Wirtschaftsauskunfteien.

Entgegen den Planungen der Anfrager ist es rechtlich nicht zulässig und möglich, einfach eine Plattform für die "Warnmeldungen" anzubieten und die Verantwortung auf den Einmelder der Daten zu delegieren.
Die "Auskunfteienlösung" ist daher nur realisierbar, wenn ein Unternehmen als Auskunftei verantwortliche Stelle ist. Lediglich im Innenverhältnis könnte die Auskunftei unter Umständen für Falschmeldungen etc. einen Regress vereinbaren.
Die Auskunftei bleibt damit nach 7 BDSG zum Schadenersatz verpflichtet.

Die Auskunftei muss nach

§ 33 Abs. 1 Satz 2 BDSG den Betroffenen nach der erstmaligen Übermittlung seiner Daten benachrichtigen,

§ 34 BDSG Auskunft an den Betroffenen erteilen,

§ 35 BDSG Berichtigung, Löschung und Sperrung der Daten vornehmen,

§ 29 Abs. 2 Nr. 1a BDSG das berechtigte Interesse des Empfängers und die glaubhafte Darlegung aufzeichnen.

Vor allem aber muss vor der Übermittlung sichergestellt werden, dass die betroffene Person kein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Die schutzwürdigen Interessen der Betroffenen wären jedenfalls verletzt, wenn keine eindeutigen, bewiesenen Fakten, sondern Behauptungen und subjektive Einschätzungen übermittelt würden. Grundsätzlich dürfen nur so genannte harte Negativmerkmale wie Zwangsvollstreckung, Abgabe einer eidesstattlichen Versicherung etc. übermittelt werden.

Mit stichprobenweisen Kontrollen muss die Auskunftei bei den Anfragern nachprüfen, ob das behauptete berechtigte Interesse, in der Regel die beabsichtigte Eingehung einer Geschäftsbeziehung mit Vorleistung, auch tatsächlich gegeben war.

Als die potenziellen Internetauskunfteien mit diesen Pflichten konfrontiert wurden, verzichteten sie auf die Umsetzung der Auskunfteienpläne.
Weitere Pflichten nach § 4d BDSG (Meldung bei der Aufsichtsbehörde) und § 9 BDSG (technische und organisatorische Maßnahmen) wurden deshalb nicht mehr erörtert.

### 8.2 Die Suche nach Personen im Internet

Ein Softwareunternehmen hat eine spezielle Technologie entwickelt, mit der Bilder auf ihre Inhalte analysiert und erkannt werden können. Der primäre Geschäftszweck des Unternehmens besteht darin, mithilfe dieser Technologie Marken- und Wettbewerbsrechtsverletzungen aufzuspüren.
Das Internet wird zu diesem Zweck ständig nach Bildern durchforscht, welche in einem Datenpool gespeichert werden, um sie danach auszuwerten, ob

beispielsweise ein geschütztes Produktlogo oder -design widerrechtlich von Konkurrenten des jeweiligen Rechteinhabers genutzt wird.

Daneben setzt das Unternehmen die Technologie in Zusammenarbeit mit verschiedenen gemeinnützigen Organisationen in einem Projekt zur Suche nach vermissten Kindern ein. Die Technologie ist in der Lage, selbst dann Bildmaterial von Personen aus dem Internet aufzuspüren, wenn dieses mit dem vorliegenden Vergleichsfoto nicht identisch ist.
Aufgrund der starken Medienpräsenz erhielt das Unternehmen mehr und mehr Anfragen von Privatleuten, die diesen Service auch für private Suchen nützen möchten, z.B. für die Suche nach alten Bekanntschaften, ehemaligen Partnern, die den Kontakt abgebrochen haben, "entlaufenen" Ehepartnern und Angehörigen.
Das Unternehmen lehnte dies ab, bat jedoch schließlich - wegen des steigenden Nachfragedruckes - die Aufsichtsbehörde um eine Bewertung. Diese konnte das Unternehmen in seinen datenschutzrechtlichen Bedenken nur bestärken.

Für die private Suche nach Personen in dem für den primären Geschäftszweck gebildeten Bild-Datenpool wäre zwar möglicherweise eine gesonderte Erhebung für den neuen Zweck entfallen, es läge jedoch eine Zweckänderung vor. Die anderweitige Nutzung bzw. Übermittlung von personenbezogenen Daten, die beim Abgleich anfallen, wäre datenschutzrechtlich nur erlaubt, wenn die Voraussetzungen des § 29 Abs. 2 Nr. 1a und 2 BDSG erfüllt wären, denn die Datenverarbeitung erfolgt ausschließlich zum Zwecke der Übermittlung an die Suchenden.

Eine Übermittlung der personenbezogenen Daten im Rahmen dieser Vorschrift ist nur erlaubt, wenn der Suchende glaubhaft ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten dargelegt hat und in Abwägung dazu kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Die Überprüfung eines objektiv berechtigten Interesses hätte das Unternehmen in vielen Fällen vor kaum zu lösende Probleme gestellt, wenn nicht Notstandssituationen, wie z.B. die Suche nach vermissten Kindern, oder gerichtliche Zahlungstitel (relevant bei der Suche nach Schuldnern) vorliegen, durch die das berechtigte Interesse amtlich bestätigt wird.
Die wahren Motive der Suchenden wären, anders als bei Wirtschaftsauskunfteien, nur schwer feststellbar.

Darüber hinaus ist fraglich, ab wann überhaupt von einem "berechtigten" Interesse gesprochen werden kann. Es sind umso höhere Anforderungen zu stellen, je gewichtiger die möglicherweise beeinträchtigten schutzwürdigen Belange der betroffenen Personen sind.

Abgesehen davon, dass die betroffenen Personen möglicherweise sehr gute persönliche Gründe haben, warum sie gerade von dem Sucher nicht gefunden werden wollen, stehen vor allem schutzwürdige Belange der gesuchten Personen grundsätzlich schon dann entgegen, wenn diese Personen nicht erkennbar selbst an der Veröffentlichung ihrer Bilddaten im Internet interessiert sind.

Schutzwürdige Interessen sind nämlich auch dann anzunehmen, wenn zweifelhaft ist, ob die §§ 22, 23 Kunsturhebergesetz verletzt sind. Nach diesen Vorschriften dürfen Bilder von Personen grundsätzlich nur mit deren Einwilligung verbreitet werden. Die Feststellung, ob die Bilder mit dem Einverständnis oder zumindest im tatsächlichen Interesse der Betroffenen ins Internet gestellt wurden, dürfte für das Unternehmen kaum möglich sein, soweit die Bilder nicht offensichtlich vom Betroffenen auf der eigenen Homepage veröffentlicht wurden.
Oftmals werden Bilder unbedacht ohne das Einverständnis der Betroffenen ins Internet gestellt, oftmals sogar in bewusst böser Absicht, wie auf so genannten "Racheseiten", die ein Forum für Beleidigungen und Denunziationen im Internet bilden.

Würde man die weitere Nutzung und Übermittlung von Bilddaten, welche unter Verstoß gegen das Kunsturhebergesetz ins Internet gestellt wurden, ohne weiteres zulassen, würde die Verletzung des Kunsturhebergesetzes und damit des Persönlichkeitsrechts der Betroffenen perpetuiert.

Die gesetzlich gebotene Abwägung führt dazu, dass beispielsweise das bloße Interesse, einen ehemaligen Bekannten wiederzufinden, keinesfalls rechtfertigt, Bilddaten auszuwerten und weiterzugeben, die der Betroffene nicht selbst veröffentlicht hat und deren Veröffentlichung auch nicht zweifelsfrei in seinem Interesse geschah.

Die Weitergabe solcher Bilddaten kommt also nur in Betracht, wenn besonders gewichtige, nachprüfbare Interessen des Suchenden vorliegen.

Aufgrund dieser Bewertung bekundete das Unternehmen, die bisherige Praxis beizubehalten, d.h. nach vermissten Personen nur zu suchen, wenn der Suchauftrag von der Polizei oder von einer gemeinnützigen Organisation vorgelegt wurde, welche das Anliegen des Suchenden zuvor sorgfältiger Prüfung unterzogen hat.

### 8.3 Elektronische Spiele

Elektronische Spiele erfreuen sich großer Beliebtheit, besonders jene, die man nicht nur allein an seinem PC, sondern über das Internet mit und gegen andere spielen kann.
Die Änderung der Nutzungsbedingungen für die Online-Spielplattform eines solchen Spieles löste in der "Spielergemeinde" eine Protestwelle aus, da die vollständige Überwachung des Spielverhaltens und die Weitergabe von Daten zu befürchten waren.

Das Spiel wird von einem hier ansässigen, aber zu einem US-Konzern gehörigen Unternehmen als CD vertrieben. Die Online-Plattform wird von der US-Konzernmutter betrieben, das deutsche Tochterunternehmen betreut jedoch die Spieler bei technischen Fragen und Problemen. Neben zahlreichen Spielern wandte sich auch dieses deutsche Tochterunternehmen an die Aufsichtsbehörde und bat um Beratung.
Da die Datenverarbeitung in den USA erfolgt, ist problematisch, ob überhaupt deutsches Recht anwendbar ist (siehe Nr. 7.6).

Geht man von der Anwendbarkeit deutschen Rechts aus, waren die Nutzungsbedingungen in einigen Punkten zu kritisieren.

Die Benutzerregeln informierten darüber, dass die Registrierungsdaten an andere Unternehmen weitergegeben werden, räumt den Nutzern jedoch ein Widerspruchsrecht hiergegen ein. Nach dem Teledienstedatenschutzgesetz (TDDSG) ist die Weitergabe der Registrierungsdaten jedoch nur mit vorheriger ausdrücklicher Einwilligung des Nutzers möglich. Dabei spielt es keine Rolle, dass - wie das Unternehmen mitteilte - die Registrierung gar nicht unter dem Realnamen erfolgen müsse, sondern ein selbstgewähltes Pseudonym genüge. Das Unternehmen muss damit rechnen, dass Realnamen angegeben werden, zumal auf die Alternative nicht hingewiesen wurde.

Die geforderte allgemeine Bestätigung der Nutzungsbedingungen erfüllt nicht die Voraussetzungen an eine wirksame Einwilligung, denn sie ist nicht ausreichend hervorgehoben und es besteht keine Wahlfreiheit für den Nutzer.
Das US-Unternehmen versicherte jedoch, dass überhaupt keine Registrierungsdaten deutscher Nutzer an andere Unternehmen weitergegeben werden.

Eine weitere Bestimmung in den Benutzerregeln sah die Erhebung von Identifizierungsinformationen und umfangreichen Daten über das Nutzungsverhalten der Spieler vor. Daten, bei denen der Nutzer bestimmt werden kann, dürfen nach dem TDDSG jedoch nur mit Einwilligung des Nutzers oder aufgrund einer gesetzlichen Erlaubnis erhoben, verarbeitet oder genutzt werden.

Eine wirksame Einwilligung wurde aber nicht eingeholt (siehe oben) Eine gesetzliche Erlaubnis besteht in Bezug auf Nutzungsdaten grundsätzlich nur, wenn die Erhebung der Daten erforderlich ist, um die Inanspruchnahme des Dienstes (hier des Spieles) oder dessen Abrechnung zu ermöglichen.

Die am 21. Dezember 2001 in Kraft getretene Novelle des TDDSG erlaubt es dem Diensteanbieter darüber hinaus, Daten zu erheben, um sich gegen schädigende Handlungen durch Nutzer zu wehren (§ 6 Abs. 8 TDDSG). Die gesetzlichen Voraussetzungen hierfür sind allerdings sehr streng. Der Erlaubnistatbestand gilt - entgegen der ursprünglich weiteren Fassung in den vorangegangenen Gesetzesentwürfen - nur, wenn der Nutzer versucht, das

Entgelt nicht oder nicht vollständig zu entrichten. Inwieweit das Vorgehen eines Diensteanbieters gegen sonstige Missbrauchsfälle nach § 6 Abs. 1 TDDSG als erforderlich angesehen werden kann, "um die Inanspruchnahme von Telediensten zu ermöglichen", wäre im konkreten Einzelfall zu prüfen. In akuten Verdachtsfällen, in denen der Missbrauch eines Spielers die Teilnahme der anderen Nutzer am Spiel erheblich beeinträchtigt, könnte dies gerechtfertigt sein.

Die Daten müssten gelöscht werden, sobald sie für diesen Zweck, d.h. Vorgehen gegen den Nutzer, welcher den Missbrauch begangen hat, nicht mehr benötigt werden. Pauschale Vorratsdatenerhebungen wären durch die oben genannten gesetzlichen Erlaubnistatbestände nicht gedeckt.

Das US-Unternehmen versicherte jedoch, dass solche nicht erfolgen und das "lokale" Recht stets beachtet würde. Leider wurden die Benutzerregeln aber bis heute nicht an die eigenen Verlautbarungen des Unternehmens angepasst.

Anhaltspunkte für tatsächliche Verstöße, d.h. dass unzulässige Datenerhebungen erfolgen, liegen jedoch nicht vor. Da die Aufsichtsbehörde keine Prüfmöglichkeiten in den USA hat, kann freilich keine definitive Aussage getroffen werden.
Jeder Nutzer sollte sich dessen bewusst sein und muss selbst entscheiden, ob er unter diesen Umständen die Online-Spielmöglichkeit nutzt. Selbst wenn man nach § 1 Abs. 5 Satz 2 BDSG die Anwendbarkeit deutschen Rechts für Angebote auf US-Websites bejaht, besagt dies noch nicht, dass die tatsächliche Umsetzung des deutschen Rechts gewährleistet wäre.

### 8.4 Recht auf pseudonyme Inanspruchnahme von Telediensten

Zu den datenschutzrechtlichen Pflichten der Anbieter von Telediensten gehört es nach § 4 Abs. 6 TDDSG, dem Nutzer die Inanspruchnahme von Telediensten anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist.

Durch die Eingabe eines Betroffenen wurde die Datenschutzaufsichtsbehörde auf eine besondere Konstellation bei einem großen Internet-Provider mit Sitz in Südhessen aufmerksam. Bei einem Teil seiner Kunden wurde diese gesetzlich vorgeschriebene und üblicherweise auch vorhandene Pseudonymität bei der Nutzung der Dienste "E-Mail" und "News" nicht mehr gewahrt.

Der Provider bietet seinen Kunden eine Vielzahl unterschiedlicher Internet-Dienstleistungen, unter anderem E-Mail-Adressen, Newsgroups und auch eigene private Homepages als Sub-Domains im WWW an. Die private Homepage eines jeden Kunden trägt nach den geltenden AGB und in Übereinstimmung mit den Vorschriften zur Anbieterkennzeichnungspflicht nach dem Teledienstegesetz und dem Mediendienstestaatsvertrag (MDStV) ein Impressum mit Name und Postanschrift des Provider-Kunden. Diese Homepages sind immer auch über die Angabe einer individuellen Kundenummer in der Browserzeile zu erreichen. Der Provider fügt nun aus praktischen Gründen (in Bezug auf sein EDV-System) diese Kundennummer automatisch dem Header einer jeden E-Mail und eines jeden Newsgroup-Beitrages des jeweiligen Kunden in einer so genannten zusätzlichen "X-Sender-Zeile" bei. Das wäre an sich kein Problem, denn diese Nummer ist immer auch Bestandteil der originären E-Mail-Adresse und somit nicht geheim. Wer nicht gleichzeitig eine Homepage bei diesem Provider betreibt, bleibt mit seiner E-Mail-Adresse durchaus trotz zugefügter "X-Sender-Zeile" weiter pseudonym, d.h. für Dritte nicht bestimmbar.

Für die vielen privaten Homepage-Kunden dieses Providers bedeutet der Zusatz der Kundennummer in der X-Sender-Zeile aber, dass sie weltweit z.B. nach jedem Newsgroup-Beitrag über das - an sich ebenfalls zulässige - Impressum ihrer Homepage vollständig identifiziert werden können, selbst wenn sie hierfür absichtlich eine zweite E-Mail-Adresse benutzen, da die X-Sender-Zeile immer gleich bleibt. Gerade in internationalen, aber auch deutschen Newsgroups, in denen oft heftige und auch emotionale oder politische Diskussionen weitgehend anonym ausgetragen werden, und viele für die anonyme Nutzung vorgesehene Beratungs- und Hilfeangebote zu finden sind, ist eine, wenn nicht vollständig anonyme, dann doch zumindest gegenüber den anderen Teilnehmern pseudonyme Nutzungsmöglichkeit im Sinne des § 4 Abs. 6 TDDSG unabdingbar.

Der Provider wurde daher unter Hinweis auf das gesetzliche Gebot zur Ermöglichung der pseudonymen Kommunikation aufgefordert, die privaten Kunden-Homepages und die Dienste "E-Mail" und "Newsgroups" zu entkoppeln. Er war jedoch zunächst der Auffassung, dass die Umsetzung dieser Forderung technisch nicht möglich bzw. zumutbar im Sinne des Gesetzes sei. Nachdem einige Überzeugungsarbeit durch die Aufsichtsbehörde geleistet wurde, liegt inzwischen die Zusage des Unternehmens vor, diese dort historisch gewachsene und programmtechnisch bedingte Verknüpfung der genannten Dienste mit der Homepage aufzuheben. Zum Zeitpunkt der Berichterstellung waren diese Zusagen allerdings noch nicht umgesetzt, erfreulicherweise wurden jedoch zumindest erste Maßnahmen zur Abhilfe getroffen.

### 8.5 Unzulässige umfangreiche Datenerhebung auf einer WWW-Seite

Eine Kundin wies die Datenschutzaufsichtsbehörde auf die WWW-Seiten eines Unternehmens hin, das Zubehör und Geräte für den Sport- und Fitnessbereich herstellt und über Sanitätshäuser und Kaufhäuser vertreibt. Auf einer WWW-Seite unter der Homepage des Unternehmens konnten sich Käuferinnen und Käufer des Produkts registrieren lassen. Für die Registrierung wurden neben den Daten des gekauften Produkts und Name und Anschrift der Kunden auch noch das genaue Geburtsdatum, die E-Mail-Adresse, die Telefonnummer, der Beruf und die Krankenkasse sowie einige andere persönliche Daten als erforderliche Pflichtangaben abgefragt. Ohne diese Felder komplett auszufüllen, konnte die Online-Registrierung nicht durchgeführt werden. Auf Beschwerden der Kundin über diese übermäßige Datenerhebung, die kaum nur der Produktregistrierung zu Gewährleistungs- und Garantiezwecken dienen konnte, hatte das Unternehmen einfach nicht reagiert.

Die Datenerhebungsseiten des Betriebes im WWW fielen zunächst durch bemerkenswerte Intransparenz und damit Verbraucherunfreundlichkeit auf. Zum eigentlichen Zweck der umfassenden Datenerhebung durch den Teleddiensteanbieter auf der Produktregistrierungsseite waren entgegen § 4 Abs. 3 Nr. 2 BDSG und entgegen § 3 Abs. 5 der im Berichtsjahr noch geltenden Fassung des Teledienstedatenschutzgesetzes (TDDSG) keine Angaben zu finden, ebenso wenig waren die weiteren notwendigen Unterrichtungen oder Datenschutzhinweise auf der Homepage des Unternehmens vorhanden. Je nach Zweckbestimmung wäre zu bewerten gewesen, welche Daten hierfür überhaupt benötigt werden. Daten, die für den entsprechenden Zweck nicht erforderlich sind, dies dürfte zumindest bezüglich der Angaben zu Telefonnummer, Beruf und Krankenkasse der Fall sein, dürfen nur mit Einwilligung der Betroffenen erhoben werden (§§ 3, 5 TDDSG). Soweit die "Inhaltsebene" betroffen ist, müssten die Angaben jedenfalls als "freiwillig" gekennzeichnet und unter Hinweis auf das Widerspruchsrecht nach § 28 Abs. 4 BDSG, bei beabsichtigter werblicher Nutzung, behandelt werden (§ 4 Abs. 3 BDSG). All dies war nicht beachtet. Zusätzlich war zu beanstanden, dass die nach § 6 Teledienstegesetz a.F. (TDG) erforderliche Anbieterkennzeichnung des Unternehmens unvollständig war, da unter anderem der Name des Geschäftsführers der im Handelsregister eingetragenen GmbH fehlte.

Beim Gespräch mit dem Unternehmen stellte sich heraus, dass die Erstellung der WWW-Seiten von einer externen Web-Design-Agentur durchgeführt worden war und weder bei dem Unternehmen selbst noch bei der beteiligten Web-Agentur irgendwelche datenschutzrechtliche Kenntnisse vorhanden waren. Man hatte sich ganz einfach keinerlei Gedanken darüber gemacht, wie die Verbraucherinnen und Verbraucher unterrichtet werden müssen und welche Daten ein Unternehmen erheben darf bzw. für welche Datenerhebungen und Verwendungszwecke es einer ausdrücklichen Einwilligung der Betroffenen nach dem TDDSG bedarf. Selbst zum Zweck der umfangreichen Datenerhebung und damit zur geplanten anschließenden Verwendung dieser Daten konnte keine schlüssige Erklärung gegeben werden.

Nach den Hinweisen der Datenschutzaufsichtsbehörde hat das Unternehmen die beanstandete Produktregistrierungsseite aus dem WWW genommen. Die bereits erhobenen Kundendaten wurden gelöscht. Die beanstandete Anbieterkennzeichnung wurde gesetzeskonform ergänzt und beinhaltet nun auch den Namen des Geschäftsführers, die Handelsregisternummer sowie die Umsatzsteueridentifikationsnummer, wie es das seit Dezember 2001 novellierte TDG verlangt.

### 8.6 Alles nur Marketing? - Unzulässige Geschäftspraktiken zur Gewinnung von Internet-Kunden

In den Krisenzeiten der Internet-Wirtschaft wird offensichtlich mit immer härteren Bandagen um die verbliebenen Neukunden und weiteren potenziellen Internet-Surfer gekämpft. Dies betrifft auch das Geschäft der vielen Internet-Zugangsprovider, die neue Kunden gerne mit Vertrag möglichst langfristig an sich binden möchten.

Dies mussten im Berichtsjahr mehrere Beschwerdeführer erfahren, die sich an das Regierungspräsidium Darmstadt wandten, weil sie Rechnungen für Internet-Verträge von Internet-Zugangsprovidern erhalten hatten, von denen die Petenten angaben, dass sie diese nie abgeschlossen und unterschrieben hätten. Alle Beschwerdeführer wandten sich zunächst selbst mit Briefen und Telefaxen an die betroffenen Internet-Provider mit der Bitte um Auskunft nach § 34 Abs. 1 BDSG nach dem Umfang und der Herkunft der bei den Internet-Zugangsprovidern gespeicherten Daten, um die Vorfälle aufklären zu können. Als Reaktion auf diese Datenschutz-Anfragen gingen jedoch nur weitere Rechnungen, zumindest in Höhe der nutzungsunabhängigen Grundgebühr, bei den Betroffenen ein. Da keiner der Petenten innerhalb mehrerer Monate auch nur eine Antwort von einem Provider erhielt, wandten sich alle Betroffenen an die Datenschutzaufsichtsbehörde mit der Bitte, ihnen bei der Durchsetzung ihres Rechtes auf Auskunft über Umfang und Herkunft der gespeicherten Vertragsdaten behilflich zu sein.

Den Beschwerden der Petenten wurde nach der Einschaltung der Aufsichtsbehörde im Wesentlichen entsprochen. Die Rechnungsbeträge wurden von den Internet-Providern storniert und der Rechnungsversand eingestellt. In keinem der Fälle konnte die Herkunft der zumindest für den Rechnungsversand gespeicherten Daten von der Datenschutzaufsichtsbehörde vollständig aufgeklärt werden. Ein von einem Kunden unterschriebener Vertrag konnte von den Providern auch nicht vorgelegt werden. Als Erklärung für diese eigenartigen Sachverhalte dienten häufig Übermittlungsfehler, aber auch menschliches Versagen oder Fehlverhalten von Mitarbeitern bei Subunternehmen oder in Verkaufs- und Service-Stellen, die mit der Durchführung von "Sonder-Aktionen zur Neukundengewinnung" beauftragt worden seien. Auf Nachfrage stellte sich dann oft heraus, dass der jeweilige Mitarbeiter inzwischen entlassen worden sei oder dass der Provider seine Geschäftsbeziehung mit dem beauftragten Marketing-Unternehmen zwischenzeitlich eingestellt habe.

Die Nichterteilung der nach § 34 Abs. 1 BDSG angeforderten Auskunft an die Betroffenen wurde regelmäßig bedauert. Die Anfragen seien entweder nie eingegangen oder dem Datenschutzbeauftragten des Providers nicht vorgelegt worden. Organisatorische Maßnahmen, die hier Abhilfe schaffen sollen, und eine Datenschutzschulung der betroffenen Service-Mitarbeiter über die Rechte der Kundinnen und Kunden wurden der Aufsichtsbehörde zugesagt.

Auch wenn den Verbrauchern in den Beschwerdefällen letztendlich geholfen werden konnte, bleibt - nicht zuletzt unter dem Eindruck der hohen Provision, die die Werber erhalten - in diesen Fällen der Eindruck zurück, dass hier so genannte moderne Kundengewinnungsstrategien immer mehr auf Methoden der "Bauernfängerei" mit "Kopfprämie" zurückgreifen.

### 8.7 Veröffentlichung personenbezogener Daten von deutschen Domain-Inhabern über Who-Is-Datenbanken im WWW

Im Tätigkeitsbericht für das Jahr 1999 wurde die Veröffentlichung personenbezogener Daten im Internet durch die DENIC e.G., der deutschen Vergabestelle für Internet-Domains unterhalb der Top-Level-Domain ".de", bereits detailliert dargestellt (13. Tätigkeitsbericht vom 30. August 2000, LT-Drucks. 15/1539, Nr. 9.2).

Die DENIC e.G. veröffentlicht aus Datenschutzgründen auf ihrem Who-Is-Server im WWW seit den Gesprächen mit dem Regierungspräsidium Darmstadt keine Telefon- und Telefaxnummern oder E-Mail-Adressen von Domain-Inhabern oder der admimistrativen Kontaktperson der jeweiligen Domain mehr. Die Zahl der Beschwerden über die Veröffentlichungen der DENIC e.G. sind seitdem deutlich zurückgegangen.

Dennoch werden die Datenschutzaufsichtsbehörden für den nicht öffentlichen Bereich weiter darauf achten müssen, dass die vielen deutschen Domain-Provider und Discounter ihre Kunden bei der Domain-Beantragung ausführlich im Sinne des § 4 TDDSG unterrichten und auf ihren eigenen Who-Is-Servern (soweit vorhanden) nur die Datenarten veröffentlichen, die auch bei der DENIC e.G. abrufbar sind. Falls keine ausdrückliche Einwilligung des Betroffenen vorliegt, dürften weder E-Mail-Adresse noch Telefax- oder Telefonnummer eines Domain-Inhabers oder "admin-c" bei der Who-Is-Abfrage eines deutschen Who-Is-Severs auftauchen, weil hierfür - im Gegensatz zu Name und zustellungsfähiger Anschrift - keine Rechtsgrundlage im BDSG oder im TDDSG vorliegt.

Bezüglich der Veröffentlichung personenbezogener Daten deutscher Domain-Inhaber und der bei der europäischen Vergabestelle für IP-Nummern RIPE (Réseaux IP Européens) in den Niederlanden existierenden vielfältigen Abfragemöglichkeiten (z.B. Invers-Suche) arbeitete das Regierungspräsidium Darmstadt mit dem Bundesbeauftragten für den Datenschutz zusammen. Nachdem die DENIC e.G. ihre Domain-Verwaltung soweit wie möglich von RIPE entkoppelt und einen eigenen Datenbestand aufgebaut hatte, bat der Bundesbeauftragte für den Datenschutz auf Anregung des Regierungspräsidiums Darmstadt die niederländische Datenschutzaufsichtsbehörde darum, die Verarbeitungs- und Veröffentlichungspraxis personenbezogner Daten bei RIPE datenschutzrechtlich zu überprüfen. Die niederländischen Datenschützer kamen zu dem Ergebnis, dass das Vorhalten der Personendaten deutscher Domain-Inhaber durch RIPE nicht erforderlich ist, da die Domainvergabe ausschließlich in Deutschland durch die DENIC e.G. erfolgt. Die deutschen Personendaten wurden daraufhin bei RIPE gelöscht. Bei Who-Is-Abfragen nach deutschen Domains greift RIPE seit einiger Zeit auf den datenschutzrechtlich zulässigen Datenbestand der DENIC e.G. zurück.

### 8.8 Unzulässige Nutzung von E-Mail-Adressen für unverlangte Werbung (Spam)

Werbung per E-Mail zu versenden, ist unkompliziert, schnell und kostengünstig. Allerdings hat sich in der deutschen Rechtsprechung in den letzten Jahren in Anlehnung an die bereits ergangenen Urteile zur unverlangten Telefon- und Telefaxwerbung die verbraucherfreundliche Auffassung etabliert, dass es grundsätzlich gegen das Verbot unlauteren Wettbewerbs verstößt, wenn Werbung unverlangt an einen E-Mail-Anschluss versandt wird (siehe LG Traunstein, Az. 2 HKO 3755/97, AG Brakel, Az. 7 C 748/97, LG Berlin, Az. 16 O 201/98, 16 O 301/98 und 16 O 320/98, LG Ellwangen, Az. 2 KfH o 5/99). Dies gilt nicht nur im Privatbereich, sondern auch bei E-Mail-Werbung an Selbstständige, Gewerbetreibende und Freiberufler, wenn kein Einverständnis vorliegt oder nicht bereits eine Geschäftsverbindung besteht. Wie beim Empfang unverlangter Telefaxe wird dies von den Gerichten in der Hauptsache mit der Verursachung von Aufwand und Kosten beim Empfänger der unverlangten Werbung begründet.

Aber auch aus der datenschutzrechtlichen Perspektive werden an die Zulässigkeit der werblichen Nutzung von personenbeziehbaren E-Mail-Adressen hohe Anforderungen gestellt.
In der Regel benötigt der Versender einer Werbe-E-Mail für die werbliche Nutzung der E-Mail-Adresse nach dem deutschen "Online-Recht" - soweit er sich mit der E-Mail nicht im Rahmen der Voraussetzungen § 5 TDDSG bewegt (Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses) - die ausdrückliche Einwilligung des betroffenen E-Mail-Adress-Inhabers.

Und selbst bei Anwendung des weniger strengen "Offline-Rechts" auf die werbliche Nutzung von E-Mail-Adressen lässt sich kein gesetzlicher Erlaubnistatbestand für die Versendung unverlangter E-Mail-Werbung im BDSG erkennen, da der Gesetzgeber in den einschlägigen Vorschriften des § 28 BDSG der Beachtung schutzwürdiger Interessen der Betroffenen einen hohen Wert eingeräumt hat. Bei einer Verarbeitung personenbezogener Daten, die nach einschlägiger Rechtsprechung offensichtlich wettbewerbswidrig ist, besteht ganz deutlich Grund zur Annahme, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung im Sinne des § 28 Abs. 1 Nr. 2 und Nr. 3 BDSG überwiegt bzw. offensichtlich überwiegt.

Ohne eine ausdrückliche informierte Einwilligung der Betroffenen ist die werbliche Nutzung von E-Mail-Adressen also sowohl wettbewerbsrechtlich

als auch datenschutzrechtlich unzulässig. Die führenden deutschen Verbände des Direktmarketings und der Online-Wirtschaft (z.B. DDV, eco) haben diese datenschutzrechtlichen und wettbewerbsrechtlichen Anforderungen an E-Mail-Werbung bereits weitgehend in ihren Richtlinien und Empfehlungen an ihre Mitglieder umgesetzt.

Im Berichtsjahr ging nun dennoch eine außerordentlich hohe Anzahl von Beschwerden gegen unverlangte Werbe-E-Mails bei der Aufsichtsbehörde ein. Nicht nur private und geschäftliche Internet-Nutzer sind hiervon in steigendem Maße betroffen, sondern auch die Datenschutzaufsichtsbehörde selbst erhält seit 2001 regelmäßig unverlangte Werbe-E-Mails von ständig wechselnden Absendern. In einigen Unternehmen, in denen täglich Hunderte dieser fragwürdigen Angebote in den E-Mail-Postfächern der Mitarbeiterinnen und Mitarbeiter eingehen, sind diese E-Mails inzwischen zu einem regelrechten Ärgernis und auch zu einem ernstzunehmenden Kostenfaktor geworden.

Dabei handelt es sich in der Regel um obskure Spendenaufrufe, Kettenbriefe, unseriöse Angebote, Erotik-Werbung oder die Aufforderung, eine ausländische Sex-Seite im WWW zu besuchen, von der aus dem Nutzer ein teures 0190er-Einwahlprogramm (0190er-Dialer) auf dem heimischen PC installiert werden soll. Der Werbecharakter der E-Mails ist dabei nicht immer zu erkennen. Oftmals wird auf einen fiktiven früheren Kontakt in einem Chatroom Bezug genommen oder es erscheint so, als handele es sich um eine private und sehr persönliche E-Mail, die für jemand anderen bestimmt war und dem Empfänger anscheinend nur "versehentlich" zugestellt wurde. Dies sind aber letztlich alles nur Tricks und Lockmittel, um den E-Mail-Empfänger zu verführen, zu den umworbenen WWW-Seiten zu surfen.

Um datenschutzrechtlich oder auch wettbewerbsrechtlich gegen den Versender vorgehen zu können, muss zunächst der so genannte "E-Mail-Header" (alle Kopfzeilen der E-Mail) analysiert und der Absender herausgefunden werden. Dabei stellte sich immer wieder heraus, dass die angegebene Absender-Adresse gefälscht wurde. Entweder existierte die Adresse gar nicht (mehr) oder sie gehörte einem an der E-Mail-Versendung ganz und gar unbeteiligten Dritten, dessen E-Mail-Adresse von dem eigentlichen Versender in böser Absicht missbraucht wurde. Bei den wenigen Fällen, in denen die Absender-Adresse nicht gefälscht war, handelte es sich um Adressen aus dem nicht europäischen Ausland, von denen keine Reaktion auf Anfragen oder Beschwerden zu erhalten war.

Diese E-Mail-Massenversender benutzen für ihre Spam-Kampagnen schlecht konfigurierte E-Mail-Server (so genannte offene Mail-Relays), die weltweit zur Versendung ohne Absenderauthentifizierung zur Verfügung stehen. Das heißt, dass diese Server alle zum Versenden eingelieferten E-Mails verschicken bzw. weiterleiten, gleichgültig wer auch immer der Absender ist. Im Berichtsjahr taten sich hierbei besonders Korea und einige andere südostasiatische Staaten hervor, wo offensichtlich in vielen Schulen schlecht gewartete oder unkonfigurierte E-Mail-Server installiert sind, die nicht ordnungsgemäß administriert werden und daher international für die Versendung unverlangter Massen-Werbung zu missbrauchen sind.

Die E-Mail-Absender bleiben also anonym oder haben ihren Sitz im Ausland. Dadurch wird die Durchsetzung der Betroffenenrechte und wettbewerbsrechtlicher Ansprüche erheblich erschwert oder in vielen Fällen gar unmöglich. Da trotz der zu erwartenden Regelungen auf EU-Ebene nicht zu hoffen ist, dass dieses Problem in Kürze gelöst werden kann, sondern eher damit gerechnet werden muss, dass E-Mail-Spam auch in Zukunft weiter zum Internet-Alltag gehören wird, kann die Datenschutzaufsichtsbehörde den E-Mail-Benutzern nur folgende Tipps und Ratschläge zum sorgsamen Umgang mit ihrer eigenen E-Mail-Adresse und unverlangten Werbe-E-Mails an die Hand geben:

1. Man sollte es vermeiden, seine "erste" private E-Mail-Adresse öffentlich überall bekannt zu geben.
2. Es empfiehlt sich, für verschiedene Zwecke, z.B. Mailinglisten, Newsletter, Chat-Rooms, Gästebücher, Usenet und andere Veröffentlichungsvarianten, eine oder mehrere zusätzliche, oft kostenlose E-Mail-Adressen zu benutzen.

3. Es sollte sich bei der "Zweitadresse" nie um eine fiktive oder falsche E-Mail-Adresse handeln. (s. http://home.pages.de/~gerlo/falsche-email-adressen.html).
4. In der Öffentlichkeit sollte immer nur die "Zweitadresse" benutzt werden. So bleibt zumindest die erste Adresse von unverlangter E-Mail-Werbung verschont.
5. Man sollte immer bedenken, dass E-Mail-Adressen bei der aktiven Teilnahme an Newsgroups oder Mailinglisten und WWW-Foren weltweit verfügbar und daher auch missbrauchbar sind. Auch wenn E-Mail-Adressen auf WWW-Seiten abgefragt werden, ist es gerade bei ausländischen Anbietern möglich, dass diese Adressen in Datenbanken landen, die später für Werbemails verwendet werden. Dies gilt leider auch für die vielen Gästebücher, die auf WWW-Seiten gerne angeboten werden. Die so beliebten "digitalen Glückwunschkarten" können ebenfalls dazu führen, dass E-Mail-Adressen in unerwünschte Hände geraten. Die Mailadressen auf WWW-Homepages werden mit großer Wahrscheinlichkeit ebenfalls durch Programme ausgelesen.
6. Man sollte nie direkt auf unseriös scheinende unverlangte Werbe-E-Mails reagieren. Die Gültigkeit der missbrauchten Adresse würde damit bestätigt und der Marktwert der E-Mail-Adresse würde damit noch steigen.
7. Der E-Mail-Header muss analysiert werden. Dies kann z.B. auch mithilfe der deutschen Spezial-Newsgroup für E-Mail-Beschwerden "de.admin.net-abuse.mail" oder der Tipps auf einschlägigen Hilfeseiten zu "Spam" im WWW oder mit einem der frei erhältlichen Software-Tools geschehen. Man sollte sich dann immer auch unter Vorlage des kompletten E-Mail-Headers beim Provider des Versenders beschweren, der zuvor bei der Header-Analyse herausgefunden wurde.
8. Jedem Nutzer ist zu raten, die E-Mail-Filter zu benutzen, die in jedem gängigen E-Mail-Programm enthalten sind und auch von allen Providern zusätzlicher kostenloser E-Mail-Adressen angeboten werden, um unerwünschte Werbe-E-Mails gar nicht erst herunterladen zu müssen, sondern gleich löschen zu lassen.

In lediglich einem Beschwerdefall gelang es der Datenschutzaufsichtsbehörde, anhand der Analyse des in diesem Fall ungefälschten E-Mail-Headers einen deutschen Newsletter-Versender aus dem Rhein-Main-Gebiet zu identifizieren. Dieser behauptete, der Adressinhaber selbst habe seine E-Mail-Adresse bei einer Newsletter-Bestellung im WWW angegeben und damit auch seine Zustimmung zur Nutzung erteilt. Der Beschwerdeführer stritt dies strikt ab. Die Behauptungen des Versenders schienen etwas unglaubwürdig, konnten aber nicht widerlegt werden. Die Herkunft der werblich genutzten E-Mail-Adresse konnte unter den gegebenen Umständen nicht geklärt werden. Die Datenschutzaufsichtsbehörde konnte aber zumindest dabei helfen, dass die genutzte Adresse bei dem Newsletter-Anbieter gelöscht bzw. für die künftige werbliche Nutzung gesperrt wurde.

### 8.9 Missbrauch eines kostenlosen Internet-Dienstes

Das Versenden von SMS-Nachrichten von Handy zu Handy ist nicht nur unter Jugendlichen sehr beliebt. Viele Internet-Provider bieten die Möglichkeit, auch aus einem WWW-Formular heraus kostengünstig und bequem SMS-Nachrichten an Handys zu versenden. Ein WWW-Anbieter aus dem Rhein-Main-Gebiet bot ohne vorherige Identifikation des Nutzers zusätzlich die Funktion, eine frei wählbare Handy-Nummer als Absender der kostenlosen SMS angeben zu können.

Dieses "feature" machte sich eine unbekannte Person zunutze, die belästigende und bedrohende E-Mails an den Arbeitgeber eines Beschwerdeführers sandte und dabei die Handynummer des Petenten als Absender-Nummer der SMS angab. Neben der bereits eingeleiteten strafrechtlichen Verfolgung des Täters bat der Betroffene die Datenschutzaufsichtsbehörde, dafür zu sorgen, dass der SMS-Versendemechanismus bei dem Provider so umgestellt wird, dass ein Missbrauch künftig nicht mehr möglich ist.

Der Provider wurde aufgefordert, durch geeignete technische und organisatorische Maßnahmen im Sinne des § 9 Satz 1 BDSG (insbesondere Nr. 5 der Anlage hierzu) sicherzustellen, dass SMS-Nachrichten erst dann verschickt

werden können, wenn ihm zuverlässige Anhaltspunkte dafür vorliegen, dass keine falsche Handy-Nummer als Absender angegeben wurde, da dem Missbrauch ansonsten Tür und Tor geöffnet sind.

Der Provider, dem der Fall bereits bekannt war, reagierte sofort auf diesen Hinweis und implementierte hier ein Anmeldeverfahren mit Verifikationsroutine für die Handynummer. Nun wird nach der Anmeldung ein Freischaltcode an die Handy-Nummer des Absenders übermittelt, der vor dem erstmaligen Versenden einer SMS als Beleg für die Echtheit der Handy-Nummer zurückgesendet werden muss. Ohne Freischaltcode zur Verifizierung der Handy-Nummer kann keine SMS mehr versandt werden.

### 8.10 Verwirrung um die weitere Gültigkeit der E-Mail-Adressen gekündigter Mitarbeiter

In drei Fällen wurde das Regierungspräsidium Darmstadt im Berichtsjahr mit Sachverhalten konfrontiert, in denen Unternehmen ihren Mitarbeitern E-Mail-Adressen in der Form "Vorname.Nachname@firma.de" zur Verfügung stellten und diese nach erfolgter Kündigung der Beschäftigten nicht löschten. In allen Fällen wurden die E-Mail-Adressen nach der recht konfliktreichen Kündigung der ehemals als leitende Angestellte beschäftigten Mitarbeiter in den Betrieben über Monate hinweg weiter aufrechterhalten. Alle eingehenden E-Mails - darunter auch private Mitteilungen - wurden von der Geschäftsführung der Unternehmen bis zu einem Jahr lang weiter abgerufen und gelesen.

In zwei Fällen beschwerten sich die betroffenen ehemaligen Mitarbeiter bei der Datenschutzaufsichtsbehörde darüber, dass ihre alten E-Mail-Accounts trotz Zusage der Geschäftsführung, diese stillzulegen, wohl immer noch voll funktionsfähig seien. Die eingehenden privaten E-Mails würden von dem Geschäftsführer nach dem Lesen gelöscht. Dies erfolge ohne einen entsprechenden geeigneten Hinweis an den Absender, dass die E-Mail dem Empfänger nicht zugestellt werden konnte und dass dieser nicht mehr in dem Betrieb beschäftigt ist. In einem für alle Beteiligten besonders unangenehmen Einzelfall hatte ein Bekannter eines gekündigten Mitarbeiters diesem versehentlich eine private E-Mail an dessen alten Firmen-Account geschickt. Die E-Mail enthielt auch einige abfällige Bemerkungen über die dortige Geschäftsführung, die sich nach Kenntnisnahme der E-Mail-Inhalte umgehend beim Arbeitgeber des E-Mail-Absenders beschwerte und diesem geschäftliche Konsequenzen androhte.

In keinem der bearbeiteten Fälle lagen Betriebsvereinbarungen zur privaten und dienstlichen Nutzung des Internet und der E-Mail-Dienste vor, es gab auch keine klaren und von der Aufsichtsbehörde nachvollziehbaren organisatorische Anweisungen oder Regelungen der jeweiligen Geschäftsleitung hierzu. Die private Nutzung des Firmenanschlusses durch die Mitarbeiter wurde seit Jahren stillschweigend geduldet. Über die Frage, wie lange ein solcher E-Mail-Anschluss nach dem Ausscheiden eines Beschäftigten aufrechterhalten wird und ob die in dieser Übergangszeit eingehenden privaten E-Mails überhaupt zur Kenntnis genommen werden dürfen, hatte in den kleinen und modernen Unternehmen zuvor noch nie jemand nachgedacht. Man wolle schließlich nur sichergehen, dass eingehende geschäftliche E-Mails auch weiter beantwortet werden können. An privaten E-Mails habe man kein Interesse und lösche diese auch sofort.

Nachdem die Datenschutzaufsichtsbehörde die Unternehmen darauf hingewiesen hatte, dass sich die beteiligten Personen (Geschäftsführer und EDV-Administrator) in den Unternehmen, wenn die private Nutzung der Internet-Anschlüsse nicht verboten oder zumindest entsprechend geregelt ist, der Gefahr eines Strafverfahrens wegen Verstoßes gegen das Fernmeldegeheimnis aussetzen, wenn sie private E-Mails ausgeschiedener Mitarbeiter lesen, wurden die betroffenen E-Mail-Accounts in allen Fällen stillgelegt.

Wie eine Anschlussüberprüfung der Datenschutzaufsichtsbehörde durch eine Test-E-Mail ergab, wurden in einem Fall die an nicht mehr existierende E-Mail-Postfächer gesandten E-Mails trotz der Löschung der E-Mail-Adresse weiter der Geschäftsführung vorgelegt. Der Absender erhielt immerhin eine automatische Nachricht, dass der Empfänger in dem Unternehmen nicht mehr erreichbar sei. Da die Kenntnisnahme privater E-Mail-Inhalte auf diese Weise immer noch nicht ausgeschlossen war, musste die Dienststelle das

Unternehmen nochmals dazu drängen, den E-Mail-Server so zu konfigurieren, dass eingehende E-Mails für nicht mehr existierende E-Mail-Adressen künftig dem Absender automatisch von dem E-Mail-Server mit einer erklärenden Bemerkung zurück gesandt werden, ohne dass in dem Unternehmen jemand vom Nachrichteninhalt Kenntnis nimmt.

Den betroffenen Unternehmen wurde grundsätzlich nahegelegt, die dienstliche und private Nutzung der Internetanschlüsse sowie mögliche Nutzungskontrollen und Fragen der Dauer des Weiterbestands der E-Mail-Adressen konkret nachvollziehbar in einer Betriebsvereinbarung zu regeln.

Wie so oft wurde die Datenschutzaufsichtsbehörde bei der Beschwerdebearbeitung auch noch auf weitere datenschutzrechtliche Mängel aufmerksam, die gegenüber den Unternehmen beanstandet wurden. In einem Fall entsprach der Umfang der Anbieterkennzeichnung auf den WWW-Seiten des Unternehmens nicht den gesetzlichen Vorschriften des § 6 TDG a.F., in einem anderen Fall musste das Unternehmen aufgefordert werden, nicht nur die E-Mail-Adresse des Beschwerdeführers zu löschen, sondern auch dessen Namen von den WWW-Seiten des Unternehmens zu entfernen. Da der Arbeitsvertrag mit dem ehemaligen Beschäftigten schon seit langem erloschen war, entbehrte die weltweite Veröffentlichung seines Namens im WWW der nach dem BDSG erforderlichen Rechtsgrundlage.

## 9. Banken

### 9.1 Versendung von PIN und TAN als Werbemaßnahme

Marketingmaßnahmen der Banken werden teilweise sehr kreativ gestaltet, der Datenschutz wird dabei leider nicht immer ausreichend berücksichtigt.
So erhielten Bankkunden Werbung zur Teilnahme am Internetbanking unter gleichzeitiger Übersendung der hierfür notwendigen individuellen PIN (Persönliche Indentifikationsnummer).
Vierzehn Tage später erhielten die Kunden unaufgefordert auch noch die TANs (Transaktionsnummern) und damit das vollständige Rüstzeug für Aktionen im Internet.
Trotz der zeitverzögerten Übersendung der TANs waren die mit dieser Werbeaktion verbundenen Risiken nicht akzeptabel. Insbesondere bei Kunden, die nicht anwesend waren, konnten PIN und TAN nacheinander im Briefkasten liegen bleiben und damit zum unkalkulierbaren Risiko werden.
Ein unbefugter Dritter hätte mit Kenntnis von Kontonummer, PIN und TAN Abfragen des Kontos und sogar Kontoverfügungen vornehmen können. Im Normalfall erfolgt die Freischaltung zum Online-Banking erst auf schriftlichen Antrag des Kunden. Es war daher unverständlich, warum im Gegensatz hierzu im Rahmen der Werbemaßnahme auf einen entsprechenden schriftlichen Antrag zur Freischaltung von Girokonten verzichtet wurde. Nach Darstellung der Bank hat es trotz der geschilderten Risiken keine Missbräuche gegeben.
Datenschutzrechtlich zu beanstanden war die Maßnahme gleichwohl.

Die geschilderte Werbemaßnahme wurde daher aufgrund entsprechender Rügen der Aufsichtsbehörde eingestellt und wird nicht wiederholt.

### 9.2 Speicherung der Empfängerdaten für die optische Zeichenerkennung (OCR)

Die Verarbeitung der vom Kunden ausgefüllten Belege geschieht weitgehend automatisiert. Die Belege werden zum einen als optisches Bild gespeichert, zum anderen wird der Inhalt des Beleges gelesen und interpretiert (optical character recognition). Bei der Informationserkennung können Lesefehler auftreten, da die Handschrift der Kunden nicht immer eindeutig ist.
Diese Lesefehler versucht der programmierbare elektronische Leser zu minimieren, indem er von vorherigen Transaktionen Daten speichert und dann beispielsweise den Namen des Empfängers mit den Kenntnissen aus früheren Überweisungen korrigiert.
Die geschilderte Datenspeicherung am Belegleser führt immer dann zu Problemen, wenn das historisch gespeicherte Datum falsch ist und der aktuelle Beleg nicht richtig gelesen werden kann: Dann wird automatisch das falsch gespeicherte Datum genutzt.

Die Speicherung beispielsweise eines falschen Empfängernamens kann entstehen, wenn der elektronische Belegleser bei der zurückliegenden Verarbeitung etwas falsch gelesen und dies trotzdem als richtig interpretiert hat. Aber auch eine manuelle Korrektur durch den zuständigen Banksachbearbeiter kann - wie im konkreten Beschwerdefall geschehen - zu einem falschen historischen Datum führen.
Der solchermaßen verursachte Fehler ließ sich mit einer erneuten manuellen Korrektur, d.h. durch eine Eingabe in den Speicher des Lesegerätes, beseitigen.

Obwohl Datenspeicherungen auf Vorrat allgemein als kritisch betrachtet werden, sind diesbezügliche Bedenken zurückzustellen. Die Bank verfügt ohnehin nochmals über die gleichen Daten, um zehn Jahre lang mit ihren Buchungssystemen eine ordnungsgemäße Buchführung nach den Vorgaben der Abgabenordnung und des Handelsgesetzbuches zu gewährleisten. Die weitere Speicherung dieser Daten für die OCR ist mit den übrigen Computersystemen nicht vernetzt und dient ausschließlich dem Zweck der besseren optischen Belegerkennung. Die Zweckbindung ist technisch-organisatorisch sichergestellt. Ohne diese Speicherung wäre der manuelle Korrekturaufwand bei der Datenerfassung erheblich höher.

Im Ergebnis war die Speicherung daher nicht zu beanstanden.

### 9.3 Speicherung einer Kundenunterschrift

Die Unterschrift unter eine Zahlungsverfügung ist weiterhin das vorherrschende Beweismittel dafür, dass die Verfügung tatsächlich vom berechtigten Kontoinhaber stammt. Bei der Prüfung von Zahlungsbelegen muss deshalb die vom Kunden hinterlegte Unterschrift zum Vergleich herangezogen werden. Damit dies rationell an allen erforderlichen Stellen der Bank durchgeführt werden kann, wird die Unterschrift des Kunden mit einem Scanner erfasst und elektronisch gespeichert.
Ein Beschwerdeführer hatte seine Art, die Unterschrift zu leisten (Duktus/Schrift), erheblich verändert und wurde deshalb gebeten, in einer Filiale der Bank unter Vorlage seines Personalausweises eine neue Musterunterschrift abzugeben.
Die dadurch verursachten Irritationen des Betroffenen entstanden, weil er die banküblichen Arbeitsweisen nicht kannte. Die elektronische Speicherung der Unterschriften war nicht zu beanstanden. Im Vergleich zur herkömmlichen Unterschriftenkartei entstehen keine besonderen zusätzlichen Risiken für den Kunden, da ohnehin jede Unterschrift auf einem Dokument mit einfachsten Mitteln erfasst und beliebig reproduziert werden kann. Es war anzuerkennen, dass die Bank die Kontrolle der Kundenunterschrift sehr sorgfältig vollzog und dabei auf Abweichungen bei der Unterschriftsleistung aufmerksam wurde. Im Interesse des Kunden und der Bank können so nicht mit der Originalunterschrift gezeichnete Dokumente besser identifiziert werden.
Leider ist die arbeitsaufwendige Unterschriftenprüfung bei den Banken ein mitunter vernachlässigter Arbeitsbereich. Dies ist jedoch in erster Linie ein finanzielles Problem des Ausfallrisikos - je nach Situation zulasten der Bank oder des Kontoinhabers - und kein Datenschutzproblem. Im vorliegenden Fall hatte die Bank jedoch gerade - unterstützt durch die elektronische Unterschriftenerfassung - die gebotene Sorgfalt bei der Unterschriftenprüfung angewandt.
Im Beschwerdefall waren beim Bankkunden zusätzliche Irritationen aufgetreten, weil das Formular für eine neue Unterschriftsleistung identisch mit einem Kontoeröffnungsformular war und darüber hinaus noch nachträglich eine Erklärung nach § 8 Geldwäschegesetz gefordert wurde. Als die Bank auch noch Vorder- und Rückseite des Personalausweises in Kopie haben wollte, ohne auf die Freiwilligkeit hinzuweisen, wurde der Kunde besonders misstrauisch. Eigentlich wollte die Bank dem Kunden nur helfen und ihm den Weg in die Bank und die persönliche Vorlage des Ausweises ersparen. Die vorherigen und anschließenden Erklärungen der Bank waren für einen Betroffenen, der sich im Bankwesen nicht näher auskennt, jedoch nicht zweifelsfrei nachvollziehbar.
Auf diese Weise entstand eine Beschwerde, die außer der unbefriedigenden Erläuterungen der Bank letztlich keinen Grund zur Beanstandung gab.

### 9.4 Unzulässige Weitergabe der Kundenadresse an einen Markt- und Meinungsforscher

Eine Bank ließ durch einen Markt- und Meinungsforscher eine telefonische Kundenbefragung durchführen.
Die Durchführung der Befragung und die Auswertung der Ergebnisse wurde von der Bank genau bestimmt, die Tätigkeiten waren deshalb als Auftragsdatenverarbeitung zu bewerten (siehe 13. Tätigkeitsbericht, LT-Drucks. 15/1539, Nr. 5.4).
Zwei Wochen vor der Datenweitergabe an das Markt- und Meinungsforschungsinstitut erhielten die ausgewählten Kunden von der Bank einen schriftlichen Hinweis auf die Telefonbefragung.
Sie bekamen die Möglichkeit, mit dem Anruf einer kostenfreien Servicetelefonnummer die Weitergabe ihrer Daten für die Telefonbefragung zu unterbinden. Der Hinweis war gut sichtbar, klar und deutlich formuliert. Es bestanden diesbezüglich keine datenschutzrechtlichen Einwendungen.

Die Bank hatte jedoch an den Markt- und Meinungsforscher nicht nur die für die Befragung notwendige Telefonnummer, sondern auch die Kundenadresse weitergegeben. Die Datenweitergabe muss sich jedoch strikt an den Erfordernissen der jeweiligen Studie orientieren. Für die telefonische Befragung wurde die Kundenadresse nicht benötigt. Die Weitergabe der Adresse wurde deshalb beanstandet, denn auch im Rahmen einer Auftragsdatenverarbeitung sind die Zugriffsmöglichkeiten des Markt- und Meinungsforschungsinstituts auf das für die jeweilige Aufgabe erforderliche Maß zu beschränken (siehe Anlage zu § 9 Satz 1 Nr. 3 BDSG - Zugriffskontrollen).
Nach der Marktforschungsaktion wurden alle Bank-Kundendaten beim Markt- und Meinungsforschungsunternehmen gelöscht, ein bleibender Schaden entstand deshalb nicht.

Die Bank versicherte, Datenweitergaben künftig nur im wirklich erforderlichen Umfang vorzunehmen.

### 9.5 Unzulässige Übermittlung von Kundendaten an Finanzberater

Ein in Berlin ansässiger selbständiger Finanzberater hatte von einem nicht mehr existierenden Finanzberatungsunternehmen, dessen Mitarbeiter er war, die Unterlagen mit Kopien von Kreditverträgen der Mandaten des Unternehmens für seine eigenen Zwecke behalten. Er war kein Rechtsnachfolger des aufgelösten Unternehmens, daher war bereits die Ansichnahme dieser Unterlagen durch den ehemaligen Unternehmensmitarbeiter als unzulässig zu bewerten. Auf die Beanstandungen des insoweit zuständigen Berliner Beauftragten für Datenschutz und Informationsfreiheit löschte der Finanzberater sämtliche Datenbestände bezüglich dieser "Altkunden".

Der Finanzberater hatte mit den bei ihm verbliebenen Kopien der Kreditverträge genaue Kenntnis darüber, wann die jeweiligen Zinsbindungsfristen enden würden und konnte so seine Dienste gezielt anbieten. Darüber hinaus hatte er bei der finanzierenden Bank den aktuellen Stand eines Kredits abgefragt, ohne vom betroffenen Bankkunden hiermit beauftragt worden zu sein. Die in Hessen ansässige Bank erteilte - entgegen dem in den Geschäftsbedingungen dem Bankkunden zugesicherten Bankgeheimnis - Auskunft an den Finanzberater. Die betroffenen Kunden erfuhren hiervon, da der Finanzberater ihnen ein entsprechendes Fortsetzungsangebot für den Kreditvertrag mit der Bank zusandte. Zu Recht beschwerten sie sich, denn sie hatten den Finanzberater nicht ermächtigt, für sie tätig zu werden. Die Aufsichtsbehörde beanstandete daraufhin gegenüber der Bank die Erteilung der Bankauskunft.
In Zweifelsfällen muss sich die Bank bei ihrem Kunden rückversichern, ob ein Dritter für den Kunden empfangsberechtigt ist.
Die Bank bedauerte den Vorfall. Es ist davon auszugehen, dass derartige unzulässige Übermittlungen zukünftig unterbleiben.

### 9.6 Datenübermittlung zwischen Banken und Versicherungen

Wenn Banken und Versicherungen in einem Konzern verbunden sind, besteht aus unternehmerischer Sicht naturgemäß das Interesse, den Kunden für die gesamte Produktpalette zu gewinnen. Da es nach dem BDSG kein Konzernprivileg gibt, müssen die datenschutzrechtlichen Schranken bei der Übermittlung personenbezogener Daten beachtet werden. Durch die Novelle des BDSG hat sich hieran nichts geändert.

Zu Recht beschwerte sich daher die Kundin einer thüringischen Bank, als sie Werbung von einer Versicherung erhielt und erfuhr, dass der im Werbeschreiben genannte Versicherungsmitarbeiter wusste, dass sie Kundin der betreffenden thüringischen Bank sei und über ein höheres Einkommen verfüge.
Die Kundin war, wie es der Zufall will, selbst in leitender Position in einer anderen Versicherung tätig.

Da sich die Bank in der Korrespondenz mit der an sich örtlich zuständigen Datenschutzbehörde, dem Thüringer Landesverwaltungsamt, von einer in Hessen ansässigen Bankenorganisation vertreten ließ, gab das Thüringer Landesverwaltungsamt den Vorgang an das Regierungspräsidium Darmstadt ab.
Dieses vertrat in Übereinstimmung mit dem Thüringer Landesverwaltungsamt die Auffassung, dass die vom Bankvertrag nicht gedeckte und damit zweckändernde Übermittlung an die Versicherung auch nicht nach § 28 Abs. 1 Nr. 2 BDSG erlaubt sei. Bei der gebotenen Abwägung mit den schutzwürdigen Belangen der Betroffenen ist das Bankgeheimnis zu berücksichtigen. Dieses steht der Übermittlung entgegen.

Wollen Banken und Versicherungen im Verbund zusammenarbeiten und zu diesem Zweck personenbezogene Daten der Kunden übermitteln, müssen sie hierfür die Einwilligung der Kunden einholen.

Entsprechende "Verbundklauseln" wurden bereits vor vielen Jahren zwischen dem Düsseldorfer Kreis und den Verbandsvertretern der Versicherungen und Banken abgesprochen.

Nach intensiver Diskussion teilten die Unternehmens- bzw. Verbandsvertreter mit, dass die Versicherung (!) die Banken entsprechend informiert habe.

Es bleibt abzuwarten und durch Überprüfung der Banken zu kontrollieren, ob das Einwilligungserfordernis künftig beachtet wird.

### 9.7 Auswertung der Betreff-Angabe bei Banküberweisungen

Ein Betroffener ging davon aus, dass eine Bank aufgrund der Betreff-Angaben im Überweisungsbeleg für ihn negative Kenntnisse erlangt und diese genutzt habe.
Es ließ sich nicht völlig ausschließen, dass in diesem Einzelfall der Sachbearbeiter bei der kontoführenden Bank - ohne besondere Notwendigkeit - Einblick genommen hatte. Beispielsweise für die Klärung einer fehlgeleiteten Zahlung muss es für den Kontoführer grundsätzlich im Einzelfall möglich bleiben, auch den Betreff einer Überweisung einzusehen.
Es bestand jedoch - auch mit der Bank - allgemein Konsens darüber, dass eine systematische Auswertung der Betreff-Angaben einer Überweisung unzulässig ist. Diese Angaben unterliegen einer strikten Zweckbindung. Die Bank ist insoweit nur der Bote für die Überbringung einer Nachricht.

### 9.8 Beschränkung von Zugriffsrechten innerhalb überregional tätiger Banken

Die privaten Konten der Beschäftigten einer überregional tätigen Bank waren bisher jeweils bei derjenigen rechtlich unselbständigen Filiale geführt worden, in der sie tätig waren. Weitere Bankmitarbeiter außerhalb der Region konnten keine Kenntnis über die Konten erlangen. Als mit der Umorganisation der Bank überregionale Zugriffsmöglichkeiten eingeführt wurden, beschwerten sich betroffene Bankmitarbeiter bei der Aufsichtsbehörde, weil ihre Kontodaten von zahlreichen Bankkollegen im gesamten Bundesgebiet eingesehen werden konnten.

Das Problem wurde entschärft, indem die Mitarbeiter der Bank ihre Konten einer zentralen Filiale übertragen konnten. Bei dieser Filiale waren die Zugriffsmöglichkeiten eingeschränkt.
Mit dieser Alternative ging zwar ein gewisser Komfortverlust für die Beschäftigten einher. Eine direkte Kommunikation mit den Kollegen vor Ort in eigenen Finanzangelegenheiten war nur noch eingeschränkt möglich, weil diese für die jeweiligen eigenen Belange nicht mehr zuständig waren. Andererseits aber konnte die mit der "Mitarbeiterfiliale" geschaffene Distanz gerade wieder als Vorteil empfunden werden, denn nicht jeder Beschäftigte,

der ein privates Konto bei seinem Arbeitgeber hat, möchte, dass die direkten Kollegen hierin Einblick nehmen können.
Da die Mitarbeiter jedenfalls diese datenschutzgerechte Alternative wählen können, bestand insoweit kein Grund zur Beanstandung.
Die Beschwerde offenbarte jedoch grundsätzliche Probleme, da natürlich nicht nur Mitarbeiter, sondern vor allem Kunden von der Umorganisation betroffen waren. Wenn überregionale Banken ihren Kunden im gesamten Bundesgebiet den gleichen Service bieten wollen, führt dies zwangsläufig zu einem größeren Kreis von Berechtigten und damit zu einem statistisch höheren Missbrauchsrisiko. Dies ist im Hinblick auf die Anforderungen des § 9 BDSG kritisch zu sehen.
Die Aufsichtsbehörde befürwortet deshalb einen regional und sachlich beschränkten Zugriff auf die Kundendaten. Außerhalb der Region muss es im Einzelfall ausreichen festzustellen, ob z.B. für eine Barauszahlung ausreichend Deckung vorhanden ist.
Für die Größe einer regionalen Gliederung lassen sich keine Vorgaben nennen, da dies von der Größe der Bank abhängig ist. Es wird sich in der Regel - je nach Kundenstamm - eine praktikable und auch datenschutzrechtlich vertretbare Größe herausgebildet haben.
Bei den heutigen Kommunikationsmöglichkeiten sollte es jedenfalls möglich sein, bundesweite Berechtigungen einzuschränken. Im Einzelfall können immer noch weitergehende Zugriffe ermöglicht werden.

### 9.9 Falschversendung von Aktien-Mitteilungen

Die Verwaltung und Benachrichtigung von Aktionären mit Namensaktien ist eine Aufgabe, die von Aktiengesellschaften häufig an spezialisierte Dienstleister vergeben wird. Ein in Hessen ansässiger Dienstleister führt beispielsweise die Aktienregister von Emittenten girosammelverwahrter Namensaktien. In dieser Funktion als Aktienregisterführer erhält das Unternehmen auf elektronischem Wege von Kreditinstituten Umschreibungsanträge in einem standardisierten Format. Aufgrund dieser Umschreibungsanträge werden nach formaler Prüfung der Daten automatisch Eintragungen in dem Aktienregister vorgenommen.
Bei einem Aktien-Umschreibungsantrag wurde der Datensatz des neuen Aktionärs beim Dienstleister unvollständig empfangen. Lediglich der erste Buchstabe des Vornamens, der Titel und die Anschrift kamen an. Ob die einmeldende Bank die Daten unvollständig eingegeben hatte - das wurde von dieser bestritten - oder ein Fehler in dem speziellen elektronischen Übermittlungssystem vorlag, ließ sich nicht klären. Der Dienstleister fragte jedenfalls nicht bei der Ursprungsbank zurück oder gab auch nicht den verfälschten Datensatz zwecks Klärung zurück. Vielmehr recherchierte er eigenmächtig in Telefonverzeichnissen und ermittelte den Namen und die Adresse des Beschwerdeführers, der jedoch die ihm zugeschriebenen Aktien nicht besaß. Er wurde gleichwohl als Aktieninhaber eingetragen. Als er verwundert nachfragte, wurde die Sache zunächst nicht aufgeklärt. Die falsche Eintragung blieb bestehen. Erst als er seinen Wohnort wechselte und der von der Post über die Adressänderung informierte Dienstleister ihm die Eintragung der neuen Adresse mitteilte, wurde die Verwechslung aufgedeckt.

Der Beschwerdeführer konnte mit seiner früheren Wohnadresse unschwer feststellen, welcher seiner früheren Hausmitbewohner der wahre Aktionär war. Die Aktionärsmitteilung an den falschen Empfänger führte damit zu einer unzulässigen Datenübermittlung über die Besitzverhältnisse eines Dritten.
Eine arbeitsteilige Vorgehensweise mag zu größerer Effizienz führen, dies gilt jedoch nur solange, wie die Vorgaben strikt eingehalten werden. Die eigenmächtige Korrektur von fehlerhaft übermittelten Daten muss deshalb unterbleiben.
Der betriebliche Datenschutzbeauftragte des Dienstleisters wies die Mitarbeiter nochmals ausdrücklich hierauf hin.

### 9.10 Falschversendung eines vertraulichen Telefaxes

Leider kommt es auch bei Banken vor, dass Telefaxe an einen falschen Adressaten gesandt werden. Im Beschwerdefall wurden gleich 48 Seiten mit Vermögensaufstellungen und Einkommenssteuerberechnungen an den falschen Empfänger geleitet.
Das Problem der Anwahl eines falschen Empfängers ist so alt, wie es Faxgeräte gibt. Von einer Bank muss aber erwartet werden können, dass beson-

dere Sorgfalt angewandt wird. Vor Absendung ist die angewählte Faxnummer noch einmal zu vergleichen. Hierbei sollte in jedem Fall berücksichtigt werden, dass bei Nebenstellenanlagen in der Regel eine Null vorher gewählt werden muss. Im anderen Fall wird - wie hier geschehen - die erste Null der Ortsvorwahl für die Wahl der Amtsleitung genutzt und die restlichen Ziffern der Zielnummer führen zu einem unbekannten Dritten. Im günstigsten Fall erfolgt die Meldung "kein Anschluss unter dieser Nummer". Theoretisch könnte das vertrauliche Fax unter Umständen aber auch bei der Konkurrenz oder sonstigen Dritten ankommen.
Da derartige Ereignisse leider zu häufig - nicht nur bei Banken - vorkommen, muss immer wieder auf diese Schwachstelle hingewiesen werden.
Empfehlungen zum datenschutzgerechten Umgang mit Telefaxgeräten wurden unter anderem von der Konferenz der Datenschutzbeauftragten herausgegeben (www.datenschutz.hessen.de/o-hilfen/telef-tx.htm).

## 10. Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA)

### 10.1 Neustrukturierung der SCHUFA

Die SCHUFA Holding AG hat sich zum 1. Januar 2002 zu einem einheitlichen Unternehmen in Wiesbaden zusammengeschlossen. Die bisher bestehenden regionalen SCHUFA-Gesellschaften (rechtlich selbstständige GmbHs) wurden zu diesem Termin mit der Holding verschmolzen. Die Bezeichnung Holding wird trotzdem beibehalten.

Weil die SCHUFA ihren Sitz in Wiesbaden hat, ist die grundsätzliche Zuständigkeit des Regierungspräsidiums Darmstadt gegeben. Es ist jedoch nicht sinnvoll, wenn deshalb alle Beschwerden über die SCHUFA an das Regierungspräsidium abgegeben werden.
Fehler treten in der Regel im Zusammenhang mit Meldungen von Anschlussunternehmen der SCHUFA auf. Diese SCHUFA-Anschlusspartner sind über die ganze Bundesrepublik verteilt und für diese "Fehlerverursacher" sind dann andere Aufsichtsbehörden zuständig. Mit den übrigen Datenschutzaufsichtsbehörden wurde deshalb vereinbart, dass einer Betroffenenbeschwerde zunächst in der jeweiligen Region nachgegangen und eine Klärung mit der dortigen SCHUFA-Niederlassung herbeigeführt wird, jedenfalls soweit es sich um übliche Standardfälle oder einfache Anfragen von Bürgern handelt.

Sollten sich im Einzelfall Auffassungsunterschiede mit der SCHUFA oder Grundsatzfragen abzeichnen, wird der Fall zuständigkeitshalber von der jeweiligen Datenschutzaufsichtsbehörde an das Regierungspräsidium Darmstadt zur Bearbeitung abgegeben werden.

Weiterhin findet in der Arbeitsgruppe "Auskunfteien/SCHUFA" des "Düsseldorfer Kreises" (=Arbeitskreis der obersten Datenschutzaufsichtsbehörden der Bundesländer) ein Meinungs- und Erfahrungsaustausch zu Grundsatzfragen statt. Den Vorsitz dieser Arbeitsgruppe hat zum 1. Januar 2002 das Hessische Ministerium des Innern und für Sport übernommen, soweit die SCHUFA betroffen ist.

### 10.2 Zustandekommen des SCHUFA-Scores, Gewichtung der Faktoren

Die Berechnung des Scores zu einer bei der SCHUFA gespeicherten Person ist weiterhin umstritten. Klarheit wird hierbei erst entstehen, wenn die SCHUFA eine von ihr in Auftrag gegebene Studie zur Wissenschaftlichkeit des Verfahrens gegenüber der Aufsichtsbehörde offen legt.
Als Faktoren für die Scoreberechnung kommen laut Aussage der SCHUFA sämtliche bei der SCHUFA gespeicherten Daten in Betracht.
Auf heftige Kritik - auch in den Medien - stieß die Einbeziehung der Selbstauskünfte in die Ermittlung des Score-Wertes. Mag es auch statistisch zutreffend sein, dass diejenigen, die besonders häufig Selbstauskünfte verlangen, schlechte Schuldner sind, so ist es für Betroffene gleichwohl nicht verständlich, dass sich die Geltendmachung ihres Auskunftsrechts gemäß BDSG negativ auswirken soll.
Auf Drängen der Aufsichtsbehörden erklärte sich die SCHUFA bereit, die Selbstauskünfte nicht mehr in die Score-Wertermittlung einzubeziehen. Die Umstellung des Verfahrens soll bis spätestens Ende Juni 2002 bei allen Vertragspartnern abgeschlossen sein, sodass Selbstauskünfte keinerlei negative Auswirkungen mehr haben.

Auf Kritik stieß jedoch auch die Gewichtung anderer Faktoren.
Ein Management-Berater mit hervorragender finanzieller Situation wandte sich an die Aufsichtsbehörde, als er erfuhr, dass er nicht - wie erwartet - einen erstklassigen Score hatte, sondern das Gegenteil der Fall war. Die häufigen berufsbedingten Umzüge hatten sich negativ auf seinen SCHUFA-Score ausgewirkt. Häufige Umzüge mögen statistisch ein Indiz für eine schlechte Zahlungsmoral sein, sie können jedoch auch einfach ein Zeichen berufsbedingter Mobilität sein. Die statistische Quasi-Gleichstellung von Management-Beratern, guten Köchen, Journalisten etc. mit flüchtigen Schuldnern war jedenfalls unbefriedigend.

Die SCHUFA hat dieses Problem erkannt und mit einer anderen Gewichtung wird die Einflussgröße von Umzügen minimiert.

Da der Score nur eine Gruppenaussage ist und über das konkrete Verhalten eines Einzelnen in dieser Gruppe nichts Definitives aussagen kann, ist - außer einer richtigen und "gerechten" Gewichtung der Faktoren - für die Betroffenen maßgeblich, dass die Vertragspartner den Score auch entsprechend verwenden, d.h. ihre Entscheidungen nicht nur auf den Score stützen, sondern dem Betroffenen ausreichend Gelegenheit geben, seinen Standpunkt geltend zu machen und seine individuelle Situation darzulegen (siehe hierzu bereits 13. Tätigkeitsbericht vom 30. August 2000, LT-Drucks. 15/1539 Nr. 6.1).

### 10.3 Auskunft über den SCHUFA-Score

Auch wenn der Score nur eine Gruppenaussage darstellt, ist es für den Betroffenen trotzdem wichtig zu wissen, welchen Score-Wert er hat, kann dieser Wert doch beispielsweise bei einer Bank die angebotenen Kreditkonditionen beeinflussen.
Erfreulicherweise hat sich die SCHUFA - entgegen der bisherigen Haltung - grundsätzlich bereiterklärt, den Kunden den aktuellen Score-Wert des Tages mitzuteilen. Im Hinblick auf das verständliche Interesse der Kunden an weitestgehender Transparenz ist dies jedoch unzureichend, weil der SCHUFA-Anschlusspartner zu einem anderen Zeitpunkt einen ganz anderen Score erhalten haben kann. Der Kunde möchte daher nicht nur den tagesaktuellen, sondern auch den tatsächlich übermittelten Score erfahren.
Die Vertreter des Zentralen Kreditausschusses (ZKA) sagten zu, dass die Banken generell über den Score-Wert Auskunft erteilen werden, wenn er bei den Banken in Dateien oder in Akten vorliegt. Besser wäre, die SCHUFA würde ihre Vertragspartner zur Beauskunftung des Scores verpflichten. Damit würde diese Auskunft auf eine breitere und verlässlichere Grundlage auch für Nichtbanken und nicht dem ZKA angeschlossene Banken gestellt.

In einem konkreten Beschwerdefall hatte die Bank der betroffenen Kundin keine Auskunft über den übermittelten Score erteilt, der bei der Ablehnung des Kreditantrages mit herangezogen worden war. Bei einer Prüfung in der Bank konnte die Aufsichtsbehörde jedoch feststellen, dass der von der SCHUFA übermittelte Score noch dokumentiert war.
In Zukunft wird - zumindest in dieser Bank - bei einem Auskunftsersuchen von Kunden auch über den vorliegenden Score Auskunft erteilt.

Ob bzw. wieweit die Beauskunftung des übermittelten Score-Wertes durch die SCHUFA-Anschlusspartner künftig sichergestellt ist, bleibt abzuwarten.

Die SCHUFA selbst lehnt die Beauskunftung dieses Wertes nach wie vor ab, da er nur aus den so genannten "logfiles" zu ermitteln sei und auch dies nur mit außerordentlich hohem Aufwand.
Daher vertritt die SCHUFA die Ansicht, dass aufgrund der §§ 34 Abs. 4, 33 Abs. 2 BDSG kein Anspruch auf eine Auskunft aus dem "logfile" bestehe, weil dieser nur der Datensicherung und Datenschutzkontrolle diene. Die gegenwärtig genutzte Software lasse die Speicherung des übermittelten Score-Wertes nicht zu.

Die Aufsichtsbehörden des Bundesgebietes sprachen sich jedoch im Rahmen der Arbeitsgruppe "Auskunfteien/SCHUFA" dafür aus, dass - ungeachtet der rechtlichen Problematik - für mehr Transparenz gegenüber den Betroffenen bzw. Verbrauchern gesorgt werden solle. Die SCHUFA sollte daher spätestens mit der Einführung einer neuen Software die übermittelten Score-Werte speichern und beauskunften.

### 10.4 Widerspruch gegen die Übermittlung des SCHUFA-Scores

Betroffene haben nicht nur ein Interesse an Transparenz bezüglich des Score-Verfahrens, sondern möchten von der Aufsichtsbehörde auch wissen, ob sie die Übermittlung eines Score-Wertes verhindern können.

Seit ca. Mitte des Berichtsjahres ermittelt und übermittelt die SCHUFA zu einem Betroffenen keinen Score-Wert, wenn er hiergegen Widerspruch einlegt. Dieser Widerspruch muss nicht begründet werden. Wenn der Betroffene nach einer Aufklärung über das SCHUFA-Verfahren den Widerspruch aufrechterhält, übermittelt die SCHUFA in Auskünften an Vertragspartner den Text "Über die angefragte Person erfolgt keine Score-Wertermittlung". Dieser Text ist laut SCHUFA notwendig, da die Vertragspartner darüber informiert werden müssten, weshalb zu einem Betroffenen, zu dem keine Negativ-Daten vorliegen, kein Score-Wert ermittelt wird.
Es wird zu beobachten sein, wie die Vertragspartner mit dieser Zusatzinformation im Rahmen von Bonitätsprüfungen umgehen.

Die Aufsichtsbehörden werden jedenfalls künftig die Betroffenen auf die Möglichkeit des Widerspruchs gegen die Score-Wertermittlung hinweisen.

### 10.5 Meldung falscher Daten an die SCHUFA

Wenn eindeutig falsche Daten der SCHUFA gemeldet werden, lässt sich der Fall sehr schnell bereinigen. In diesem Zusammenhang sind die SCHUFA-Mitarbeiterinnen und -Mitarbeiter sehr engagiert tätig.
Leider sind die von den Betroffenen gegebenen Informationen häufig unzureichend. Erst nach aufwendigen Recherchen ließ sich in einem Fall klären, dass eine zurückgewiesene Lastschrift im Zusammenhang mit einer Kreditverpflichtung eine ganz andere Bank betraf, als der Betroffene angegeben hatte. Danach konnte die negative SCHUFA-Eintragung gelöscht werden, weil die Lastschrift nicht hätte zurückgegeben werden dürfen.

In einem anderen Fall hatte eine Bank ein Sparkonto der SCHUFA als Girokonto gemeldet. Zahlreiche Girokonten können aber auch ein Indiz für hohe Überziehungskredite sein und verschlechtern deshalb auch den Scorewert. Insoweit konnte sich der Fehler der Bank negativ für den Betroffenen auswirken. Dessen ungeachtet war der SCHUFA-Eintrag auf jeden Fall falsch und daher zu löschen. Eine bloße Berichtigung (Sparkonto statt Girokonto) kam nicht in Betracht, denn Sparkonten führt die SCHUFA nicht in ihren Dateien.

Allgemein ist hierbei klarzustellen, dass die SCHUFA-Daten keine Rückschlüsse auf Vermögens- und Einkommensverhältnisse zulassen. Im Grunde enthalten die SCHUFA-Daten nur Aussagen über die möglichen Zahlungsverpflichtungen und das Zahlungsgebahren. Lediglich Hypothekarkredite geben einen Hinweis auf Immobilienbesitz.

## 11. Handels- und Wirtschaftsauskunfteien: Geschäftsgeheimnis als Auskunftsverweigerungsgrund

Mit der Neuregelung in § 34 Abs. 2 BDSG sollten die Auskunftsrechte der Betroffenen verbessert und gestärkt werden. Vor der Novelle konnten die Betroffenen von einer Auskunftei nur dann Auskunft über den Datenempfänger verlangen, wenn sie begründete Zweifel an der Richtigkeit ihrer Daten geltend machten. Nun aber ist die Verpflichtung zur Nennung des Empfängers der Auskunft nicht mehr davon abhängig, ob die erteilte Auskunft richtig oder falsch war. Die Auskunftei kann die Mitteilung des Empfängers nur verweigern, wenn das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt.
Im Beschwerdefall war die Auskunft unzutreffend und trotzdem wurde die Nennung des Empfängers zunächst unter Berufung auf das Geschäftsgeheimnis verweigert. Erst nach Intervention der Aufsichtsbehörde wurde die Auskunft erteilt. In der sich anschließenden Grundsatzdiskussion wurde dann auch anerkannt, dass bei einer fehlerhaften Auskunft immer Auskunft über den Empfänger zu erteilen ist, denn in diesem Fall geht die Interessenabwägung zwischen dem Bekanntgabeanspruch des Betroffenen und der Wahrung des Geschäftsgeheimnisses der Auskunftei immer zugunsten des Betroffenen aus.

Wenn jedoch zutreffende Auskünfte erteilt wurden, ist die Auskunftei der Auffassung, dass dann allgemein ihr Interesse an der Wahrung des Geschäftsgeheimnisses überwiege. Diese Auffassung kann von der Aufsichtsbehörde so nicht akzeptiert werden.
Die Einholung von Auskünften gehört zu den allgemeinen wirtschaftlichen Gepflogenheiten von potenziellen Gläubigern. Etwas mehr Transparenz würde hier der Auskunfteienbranche und ihren Kunden sicher nicht schaden. Würde nicht mit Kreditauskünften gearbeitet, müssten ehrliche und kreditwürdige Kunden die höheren Forderungsausfälle über die Preise mitbezahlen.
Die Verweigerung der Auskunft über den Namen des Empfängers muss deshalb in jedem Einzelfall besonders begründet werden und kann nicht pauschal unter Berufung auf das Geschäftsgeheimnis erfolgen. Bei einer Abwägung der Interessen sind nur wenige Ausnahmefälle vorstellbar, in denen das Geschäftsgeheimnis der Auskunftei im Interesse des Auskunfteienkunden eine Nennung des Auskunftsempfängers nicht zulässt, z.B. ein Verwandter des Betroffenen ist Kreditgeber.

## 12. DNA-Vaterschaftstests

Mehrere Unternehmen im Bundesgebiet bieten DNA-Vaterschaftstests an.
Bei einem solchen in Südhessen ansässigen Labor wird die erforderliche DNA-Probe überwiegend aus einem Speichelabstrich der Mundschleimhaut an der Innenseite der Wangen gewonnen. In der Regel nimmt das Unternehmen die Probe nicht selbst, vielmehr legt der Auftragnehmer sie vor bzw. sendet sie per Post zu, nachdem das Unternehmen ihm das Testmaterial (steriles Wattestäbchen etc.) zugesandt hat.
Als Ausgangsmaterial für die DNA-Analyse kann auch Speichel von anderen "Trägern" (Trinkglas, Zahnbürste etc.), ausgerissene Haare oder Blut verwendet werden.

Die Problematik dieser Tests besteht zunächst darin, dass selbst Unbeteiligte, also die neugierige Verwandtschaft oder Bekanntschaft, die Tests veranlassen könnten. Eine Identitätsprüfung findet nicht statt, d.h. das Unternehmen prüft nicht einmal, ob der Auftraggeber derjenige ist, von dem die eine DNA-Probe stammt. Der Vertrag enthält daher die Klausel, dass die Verantwortung für die Identität der Testperson beim Auftraggeber liegt. Zwar werden zu einem Großteil die Proben mit einem Identitätsnachweis eines Jugendamtes oder Arztes vorgelegt, aber das Labor lehnt andere Tests keinesfalls ab. Es lässt sich lediglich durch vorformulierte Vertragsklauseln versichern, dass die Proben von den anzugebenden Personen stammen und die Teilnahme am Test durch alle Beteiligten freiwillig sei.

Das weitere grundsätzliche Problem liegt darin, dass die Tests nicht im Rahmen der gesetzlich vorgesehenen Verfahren für eine Vaterschaftsanfechtung oder Vaterschaftsfeststellung erfolgen. Dies berührt auch die Frage, ob das Wohl des Kindes verletzt wird, wenn die gesetzlichen Sorgeberechtigten nicht zugestimmt haben.

Die Problematik kann mit den bestehenden Regelungen des BDSG nicht zufriedenstellend bewältigt werden.

Eine klare gesetzliche Regelung - wie von der 62. Datenschutzkonferenz der Datenschutzbeauftragten des Bundes und der Länder bereits vorgeschlagen - ist daher dringend erforderlich.

## 13. Gesundheitswesen

### 13.1 Datenerhebung im Wartezimmer

Die Verarbeitung und Nutzung von Gesundheitsdaten als besondere Arten personenbezogener Daten nach § 3 Abs. 9 BDSG ist mit der Novellierung des BDSG stärker eingegrenzt worden als zuvor. Die mangelnde Umsetzung dieser neuen, aber auch der bisherigen Vorgaben im Klinik- oder Praxenalltag führt jedoch immer wieder zu Eingaben von Betroffenen an die Aufsichtsbehörde.

So zeigte ein Patient an, dass ihn vor einem operativen Eingriff die für die Praxis tätige Narkoseärztin im Wartezimmer der Praxis im Beisein anderer Patienten über die Risiken des Eingriffs aufgeklärt, ihn zu seinen Vorerkrankungen befragt und die Daten dort aufgenommen habe.
Die Praxis bezeichnete dies als bedauerlichen Ausnahmefall, da die Narkoseärztin einen eigenen Raum in der Praxis für diese Zwecke habe.

### 13.2 Unbefugte Datenübermittlungen im Zusammenhang mit der Einholung einer Zweitbeurteilung

Eine für den Betroffenen vermeintlich nützliche Weitergabe seiner Gesundheitsdaten ist zu beanstanden, wenn der Betroffene darin nicht eingewilligt hat. Ein Betroffener schrieb eine Privatklinik mit der Frage an, ob diese seine Röntgenaufnahmen, die in einer anderen Klinik gemacht wurden, begutachten könne. Er wollte diese Aufnahmen dann gegebenenfalls ohne die ursprüngliche Bewertung einreichen, um eine weitere unabhängige Beurteilung zu erhalten.

Die Privatklinik schaltete auf diese Anfrage hin, ohne den Betroffenen zu informieren, eine Röntgenärztin ein, deren Praxis sich ebenfalls im Gebäude der Privatklinik befand und mit der die Klinik hin und wieder zusammenarbeitete. Diese forderte wiederum ohne Rücksprache mit dem Betroffenen die Röntgenunterlagen bei der anderen Klinik an. Die Unterlagen wurden ihr samt ursprünglicher Bewertung übermittelt. Nicht nur ärgerlich für den Betroffenen, dass damit eine zweite unabhängige Beurteilung unmöglich wurde, sondern auch, dass seine Daten unbedarft an die ihm unbekannte Röntgenärztin und die andere Klinik übermittelt wurden.

Fazit dieses Vorfalls war, dass das Fehlen betrieblicher Datenschutzbeauftragter und die fehlende Schulung der Klinik- bzw. Praxismitarbeiter Auslöser für den fehlerhaften Umgang mit Gesundheitsdaten war. In der Klinik und Praxis waren umgehend die erforderlichen Maßnahmen zur Sicherung des Datenschutzes, insbesondere zur Beachtung des Einwilligungserfordernisses, zu ergreifen.

### 13.3 Externe Archivierung von Patientendaten

Auch die Archivierung von Patientendaten aus Arztpraxen durch einen externen Archivar erweist sich weiterhin als problematisch, auch dann, wenn der Archivar selbst Arzt ist. Der Archivar ist nicht in das Behandlungsgeschehen wie ein Praxisgehilfe oder mitbehandelnder Arzt einbezogen, sodass er im Regelfall keine Befugnis zur Kenntnisnahme der Daten besitzt. Im Hinblick auf § 203 StGB musste einem Arzt, der anfragte, ob er die Archivierung unter anderem für andere Arztpraxen durchführen könne, daher mitgeteilt werden, dass dies nur nach vorheriger Verschlüsselung der Patientendaten oder nach dem "Zwei-Schlüssel-System" zulässig ist. Dabei spielt es keine Rolle, ob die Archivierung als Auftragsdatenverarbeitung im Sinne des § 11 BDSG ausgestaltet ist, denn § 203 StGB differenziert nicht zwischen einer Übermittlung und einer Weitergabe an einen Auftragsdatenverarbeiter.

Zu beachten ist allgemein auch, dass der Beschlagnahmeschutz des § 97 StPO für Patientendaten bei einer externen Archivierung möglicherweise nicht gesichert ist.

## 14. Datenverarbeitung in Vereinen und Verbänden

### 14.1 Übermittlung von Mitgliederdaten an Versicherungsunternehmen trotz Widerspruchs

Viele Vereine arbeiten aus wirtschaftlichen Gründen über ihre Dachverbände auf Bundes- und Landesebene mit Versicherungskonzernen zusammen und bieten ihren Mitgliedern günstige Versicherungstarife an, die über den Abschluss von Gruppenversicherungsverträgen erreicht werden können. Um in den Genuss dieser günstigen Tarife kommen zu können, muss dabei oftmals eine bestimmte Anzahl von Mitgliedern überzeugt werden, entsprechende Einzelverträge abzuschließen. Daher wird für den Abschluss solcher Versicherungsverträge in den Vereinen und Verbänden intensiv geworben.

Für die datenschutzrechtliche Zulässigkeit der Übermittlung der Mitgliederdaten vom Verein an die Versicherung bedarf es grundsätzlich einer Einwilligung der Betroffenen, da § 28 BDSG diese Übermittlung personenbezogener Daten aus dem vertragsähnlichen Vertrauensverhältnis zwischen Mitglied und Verein heraus üblicherweise nicht abdeckt. In der Regel können die Mitglieder sofort bei Vereinseintritt der Übermittlung ihrer Daten an die Versicherungsunternehmen ihre Zustimmung verweigern, indem sie die auf dem Eintrittsformular entsprechend vorgesehene Einwilligungserklärung nicht unterschreiben. Mitglieder, die zunächst ihre Einwilligung erteilt hatten und dann später keine Angebote und Werbung der Versicherung oder Haustürbesuche der Versicherungsvertreter mehr erhalten möchten, können die Einwilligung jederzeit widerrufen.

Durch die Beschwerden betroffener Vereinsmitglieder erhielt das Regierungspräsidium Darmstadt davon Kenntnis, dass ein großer hessischer Dachverband mit Sitz in Frankfurt am Main die Mitglieder in allen hessischen Ortsvereinen angeschrieben hatte, die in den Jahren zuvor ihre Einwilligung in die Übermittlung ihrer Daten an den Gruppenversicherungspartner verweigert bzw. diese später widerrufen oder der Übermittlung nach § 28 Abs 3 BDSG a.F. widersprochen hatten und deren Datensatz daher in der Mitgliederdatei des Verbandes mit einer Übermittlungssperre gekennzeichnet war. In diesem Schreiben wurde den Mitgliedern mitgeteilt, dass man es sehr bedauere, dass die für eine Übermittlung der Mitgliederdaten an die Versicherung erforderliche Einwilligung nicht vorliege bzw. noch ein Übermittlungswiderspruch bestehe. Immerhin habe der Versicherer doch äußerst günstige Angebote zu machen. Daher würden die Mitgliederdaten jetzt trotz des bestehenden Sperrvermerks an die Versicherung übermittelt, falls nicht innerhalb von vier Wochen ein Widerspruch gegen dieses Vorhaben des Verbandes erfolge.

Die Datenschutzaufsichtsbehörde beurteilte dieses Vorgehen des Landesverbandes als eklatante Missachtung des informationellen Selbstbestimmungsrechtes der betroffenen Vereinsmitglieder. Eine Einwilligung in die Datenübermittlung, die bei Vereinseintritt bewusst verweigert wurde, kann auf keinen Fall durch das spätere Unterlassen eines Übermittlungswiderspruchs ersetzt werden. Aber auch in den Fällen, bei denen zunächst eine Einwilligung erteilt wurde, das Mitglied später aber diese widerrufen bzw. gegen die Datenübermittlung an die Versicherung Widerspruch eingelegt hatte, kann der Widerruf/Widerspruch nicht mit einem einfachen Ankündigungsschreiben übergangen werden. Um eine erfolgte Willensänderung deutlich zu machen, bedarf es immer eines aktiven Handelns des betroffenen Vereinsmitgliedes. Die Nicht-Reaktion auf ein entsprechendes Anschreiben genügt jedenfalls nicht.

Obwohl dem Verband die Rechtslage deutlich geschildert wurde und die Versicherung die Aufforderung erhielt, bereits übermittelte Mitgliederdaten nicht werblich zu nutzen, sondern umgehend zu löschen, erfolgte zunächst nur eine unzureichende Reaktion des Landesverbandes. Erst nach der Ankündigung, bei weiteren Verzögerungen die für den Hauptsitz der Versicherung lokal zuständige Datenschutzaufsichtsbehörde mit dem Fall zu befassen und nach einem persönlichen Gespräch mit dem Datenschutzbeauftragten des Landesverbandes und dem Versicherungsunternehmen wurde das Versenden der fragwürdigen Anschreiben eingestellt. Die bereits übermittelten Daten wurden gelöscht.

Auch in Zeiten des Mitgliederschwunds und knapper Vereinskassen rechtfertigt das wirtschaftliche Interesse an der Vermarktung der Daten von Vereinsmitgliedern nicht die Missachtung der datenschutzrechtlichen Interessen der Vereinsmitglieder.

### 14.2 Unzulässige Mitglieder- und Spendenwerbung und andere Missstände

Auf die Datenverarbeitung einer bundesweit tätigen gemeinnützigen Organisation bzw. deren örtlicher Untergliederungen wurde die Aufsichtsbehörde aufgrund von Betroffeneneingaben aufmerksam.
Diese Organisation ist in mehrere Landesverbände gegliedert. Die Landesverbände enthalten ihrerseits selbständige Untergliederungen. Die Beschwerden richteten sich gegen zwei benachbarte eigenständige Organisationseinheiten (Vereine).

Zum einen fühlten sich die Betroffenen durch unaufgeforderte Telefonanrufe belästigt, mit denen für eine Vereinsmitgliedschaft bzw. eine Spende geworben wurde. Zum anderen befürchteten sie, dass ihre persönlichen Daten unberechtigt an unbekannte Dritte übermittelt worden seien. Auf die Frage, woher die Anruferin ihren Namen und ihre Telefonnummer kenne, hatten sie nämlich die Antwort erhalten, dass die Daten von einem Krankenhaus stammten.

Die von der Aufsichtsbehörde angeschriebenen Vereine reagierten zunächst sehr zäh bzw. überhaupt nicht. Von einem Geschäftsführer erhielt die Aufsichtsbehörde ein kurzes Schreiben, welches nicht die Fragen beantwortete, sondern nur kurz erläuterte, dass zur Mitgliederwerbung eine Marketing-Aktion erfolgt sei, was wohl nichts Anrüchiges sei. Auf das erneute Anfragen erhielt die Aufsichtsbehörde ein Schreiben als Antwort, welches inhaltlich aus Fragen bestand, u.a. inwieweit die Aufsichtsbehörde nochmals mit weiteren Fragen zur Last fallen wolle. Um weiteren unergiebigen Schriftwechsel zu verhindern, beraumte die Aufsichtsbehörde kurzfristig einen Termin für eine Datenschutzüberprüfung an.

Die Überprüfung brachte mehrere gravierende Versäumnisse zum Vorschein:

Zwar konnte der Verdacht, dass die Daten für die Telefonwerbeaktion bei einem Krankenhaus erhoben worden seien, ausgeräumt werden. Dies war eine bloße Behauptung einer Mitarbeiterin des vom Verein beauftragten Call-Centers gewesen. Tatsächlich waren die Daten einfach aus dem örtlichen Telefonbuch entnommen worden.

Aber die Anrufe selbst waren als so genanntes "kaltes Telefon-Marketing" zu bewerten und damit wettbewerbsrechtlich unzulässig. Da eine wettbewerbswidrige Nutzung personenbezogener Daten mit den schutzwürdigen Belangen der Betroffenen nicht vereinbar ist, lag somit auch eine unzulässige Datennutzung vor.

Ferner hatte der Verein entgegen seiner mindestens seit 1990 bestehenden Verpflichtung keinen betrieblichen Datenschutzbeauftragten bestellt. Noch während der Prüfung lehnte die damalige Geschäftsleitung eine Bestellung aus Kostengründen ab. Darüber hinaus lagen noch weitere Unzulänglichkeiten vor, die aufgedeckt werden konnten.
Lobend zu erwähnen ist allerdings die ausführliche und fast aktuelle Dokumentation der Datenverarbeitung. Diese Dokumentation kann eine gute Grundlage für die Tätigkeit eines Datenschutzbeauftragten darstellen.

Die Telefonaktion wurde aufgrund der Beanstandung durch die Aufsichtsbehörde eingestellt. Auch ein betrieblicher Datenschutzbeauftragter wurde schließlich bestellt.

Dies geschah allerdings kaum aus Einsicht der Geschäftsleitung, sondern weil nach der Prüfung mit den Vorbereitungen zur Einleitung eines Ordnungswidrigkeitenverfahren wegen der Nichtbestellung eines betrieblichen Datenschutzbeauftragten begonnen worden war. Bei einem Verein ist nicht die tätige Geschäftsleitung in erster Linie für die Einhaltung der Vorschriften des BDSG verantwortlich, sondern der Vorstand, vertreten durch den Vorsitzenden. Dies ist unabhängig davon, ob der Vorstand ehrenamtlich tätig ist oder nicht.

Auch der zweite Verein musste vor Ort einer Datenschutzüberprüfung unterzogen werden, da auch von dortiger Stelle keine ausreichenden Antworten auf Schreiben der Aufsichtsbehörde erteilt wurden. Hier stellte sich heraus, dass zwar eine recht ordentlich organisierte Datenverarbeitung vorhanden war, aber Sicherheitsaspekte leider keine Rolle spielten und das Thema Datenschutz bisher unbekannt war. Hier wurde die Nichtbestellung eines betrieblichen Datenschutzbeauftragten damit begründet, dass seit Jahren nach einem geeigneten Mitarbeiter zur Wahrnehmung dieser Tätigkeiten gesucht wurde. Diese Erklärung war weder plausibel noch akzeptabel; erfreulicherweise bestand jedoch Einsicht, nun unverzüglich für Abhilfe zu sorgen.

Die Aufsichtsbehörde wird - auch nach Bestellung eines betrieblichen Datenschutzbeauftragten - die Angelegenheit nicht zu den Akten legen, sondern

von Zeit zu Zeit nachfragen und nach Möglichkeit erneut Überprüfungen durchführen.

Mittlerweile ist auch der Landesverband an die Aufsichtsbehörde mit der Bitte um Unterstützung herangetreten. Es wurde vereinbart, dass die Aufsichtsbehörde für ein Datenschutz-Seminar zur Verfügung steht. Dieses wurde 2002 durchgeführt und fand große Resonanz. Insgesamt ist davon auszugehen, dass man sich nun ernsthaft des Themas Datenschutz annimmt.

### 14.3 Datenerhebung beim Verkauf von Eintrittskarten zu großen Sportveranstaltungen

Bei großen Sportereignissen, wie z.B. Weltmeisterschaften, sind die deutschen Verbände beim Ticketverkauf an die Vorgaben der Europäischen- bzw. Welt-Verbände gebunden.

Diese Abhängigkeit sowohl von örtlichen Veranstaltern in Drittländern wie auch von Weltverbänden darf jedoch nicht dazu führen, dass ohne Überprüfung im Rahmen des Kartenvorverkaufs personenbezogene Daten verarbeitet werden, die über das erforderliche Maß hinausgehen.

Aufgrund bereits bestehender Kontakte bat ein Verband die Aufsichtsbehörde um Rat, bevor er die Bestellbedingungen in der Öffentlichkeit bekannt gab. Der Weltverband hatte vorgegeben, dass die Personalausweisnummern bzw. Passnummern auf jeden Fall zu erheben und an den Weltverband und die örtlichen Ausrichter in einem Drittstaat zu übermitteln seien. Daneben beinhaltete die vorgelegte Einwilligungserklärung, dass der Betroffene sich auch mit der Nutzung seiner Daten für Werbezwecke einverstanden erklären müsse.

Eine derartige Einwilligung ist unzulänglich bzw. unwirksam.

Aufgrund der Kritik der Aufsichtsbehörde fragte der deutsche Verband nochmals beim Weltverband nach dem Zweck der Verarbeitung der Ausweisnummern und der vorgesehenen Verwendung der Daten für Werbezwecke. Dabei stellte sich heraus, dass nur dann, wenn sich an einem Veranstaltungsort erhebliche Vorfälle ereignen, unter Umständen anhand der Ausweisnummern Personen identifiziert oder verfolgt werden sollen. Zu Werbezwecken wollte der Weltverband Daten von Ticketkäufern nur nutzen, wenn die Bestellungen direkt bei ihm eingegangen waren. Der deutsche Verband hatte nicht vor, die Kartenbesteller bzw. Käufer, die über ihn Karten beziehen wollten, in seine eigene Werbedatei zu übertragen. Es konnte einvernehmlich ein Kompromiss gefunden werden. Die Ausweisnummern mussten zwar angegeben werden, denn an dieser Bedingung hielt der Weltverband fest, doch werden diese nur bis zum Abschluss der Veranstaltung in dem Datenbestand des nationalen Verbandes gespeichert und nicht automatisch an den Weltverband oder andere Stellen übermittelt. Auf diese Weise besteht immer noch die Möglichkeit des Rückgriffs, falls ein besonderes Ereignis dies erforderlich macht. Der Passus hinsichtlich der Nutzung für Werbezwecke konnte entfallen. Da die Gespräche zwischen Verband und Aufsichtsbehörde rechtzeitig vor dem Ticketverkauf stattgefunden hatten, konnten die Verkaufsunterlagen noch ohne wirtschaftlichen Nachteil geändert werden.

### 14.4 Sponsor bewirbt Vereinsmitglieder

Der Sponsor eines Sportverbandes wollte den Versand von Informationen des Verbandes finanzieren und die Vereinsmitglieder zugleich über seine eigenen Produkte informieren. Die Aufsichtsbehörde war der Ansicht, dass dem Sponsor nicht die Adressen der Vereinsmitglieder übermittelt werden sollten, sondern dass in diesem Fall die Versendung im Lettershop-Verfahren eine weniger eingreifende Alternative im Verhältnis zur direkten Adressenübermittlung an den Sponsor darstellte.

### 14.5 Bundesverband verwaltet Mitgliederdateien

Der übergeordnete Bundesverband von zahlreichen Wassersportvereinen überwachte den Zugang und Abgang von Vereinsmitgliedern dadurch, dass nur der Bundesverband in den Mitgliederdateien der Vereine Löschungen vornehmen konnte. Der Zweck dieser Beschränkung lag darin, die Abführung von Beiträgen an den Bundesverband sicherzustellen, die nach der An-

zahl der Vereinsmitglieder berechnet wurden. Verschiedentlich hatten Vereine nämlich durch Manipulation der Anzahl von Mitgliedern versucht, Beiträge zu sparen.

Da in den jeweiligen Vereinssatzungen festgelegt war, dass der Bundesverband die Mitgliederdateien verwaltet und zugleich weitere Aufgaben für die Vereine erfüllt, war diese zentrale Datenverarbeitung an sich nicht zu beanstanden.

Durch die Zugriffsbeschränkungen für die Vereine wurden nun aber dauerhaft Personen in den laufenden örtlichen Mitgliederdateien aufgeführt, die seit langem nicht mehr dem Verein angehörten, weil sie z.B. ausgetreten waren. Die Vereine übermittelten immer wieder die nicht aktualisierten Mitgliederdateien an den Bundesverband, in der sie zwar Austrittsvermerke angebracht hatten, aber die Namen der ausgeschiedenen Mitglieder noch stets in den Dateien enthalten waren. Auch für ihre eigene Vereinsarbeit stand ihnen immer nur die mit Austrittsvermerken versehene, nicht aktualisierte Version der Mitgliederdatei zur Verfügung.
Die Aufsichtsbehörde wies darauf hin, dass die Vereine verpflichtet sind, die Daten der ausgeschiedenen Mitglieder nach einem angemessenen Zeitraum zu löschen. Wenn der Bundesverband die Kontrolle über die ordnungsgemäße Einmeldung von Mitgliederzahlen behalten will, muss er den einzelnen Vereinen die Erfüllung der Löschungsverpflichtung ermöglichen. Dies muss durch regelmäßige Übermittlung der aktuellen Datenbestände an die Vereine geschehen, was per verschlüsselter E-Mail oder Diskette erfolgen kann.

### 14.6 Daten von Kindern im Internet

Als ebenfalls unzulässig bewertete die Aufsichtsbehörde die Veröffentlichung der Namen und Geburtsdaten von Kindern, die die Kinderturngruppe eines Sportvereins besuchten. Die Veröffentlichung erfolgte dabei auf der Homepage des Sportvereins, ohne dass die Eltern eingewilligt hatten. Die Beschwerden der Eltern waren völlig berechtigt.

## 15. Die tägliche Missachtung von Verbraucherrechten in der Werbebranche

Ein Aufgabengebiet der Datenschutzaufsichtsbehörden, in dem es leider in jedem Berichtsjahr wieder zu Beanstandungen bei verarbeitenden Stellen und ihren EDV-Dienstleistungsunternehmen kommt, ist die Bearbeitung von Beschwerden und Hilferufen von Verbrauchern, die Unterstützung bei der Durchsetzung ihrer gesetzlichen Rechte bei Werbetreibenden oder Spezialunternehmen der Werbewirtschaft (Adresshändler, Listbroker, Lettershops, Werbeagenturen) benötigen.

Wie schon mehrfach berichtet (siehe 13. Tätigkeitsbericht vom 30. August 2000, LT-Drucks. 15/1539 Nr. 13), halten es Werbetreibende, die personalisierte Werbe-Mailings versenden oder von beauftragten Dienstleistern versenden lassen, immer wieder für nicht erforderlich, die Herkunftsanfragen (§ 34 Abs. 1 BDSG) und Widersprüche (§ 28 Abs. 3 BDSG a.F. bzw. Abs. 4 BDSG n.F.) von Umworbenen zu beantworten. Diese sehen in der Datenschutzaufsichtsbehörde dann die letzte Möglichkeit zu erfahren, wie ihre Adresse in den gewerblichen Adresshandel eingebracht wurde, oder zu erreichen, dass ihre Namen und Anschriften nicht mehr für die Versendung unerwünschter Werbungen benutzt werden. Die Datenschutzaufsichtsbehörde hat üblicherweise - spätestens nach Androhung eines Bußgeldverfahrens wegen der Nichterteilung von Auskünften nach § 43 Abs. 1 Nr. 10 BDSG gegen den Geschäftsführer des werbenden Unternehmens - weniger Probleme, bei den verantwortlichen Stellen Gehör zu finden.

Von diesen Beschwerden sind so gut wie alle Wirtschaftszweige betroffen. Sowohl kleine Einzelhändler als auch große Versicherungen und Telekommunikationsanbieter sind darauf angewiesen, personalisierte Werbung zu betreiben.

Leider zeigt die Erfahrung der Aufsichtsbehörde, dass die Einhaltung datenschutzrechtlicher Vorschriften durch Direktmarketingunternehmen vom Auftraggeber oftmals gar nicht kontrolliert wird, obwohl dieser selbst nach § 11 Abs. 1 BDSG für die Einhaltung der datenschutzrechtlichen Vorschriften bei

den Auftragnehmern verantwortlich bleibt. Während der Gesetzgeber davon ausgeht, dass die betrieblichen Datenschutzbeauftragten der beteiligten Unternehmen die Marketing-Experten datenschutzrechtlich unterstützen, musste die Datenschutzaufsichtsbehörde feststellen, dass die Unternehmen gar keine Datenschutzbeauftragten bestellt hatten, die z.B. am Vertragstext mitarbeiten oder die an der Abwicklung von Mailings beteiligten Mitarbeiter unterweisen und schulen könnten.

In allen Beschwerdefällen konnte die Datenschutzaufsichtsbehörde zur Klärung der Adressherkunft beitragen und den Petenten die gewünschten Auskünfte verschaffen. Als Nebeneffekt der Beschwerdebearbeitung wurden in einigen südhessischen Betrieben betriebliche Datenschutzbeauftragte nach §§ 4f, 4g BDSG bestellt, deren eigene Schulung und Ausbildung sowie deren künftige Tätigkeit im Betrieb von der Datenschutzaufsichtsbehörde stichprobenartig kontrolliert werden wird.

Bei den Beschwerdefällen, die unter Gültigkeit des neuen BDSG mit seinen höheren Anforderungen an die Werbewirtschaft eingingen, musste festgestellt werden, dass der seit Mai 2001 nach § 28 Abs. 4 Satz 2 BDSG vorgeschriebene Hinweis auf das Widerspruchsrecht in den Werbeschreiben nie enthalten war. Es blieben auch berechtigte Zweifel daran bestehen, ob die für die jeweilige Werbung verantwortliche Stelle wirklich im Sinne des § 28 Abs. 4 Satz 2, 2. Halbsatz BDSG sichergestellt hatte, dass Betroffene auch beim Listbroking-Verfahren Auskunft über die Herkunft ihrer Daten erhalten können. Die Datenschutzaufsichtsbehörde nimmt natürlich Rücksicht darauf, dass Unternehmen immer eine gewisse Zeit zur Umsetzung neuer gesetzlicher Regelungen benötigen und ist bemüht, die verarbeitenden Stellen nicht über Gebühr zu belasten. Es kann allerdings nicht ohne Konsequenzen bleiben, wenn Werbetreibende und ihre Direktmarketing-Unternehmen nach mehr als einem Jahr immer noch nicht die gesetzliche geforderte Unterrichtung nach § 28 Abs. 4 Satz 2 BDSG vornehmen. Dies gilt insbesondere für einen Unterlassungstatbestand, der nach dem neuen Ordnungswidrigkeitentatbestand des § 43 Abs. 1 Nr. 3 BDSG mit einem Bußgeld bis zu 25.000 € geahndet werden kann.

Der deutsche Direktmarketingverband (Sitz in Wiesbaden) hat für seine Mitglieder einen Leitfaden zur Umsetzung der neuen Vorschriften erstellt.

Dieser kann grundsätzlich als Verhaltensregel im Sinne des § 38a BDSG bewertet werden. Wenngleich die Aufsichtsbehörde inhaltlich in einigen Punkten nicht mit dem Verband übereinstimmt und daher die Diskussionen nicht abgeschlossen sind, ist dies doch ein hoffnungsvoller Ansatz, um zu einer besseren Beachtung der neuen Vorgaben beizutragen.

Der Verband beabsichtigt, den Leitfaden zu überarbeiten, dessen Bewertung im nächsten Bericht dargestellt werden wird.

## 16. Öffentliche Telekommunikationsverzeichnisse

Im Berichtszeitraum gingen mehrfach Beschwerden von Telekommunikationsteilnehmern ein, deren Teilnehmerdaten in verschiedenen öffentlichen Verzeichnissen erstmals oder erneut eingetragen worden waren, obwohl sie dem nicht zugestimmt oder widersprochen hatten, deren Löschungsantrag nicht berücksichtigt worden war oder die mit falschen Verbindungsdaten eingetragen worden waren.
Der im Aufsichtsbezirk ansässige Verlag machte zunächst allgemein die Nichtaufklärbarkeit der Beschwerdefälle geltend.
Im nachfolgenden Gespräch mit der Aufsichtsbehörde stellte sich heraus, dass der Verlag, der die Teilnehmerdaten täglich online von dem Telekommunikationsanbieter zur Aktualisierung der Verzeichnisse überspielt bekommt, durch das automatisierte Verfahren keine Einfluss- bzw. Kontrollmöglichkeiten auf diese Daten hat und der vom Bundesbeauftragten für den Datenschutz überwachte Telekommunikationsanbieter für die korrekte Aufnahme der Teilnehmerdaten bzw. die Abwicklung von Löschungs- oder Änderungswünschen verantwortlich ist.

## 17. Der betriebliche Datenschutzbeauftragte

### 17.1 Vertragslaufzeit für die Dienstleistung eines externen Datenschutzbeauftragten

Die Bestellung interner betrieblicher Datenschutzbeauftragter darf nach § 4f Abs. 3 Satz 3 BDSG nur aus wichtigem Grund entsprechend § 626 BGB widerrufen werden. Damit dieser Widerrufsschutz nicht unterlaufen wird, darf die Bestellung auch nur bei Vorliegen eines wichtigen Grundes befristet werden. Ein solcher läge beispielsweise vor, wenn der ursprünglich bestellte Datenschutzbeauftragte wegen Krankheit, Erziehungsurlaub etc. längerfristig verhindert ist und nur ein zeitweiliger Ersatz bestellt werden soll.

Bei externen betrieblichen Datenschutzbeauftragten ist die Rechtslage nicht so eindeutig.
Teilweise wird die Auffassung vertreten, externe Datenschutzbeauftragte könnten sich nicht auf den Widerrufsschutz des § 4f Abs. 3 Satz 3 BDSG berufen und die Bestellung bzw. der Vertrag könne beliebig befristet werden (Helfrich in Ehmann, Der Datenschutzbeauftragte im Unternehmen: Funktion, Stellung, Berufsbild; Köln 1993).

Nach gegenteiliger Meinung hingegen sind interne und externe Datenschutzbeauftragte gleich zu behandeln.
Zum Teil wird zwischen Dienstverträgen und Werkleistungsverträgen mit externen Beratungsfirmen differenziert.
Eine "vermittelnde" Meinung hält zwar den Widerrufsschutz auch bei externen Datenschutzbeauftragten für gegeben, ist bezüglich der Befristung jedoch großzügiger und betrachtet diese als Regelfall, allerdings müsse eine Mindestfrist von fünf Jahren vereinbart werden (vgl. Bergmann/Möhrle/Herb, § 36 Rn. 43; zum gesamten Streitstand siehe Schlemann, Recht des betrieblichen Datenschutzbeauftragten; Köln 1996).

Angesichts dieser Meinungsvielfalt wird die Aufsichtsbehörde immer wieder von externen Datenschutzbeauftragten um Stellungnahme gebeten, welche Auffassung sie denn vertrete. Dabei ging es stets um Datenschutzbeauftragte, die aufgrund Dienstvertrages tätig waren.

Die Aufsichtsbehörde teilt die oben genannte "vermittelnde" Meinung. Da § 4f Abs. 3 Satz 3 BDSG nicht zwischen externen und internen Datenschutzbeauftragten differenziert, gilt der Widerrufsschutz gleichermaßen.

Andererseits ist das Interesse eines Unternehmens, bezüglich der Organisation des Datenschutzes eine gewisse Flexibilität zu behalten und sich daher nicht unbefristet an einen externen Datenschutzbeauftragten zu binden, berechtigt.
Aus der Aufsichtspraxis sind beispielsweise Fälle bekannt, in denen ein Unternehmen nun die Bestellung eines internen Datenschutzbeauftragten, statt des vor vielen Jahren bestellten externen Datenschutzbeauftragten, wegen der räumlichen Nähe zur Datenverarbeitung bevorzugen würde oder das Unternehmen aufgrund der Internationalisierung des Unternehmens nun einen Datenschutzbeauftragten wünscht, welcher die Schulungen auch in englischer Sprache halten und englische Vertragstexte etc. bewerten könnte. In diesen Fällen ist zweifelhaft, ob ein wichtiger Grund im Sinne des § 4f Abs. 3 Satz 3 BDSG zur Abberufung des externen Datenschutzbeauftragten vorläge. Gleichwohl ist es verständlich, dass ein Unternehmen nicht auf unbegrenzte Dauer an einen externen Datenschutzbeauftragten gebunden sein will.

Daher ist eine Befristung gerechtfertigt und sinnvoll. Eine Frist von fünf Jahren erscheint als sinnvolle Richtschnur. Unberührt bleibt die Möglichkeit einer kürzeren Befristung, wenn von vornherein entsprechende wichtige sachliche Gründe hierfür vorliegen (wie der oben genannte Vertretungsfall).

Auch das Interesse, sich ein genaues Bild über die Kenntnisse und Fähigkeiten des externen Datenschutzbeauftragten zu verschaffen, kann die Vereinbarung einer kurzfristigen Probezeit rechtfertigen. Keinesfalls vertretbar wären aber Kettenverträge von jeweils kurzer Laufzeit.

### 17.2 Betriebsrat als Datenschutzbeauftragter

Ein Datenschutzbeauftragter eines mittelständischen Unternehmens wandte sich mit der Bitte um Unterstützung in einer speziellen Problematik an die Aufsichtsbehörde. Er begrüßte den Vorschlag der Aufsichtsbehörde, zunächst eine allgemeine Datenschutzüberprüfung nach § 38 BDSG im Unternehmen durchzuführen. Während der Überprüfung im Unternehmen stand er selbst bedauerlicherweise nicht zur Verfügung. Er hatte sich aber dennoch mit dem Termin der Überprüfung vor Ort einverstanden erklärt.

Die Vertreter des Unternehmens erteilten alle Auskünfte in ausreichender Form. Bei der Überprüfung vor Ort musste die Aufsichtsbehörde erstaunt feststellen, dass der Datenschutzbeauftragte seine Tätigkeit völlig unzureichend wahrgenommen hatte. Seit mehr als zehn Jahren war der betriebliche Datenschutzbeauftragte nicht nur als Beauftragter für den Datenschutz bestellt, sondern gleichzeitig Vorsitzender des Betriebsrates des Unternehmens gewesen. Er war für die Tätigkeit als Betriebsratsvorsitzender freigestellt. In all diesen Jahren wurden keine Schulung und keine Maßnahme zur Unterrichtung der Mitarbeiter hinsichtlich Maßnahmen zum Datenschutz und zur Datensicherheit im Unternehmen ausgeführt. Weder eine Prüfung der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen, mit deren Hilfe personenbezogene Daten verarbeitet werden, hatte stattgefunden, noch konnte der Datenschutzbeauftragte auf einen Dateiennachweis oder sonstige Dokumentationen zur Datenverarbeitung zugreifen. Der Dateiennachweis war nicht versäumt worden, weil das Unternehmen sich dagegen gesperrt hätte, sondern weil der Datenschutzbeauftragte einen solchen nicht angefordert hatte. Bei einem schwerwiegenden Verstoß gegen Datensicherheitsvorschriften im Unternehmen (missbräuchliche Verwendung von Passworten) war der Datenschutzbeauftragte von der Geschäftsführung schriftlich über die Angelegenheit informiert worden und um eine Überprüfung gebeten worden. Auch hier erfolgte keinerlei Reaktion des Datenschutzbeauftragten.

Unterlagen, die der Datenschutzbeauftragte der Aufsichtsbehörde über seine Tätigkeit und seine Aus- und Fortbildung zur Akte nachreichte, waren mehr als fünf Jahre alt. Die Unterlagen selber enthielten lediglich Hinweise, die von der Gewerkschaft veröffentlicht oder den Betriebsräten zur Verfügung gestellt worden waren. Diese behandelten nur den Arbeitnehmerdatenschutz in allgemeiner Form. Auch die vorgelegten Betriebsvereinbarungen enthielten gar nur unzulängliche Regelungen zum Datenschutz. Für die Aufsichtsbehörde insgesamt ein niederschmetterndes Ergebnis. In diesem Fall zeigte sich, dass der Mitarbeiter durch seine Tätigkeit als Vorsitzender des Betriebsrates dermaßen ausgelastet schien, dass ihm überhaupt keine Zeit mehr für eine Tätigkeit als Datenschutzbeauftragter verblieb. Daneben war er der Auffassung - und dies zeigt sich bedauerlicherweise häufig bei Betriebsräten -, dass die Tätigkeit nach dem Betriebsverfassungsgesetz wesentlich wichtiger sei als die Wahrnehmung der Aufgabe als Datenschutzbeauftragter. Auch wird in derartigen Fällen oft übersehen, dass der Datenschutz in einem Unternehmen sich nicht ausschließlich auf Mitarbeiterdaten bezieht, sondern dass auch Daten von Kunden, Lieferanten, Interessenten und weitere Daten, soweit sie personenbeziehbar sind, den Regelungen des Datenschutzgesetzes unterliegen.

Der konkrete Fall warf die auch in anderem Zusammenhang häufig an die Aufsichtsbehörde gestellte Frage auf, ob die Tätigkeiten als Betriebsrat und als Datenschutzbeauftragter kompatibel sind. Die hierzu veröffentlichten Meinungen sind höchst unterschiedlich. Teilweise wird eine Inkompatibilität angenommen (Beder, CR 1990, S. 476; Bergmann/Möhrle/Herb, § 36 Rn. 61; Müller/Wächter, Der Datenschutzbeauftragte, S. 85, 1991; Tinnefeld CR 1991, S. 32; Schlemann, Recht des betrieblichen Datenschutzbeauftragten, S. 215, 1996), teilweise nicht (Gola, NJW 1993, S. 3112; Innenministerium Brandenburg, 2. TB, S. 11; Breinlinger, RDV 1993, S. 55).

Das Regierungspräsidium Darmstadt vertritt die Auffassung, dass nicht von vornherein von derartigen Interessenskonflikten auszugehen sei, dass die gesetzlich geforderte Zuverlässigkeit eines Datenschutzbeauftragten automatisch nicht gewährleistet sein könne. Eine Inkompatibilität wird daher nicht per se angenommen. Allerdings lehrt die bisherige Erfahrung, dass bei derartigen Konstellationen besonders genau zu prüfen ist, ob der betriebliche Datenschutzbeauftragte die gesetzlichen Aufgaben nach § 4g BDSG tatsächlich wahrnehmen kann und auch wahrnimmt.

**18. Bildungswesen**

Ein Seminarteilnehmer beschwerte sich bei der Aufsichtsbehörde, dass der Seminarveranstalter vorab eine Liste mit den Namen, privaten Adressen und Telefonverbindungen aller Seminarteilnehmer versandte, ohne eine vorherige Einwilligung der Betroffenen eingeholt zu haben. Diese Teilnehmerliste wurde während des Seminars nochmals ergänzt und am Ende an alle Teilnehmer verteilt.
Darüber hinaus hing die Teilnehmerliste in der Empfangshalle des Veranstaltungsortes, der auch durch Hotelgäste genutzt wurde, aus.

Die Aufsichtsbehörde beanstandete dieses Verfahren.
Der Seminarveranstalter konnte für den Aushang der Teilnehmerliste am Tagungsort keine Gründe nennen. Die Übersendung der Teilnehmerliste begründete er mit der Möglichkeit der Teilnehmer, auf diese Weise Fahrgemeinschaften zu verabreden. Grundsätzlich ist es gerechtfertigt, wenn ein Seminarveranstalter den Namen und ggfs. das Unternehmen, die Behörde oder sonstige Organisation, welche der Teilnehmer vertritt, in eine Teilnehmerliste aufnimmt und an alle Teilnehmer verteilt. Dies ergibt sich daraus, dass in einem Seminar in der Regel auch die Möglichkeit zur Kontaktaufnahme und zum gegenseitigen Erfahrungsaustausch geboten werden soll und diese Angaben daher üblicherweise auch auf Namensschildern ersichtlich sind.

Je nach Gegenstand und Teilnehmerkreis eines Seminars, z.B. Aids-Informationsveranstaltung, können die schutzwürdigen Interesse der Teilnehmer aber sogar der Verteilung einer Teilnehmerliste mit den oben genannten begrenzten Angaben entgegenstehen.

Die Aufnahme zusätzlicher Daten ist in jedem Fall nur zulässig, wenn den Teilnehmern eine Wahlmöglichkeit eingeräumt wurde. Aber auch dann dürfen sie nur den Teilnehmern selbst zugänglich gemacht werden. Da der Seminarveranstalter aber auch künftig eine Option für die Weitergabe bzw. Nichtweitergabe der personenbezogenen Daten der Betroffenen an alle Seminarteilnehmer nicht in sein Anmeldeformular aufnehmen wollte, stellte er sowohl den Aushang am Veranstaltungsort als auch die Übermittlung der Teilnehmerliste ganz ein.

Wiesbaden, 25. November 2002

Der Hessische Ministerpräsident
**Koch**

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