15. Wahlperiode

Drucksache **15/1539**

HESSISCHER LANDTAG

30. 08. 2000

Vorlage
der Landesregierung

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

Vorgelegt mit der Stellungnahme zum Achtundzwanzigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten - Drucks. 15/1101 - nach § 30 Abs. 2 des Hessischen Datenschutzgesetzes in der Fassung vom 7. Januar 1999.

Eingegangen am 30. August 2000 · Ausgegeben am 11. September 2000

Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

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

Die Regierungspräsidien überprüfen als Aufsichtsbehörde nach § 38 Abs. 1 BDSG im Einzelfall die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien regeln, wenn hinreichende Anhaltspunkte dafür vorliegen, dass eine dieser Vorschriften durch eine nicht-öffentliche Stelle verletzt ist, insbesondere wenn es Betroffene selbst begründet darlegen.

Im Berichtsjahr wurden von den Aufsichtsbehörden in 233 Fällen Überprüfungen von nicht-öffentlichen Stellen vorgenommen, die Datenverarbeitung nach § 28 BDSG für die Erfüllung eigener Geschäftszwecke betreiben oder personenbezogene Daten nach §§ 29, 30 BDSG zur personenbezogenen oder anonymisierten Übermittlung speichern und nutzen. Auf Vorfälle in drei Unternehmen wurden die Regierungspräsidien durch Pressemeldungen aufmerksam.

Die 233 Eingaben und Beschwerden betrafen:

- in 40 Fällen Kreditinstitute und Banken,
- in 22 Fällen Anbieter von Internet-Zugängen und Internet-Inhalten (Provider),
- in 21 Fällen Unternehmen der Direktmarketing- und Werbebranche,
- in 17 Fällen Versicherungsgesellschaften,
- in 17 Fällen das Gesundheitswesen (Kliniken, Ärzte, Apotheken, medizinische Marktforschung),
- in 14 Fällen Vereine, Dachverbände und Interessengemeinschaften,
- in 14 Fällen Handels- und Wirtschaftsauskunfteien,
- in 12 Fällen Adressbuchverlage und Herausgeber öffentlicher Verzeichnisse, Presse,
- in 8 Fällen den Datenschutz in Arbeitsverhältnissen,
- in 8 Fällen Unternehmen der Versandhandelsbranche,
- in 8 Fällen den Groß- und Einzelhandel,
- in 7 Fällen die Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa),
- in 6 Fällen Kreditkartenunternehmen,
- in 4 Fällen Vermieter, Hausverwaltungen und Mietervereine,
- in 6 Fällen Unternehmen der Reise- und Touristikbranche,
- in 2 Fällen Adresshandelsunternehmen,
- in 2 Fällen Markt- und Meinungsforschungsunternehmen,
- in 2 Fällen politische Parteien,
- in 2 Fällen Lotterieannahmestellen,
- in 21 Fällen sonstige Stellen (z.B. Diskothek, Rechtsanwälte, Paketzusteller).

Die weiter zunehmende Konzentration von Unternehmen aus dem Bereich der Geld- und Kreditwirtschaft (Banken, Auskunfteien, Schufa, Kreditkarten) am internationalen Finanzplatz Frankfurt am Main und die unverminderte Sensibilität der Bürgerinnen und Bürger für datenschutzrechtliche Fragestellungen im Zusammenhang mit der Verarbeitung ihrer Einkommens- Vermögens- und Bonitätsdaten führten erneut zu einem hohen Beschwerdeaufkommen bezüglich dieser Branche beim Regierungspräsidium in Darmstadt. Auch beim Angebot von Internet-Dienstleistungen und bei der Nutzung neuester Technologien haben hessische Unternehmen inzwischen eine Spitzenstellung innerhalb der Bundesländer eingenommen. Die Zahl der Eingaben, die die vornehmlich in Südhessen ansässigen Online-Dienste und Internet-Provider betrafen, hat sich gegenüber dem Vorjahr folglich deutlich erhöht.

In insgesamt 54 Fällen waren die Beschwerden begründet. Sämtliche bei diesen Nachforschungen der Aufsichtsbehörden festgestellten unzulässigen

Verarbeitungen personenbezogener Daten und anderer Verstöße gegen Vorschriften des Rechts der Tele- und Mediendienste führten zu Beanstandungen der jeweiligen Verarbeitungsverfahren in den betroffenen Unternehmen.

Die durch Verstöße gegen Datenschutzbestimmungen begründeten Eingaben richteten sich im Detail in zwölf Fällen gegen Kreditinstitute und Banken, in elf Fällen gegen Anbieter von Tele- und Mediendiensten (Internet), in neun Fällen gegen Firmen aus der Werbe- und Direktmarketingbranche, in vier Fällen gegen eingetragene Vereine und Dachverbände, in jeweils drei Fällen gegen Groß- und Einzelhändler, Arbeitgeber und andere Stellen, die Personal- und Bewerberdaten verarbeiten, sowie Ärzte, Krankenhäuser und andere Stellen aus dem Gesundheitssektor und in zwei Fällen gegen Wirtschaftsauskunfteien. Weitere berechtigte Beschwerden wegen Nichtbeachtung der Datenschutzbestimmungen wurden in jeweils einem Fall gegen ein Versandhandelsunternehmen, die Schufa, einen Kreditkartenanbieter, einen Verlag, eine Anwaltskanzlei, ein Unternehmen der Reise- und Touristikbranche und einen Wohnungs- und Liegenschaftsverwalter vorgebracht.

Bei 20 Eingaben an die Datenschutzaufsichtsbehörden konnte der den Beschwerden zugrunde liegende Sachverhalt nicht mehr vollständig aufgeklärt werden, sodass eine abschließende Beurteilung, ob die Datenverarbeitung in zulässiger oder in unzulässiger Weise erfolgt war, nicht getroffen werden konnte. Auch wenn diese Verfahren nicht zu Beanstandungen durch die Aufsichtsbehörden führten, konnte durch die Diskussion der jeweiligen Sachverhalte eine zunehmende Sensibilisierung für datenschutzrechtliche Problemstellungen bei den speichernden Stellen erreicht werden.

In 68 Fällen waren die Ermittlungen der Aufsichtsbehörden zum Ende des Berichtsjahres noch nicht abgeschlossen.

Von den noch aus den Vorjahren anhängigen Beschwerden wurden 24 Fälle abgeschlossen. Die Beurteilung dieser in der Regel nur mit hohem Ermittlungsaufwand aufklärbaren Fälle durch die Aufsichtsbehörden ergab, dass davon 15 Eingaben begründet waren. Dabei hatten in vier Fällen Wirtschaftsauskunfteien, in drei Fällen Banken, in jeweils zwei Fällen Adresshändler, Internet-Anbieter und Vermieter sowie in jeweils einem Fall ein Verein und ein Versandhändler personenbezogene Daten unzulässig verarbeitet oder genutzt.

2. Von Amts wegen durchgeführte Regelüberprüfungen von Stellen, die nach § 32 Abs. 1 Nr. 1 bis 3 BDSG geschäftsmäßig personenbezogene Daten verarbeiten oder nutzen

2.1 Melderegister

Die Aufsichtsbehörden führen nach § 38 Abs. 2 BDSG 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 unterliegen nach § 32 BDSG der Meldepflicht bei den Datenschutzaufsichtsbehörden.

Am 1. Februar 2000 waren 801 meldepflichtige Unternehmen im Register der Aufsichtsbehörden eingetragen. Damit war eine Steigerung gegenüber dem Vorjahr von ca. 15 v.H. zu verzeichnen.

Den größten Anteil hieran haben mit 649 Meldungen die nach § 32 Abs. 1 Ziff. 3 BDSG gemeldeten Unternehmen, die im Auftrag Dritter als Dienstleistungsunternehmen weisungsgebunden i.S.d. § 11 BDSG personenbezogene Daten verarbeiten oder nutzen. Hierbei handelt es sich um Konzern- und Dienstleistungsrechenzentren sowie um Datenerfasser, Schreibservices, Mikroverfilmer, Datenträgervernichter sowie Lettershops und ähnliche Unternehmen aus dem Bereich des Direktmarketings.

Mit 85 Meldungen haben die nach § 32 Abs. 1 Ziff. 2 BDSG meldepflichtigen Unternehmen der Markt- und Meinungsforschung, die personenbezogene Daten zum Zwecke der anonymisierten Übermittlung speichern, den zweitgrößten Anteil am Melderegisterbestand.

Den geringsten Anteil haben mit 67 Registereinträgen die nach § 32 Abs. 1 Ziff. 1 BDSG gemeldeten Unternehmen, die personenbezogene Daten zum Zwecke der Übermittlung speichern.

2.2 Prüfungsübersicht

Im Berichtsjahr wurden 46 Prüfungen nach § 38 Abs. 2 BDSG durchgeführt. Diese betrafen folgende Unternehmen:

- Servicerechenzentren 8
- Konzerndatenverarbeiter/verbundene Unternehmen 6
- Datenvernichter 8
- Adresshändler 3
- Telemarketingunternehmen/Callcenter 4
- Markt- und Meinungsforschung 2
- Mikroverfilmer 2
- Wirtschaftsauskunfteien 3

Die Prüfungen führten zu folgendem Ergebnis:

- Beanstandungen 26
- Empfehlungen 14
- ohne wesentliche Beanstandungen 6

Folgende wesentliche Mängel wurden am häufigsten festgestellt:

1. Keine bzw. verspätete oder unvollständige Weisungen der Auftraggeber nach § 11 BDSG
2. Keine bzw. verspätete oder unvollständige Registermeldung nach § 32 BDSG
3. Fehlende oder mangelhafte Schulung bzw. Unterrichtung der nach § BDSG verpflichteten Mitarbeiter
4. Fehlende bzw. unvollständige Dokumentationen
5. Erstellen von Auswertungen bzw. Listen mit personenbezogenen Daten ohne Erlaubnistatbestand
6. Leichtsinniger Umgang mit Passworten

Zusätzlich wurden 107 Überprüfungen auf schriftlichem Weg (mittels Fragebogen) durchgeführt. Insoweit wird auf die gesonderte Darstellung unter Nr. 2.3 verwiesen.

2.3 Schwerpunktmäßige Sonderüberprüfungen nach § 38 Abs. 2 BDSG bei kleineren Auftragsdatenverarbeitern

Im zugrunde liegenden Berichtsjahr hat das Regierungspräsidium Darmstadt erneut eine besondere Datenschutzüberprüfung nach § 38 Abs. 2 BDSG durchgeführt. Die Überprüfung wurde in einem schriftlichen Verfahren mit Hilfe eines Fragenkataloges durchgeführt. Aus den nach 32 Abs. 1 Nr. 3 BDSG gemeldeten Unternehmen wurden diejenigen herausgesucht, die in einem verhältnismäßig kleinen Rahmen Datenverarbeitung betreiben, sei es nun in der Form von Adressverwaltungen, Pflege der Kundenstämme der Auftraggeber, Datenverwaltung für Kleinunternehmen, Werbeaussendungen durch Serienbriefe oder als Datenerfasser.

Derartige schriftliche Überprüfungen können selbstverständlich Vor-Ort-Überprüfungen nicht ersetzen; sie sind jedoch für die Aufsichtsbehörde ein rationelles Mittel, um sich einen groben Überblick zu verschaffen und Anhaltspunkte zu gewinnen, wo die größten Defizite bestehen und gegebenenfalls eine örtliche Kontrolle geboten ist.

Darüber hinaus können die Befragungen den Anstoß geben, dass sich die Unternehmen überhaupt mit dem Datenschutz befassen.

Insgesamt wurden 107 Unternehmen angeschrieben. Diese erhielten den Fragebogen mit insgesamt 16 Fragen und einen aktuellen Auszug aus den derzeitigen Eintragungen nach § 32 BDSG. Rund 70 Fragenkataloge wurden

im Zeitraum von zwei Monaten - mehr oder weniger vollständig ausgefüllt - zurückgesandt. Nach Erinnerung sind bisher weitere 24 Antworten eingegangen.

Der Aufsichtsbehörde ist natürlich bewusst, dass nicht alle Fragen wahrheitsgemäß beantwortet worden sind. Der Fragenkatalog enthielt eine kleine Fangfrage und weitere Möglichkeiten, eine gewisse Stimmigkeit in den Antworten feststellen zu können. Hinzu kommt die Erfahrung der Aufsichtsbehörde aus vielen Hunderten zurückliegenden Überprüfungen vor Ort. Auf diese Weise war bei ca. 10 v.H. der zurückgesendeten Fragenkataloge eine gewisse Unstimmigkeit feststellbar bzw. vermutbar.

Auffallend hoch ist bei allen Stellen das Versäumnis der rechtzeitigen und korrekten Änderungsmeldungen nach § 32 Abs. 4 BDSG. Bei bisher neun Unternehmen konnte festgestellt werden, dass bereits seit mehreren Jahren die Tätigkeit eingestellt war. Eine rechtzeitige erforderliche Abmeldung hat nicht stattgefunden. In sechs Fällen ist noch nicht einmal eine Abmeldung zum Gewerberegister vorgenommen worden.

Die Befragung gab auch Aufschluss über datenschutzrechtliche Defizite bei den Auftraggebern:

Die nach § 11 Abs. 2 BDSG vorgeschriebene sorgfältige Auswahl eines Auftragnehmers sollte zumindest die Überprüfung einer korrekten Gewerbeanmeldung und einer korrekten Meldung nach § 32 BDSG beinhalten. Laut Angaben der Dienstleister haben sich jedoch lediglich 7. v.H. ihrer Auftraggeber nach einer ordnungsgemäßen Meldung nach § 32 BDSG erkundigt und auch die Einsicht in die Registermeldung verlangt. Nach einer Gewerbeanmeldung hat kein Auftraggeber gefragt.

Nach § 11 Abs. 3 BDSG darf der Auftragnehmer die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten oder nutzen. Der Auftrag ist schriftlich zu erteilen. Dies bedeutet, dass auch die erforderlichen Weisungen in schriftlicher Form vorliegen müssen. Insgesamt 79 datenverarbeitende Stellen arbeiten jedoch ohne schriftliche Weisungen ihrer Auftraggeber. Nur 14 Auftragnehmer sind in der Lage, schriftliche Weisungen vorlegen zu können. Obwohl die Aufsichtsbehörde in zahlreichen Fällen sowohl Auftraggebern wie auch Auftragnehmern hinsichtlich der Erstellung von erforderlichen Weisungen hilfreich zur Seite gestanden hat, liegt dieses krasse Missverhältnis vor. Zu den Auftraggebern, die das angesprochene Versäumnis betrifft, gehören auch eine Reihe großer Daten verarbeitender Stellen. Dies ist umso erstaunlicher, als in den Unternehmen in Zusammenarbeit zwischen Rechtsabteilung und Datenschutzbeauftragten erforderliche Weisungen erarbeitet worden sind. Aufträge im Bereich der automatisierten Verarbeitung personenbezogener Daten wurden jedoch teilweise kurzfristig an den günstigsten Auftragnehmer vergeben. So geraten innerbetriebliche Vorschriften in den Hintergrund.

Aber auch die einfachsten Sicherheitsvorschriften können so in den Hintergrund gelangen oder ganz außer Acht gelassen werden. Zur gebräuchlichsten Absicherung eines Datenbestandes bei automatisierten Verfahren gehört die Nutzung von Passworten. Für eine sinnvolle Nutzung dieser Zugriffssicherung sind einige Mindestanforderungen an die Organisation eines Passwortverfahrens zu stellen. So sollte ein Passwort mindestens sechsstellig alphanumerisch und nur der zugriffsberechtigten Person bekannt sein. Dass nach einem bestimmten Zeitraum (längstens nach sechs Monaten) ein Wechsel stattfinden sollte, hat sich mittlerweile bei vielen Datenverarbeitern herumgesprochen. Bei sechs Unternehmen erreicht ein Passwort lediglich die maximale Größe von drei Stellen. Bei 33 Unternehmen wird ganz ohne ein Passwort zur Zugriffsberechtigung gearbeitet. Lediglich 54 Unternehmen nutzen ein sechs- und mehrstelliges Passwort. Und dies, obwohl bei 29 der angefragten Unternehmen die Datenverarbeitung in Wohnungen, Häusern und/
oder Büroräumen stattfindet, die mit Familienangehörigen geteilt werden.

Hinsichtlich des erforderlichen Datentransportes bestätigte die Befragung, dass der Anteil des Transportes von Datenträgern mit Hilfe der Post, besonderen Botendiensten oder durch Mitarbeiter des Auftragnehmers zurückgeht. Häufig wird der Versand der Daten stattdessen über das E-Mail-Verfahren durchgeführt. Ein Verschlüsselungsverfahren allerdings, obwohl dies leicht

einsetzbar wäre, wird von keinem Auftraggeber verlangt und somit in keinem Auftragsverhältnis genutzt. Eine Dokumentation der Datenverarbeitung wird in den meisten Fällen nur über die Rechnungsstellung vorgenommen.

Ein weiteres sehr bedenkliches Ergebnis dieser Überprüfung ist die Erkenntnis, dass bei den Datenverarbeitern erhebliche Mängel bezüglich der Kenntnis der eigenen Datenverarbeitungssysteme vorliegen. Nicht mehr als fünf Prozent der überprüften Unternehmen verwenden Verfahren zum Löschen von personenbezogenen Daten, die den Löschvorschriften des BDSG entsprechen. Alle übrigen Unternehmen sind der Auffassung, dass durch die softwaremäßige Vorgabe in den gängigen PC-Betriebssystemen eine ausreichende Löschung von Daten gewährleistet sei. Andere Unternehmen sind sogar der Auffassung, sich in keiner Weise Gedanken über das Löschen von Daten der Auftraggeber machen zu müssen. Dies ist auch eine Folge der nicht vorliegenden Weisungen nach § 11 BDSG, in denen auch das Löschen von Daten geregelt sein müsste. Bereits im Tätigkeitsbericht für 1998 wurde die Thematik des Löschens angesprochen (Nr. 20.2).

Wie schon dort ausgeführt, sind Daten in den heutigen Systemen nur dann als gelöscht zu bezeichnen, wenn sie mit Hilfe von spezieller Software gelöscht werden oder wenn der Anwender sich die Mühe macht, alle vorhandenen zu löschenden Datensätze vollständig mehrere Male mit Zeichen zu überschreiben.
Werden Datenbestände nicht ordnungsgemäß gelöscht, so kann es dazu kommen, dass sie in unbefugte Hände gelangen und somit eine unrechtmäßige Übermittlung stattfindet (z.B. bei der Entsorgung der Datenverarbeitungsanlage).

Im Rahmen dieses Berichtes können lediglich die wesentlichen Beanstandungen aufgezeigt werden. Sie zeigen aber deutlich, dass Sicherheitsvorkehrungen nur in einem sehr begrenzten Rahmen getroffen werden. Die Unternehmen, von denen bisher keinerlei Antworten vorliegen, müssen mit der Einleitung von Ordnungswidrigkeitenverfahren nach § 44 BDSG rechnen. In einem Fall ist dies bereits geschehen.

3. Bearbeitung von Anfragen zu Problemen des Datenschutzes

Im Berichtsjahr wurden neben den konkreten Beschwerden Betroffener erneut zahlreiche Anfragen und Bitten um datenschutzrechtliche Stellungnahmen zu laufenden Verarbeitungsverfahren oder geplanten Projekten an die Datenschutzaufsichtsbehörden herangetragen. Der Trend, dass Unternehmen die Datenschutzaufsichtsbehörden bereits in der Planungsphase um die datenschutzrechtliche Würdigung technischer und juristischer Sachverhalte für künftige Projekte bitten, hat sich fortgesetzt. Es ist offensichtlich, dass durch eine frühzeitige kooperative Zusammenarbeit der Firmen mit den Aufsichtsbehörden datenschutzrechtliche Beanstandungen problematischer oder gar unzulässiger Verfahren vermieden und damit auch Kosten minimiert werden können.

Wie auch schon bei der Beschwerdebearbeitung hatte sich vor allem das Regierungspräsidium Darmstadt im Berichtsjahr aufgrund der weiter steigenden Nutzung globaler Firmennetze und weltweiter Internet-Dienste (WWW, E-Mail) durch Unternehmen, Arbeitnehmer und Privatpersonen verstärkt mit umfangreichen neuen rechtlichen Fragestellungen zum Angebot und zur Nutzung von Tele- und Mediendiensten zu beschäftigen. Die Tendenz zur weiteren Globalisierung der Wirtschaft und die vielfältigen Anwendungsmöglichkeiten neuer Informations- und Kommunikationstechnologien bringen stets Momente der Verunsicherung mit sich, wie sich an dem großen Bedarf der Unternehmen, der Verbände und der betroffenen Bürgerinnen und Bürgern nach datenschutzrechtlichen Hinweisen und Informationen zeigt.

Die Aufsichtsbehörden haben beispielsweise zur Zulässigkeit der Veröffentlichung von personenbezogenen Daten von Sportlern und Sportfunktionären, Mitgliedern von Vereinen mit sozialem oder kulturellem Hintergrund und auch Arbeitnehmern im World Wide Web (WWW) Stellung genommen. Weiterhin erhielten verschiedenste Unternehmen datenschutzrechtliche Hilfe bei der Ausgestaltung ihres WWW-Auftrittes. Hier standen sowohl die Fragen zur Zulässigkeit und Sicherheit der Verarbeitung von Daten der Nutzer

von Telediensten als auch die Ausgestaltung von Hinweis- und Einwilligungstexten auf der Firmen-Homepage im WWW im Vordergrund. Hinweise zur Vermeidung und Abwehr des steigenden Aufkommens unverlangter Werbe-E-Mails (SPAM) waren ebenfalls gefragt. Hier zeigte sich leider schnell, dass sich die Versender dieser Massen-E-Mails oftmals im außereuropäischen Ausland befindet und den Betroffenen daher lediglich technische Abwehrmaßnahmen (z.B. Filter-Programme) empfohlen werden können.

Neben der alltäglichen Beratung von Betroffenen und der rechtlichen Information von betrieblichen Datenschutzbeauftragten, Vereinen und Unternehmen lag ein inhaltlicher Schwerpunkt wie schon im Vorjahr bei den Anfragen zur Position und Funktion des betrieblichen Datenschutzbeauftragten nach §§ 36, 37 BDSG. Vor allem in kleinen und mittleren Untenehmen gibt es immer noch erheblichen Aufklärungsbedarf zur praktischen Tätigkeit der betrieblichen Datenschutzbeauftragten. Auch problematische Fragen zur Kündigung bzw. Abberufung von Datenschutzbeauftragten mussten geklärt werden.

In den Gesprächen mit den Datenschutzbeauftragten konnte außerdem festgestellt werden, dass sich die seit Jahren erwartete und im Berichtsjahr erneut nicht vollzogene Novellierung des Bundesdatenschutzgesetzes negativ auswirkt. Das beständige Warten auf die Modernisierung rechtlicher Rahmenbedingungen der Datenverarbeitung kann weder die wirtschaftliche Entwicklung in internationalen Zusammenhängen fördern, noch zur Akzeptanz datenschutzrechtlicher Regelungen durch die Unternehmen beitragen.

Einige der von den Aufsichtsbehörden beantworteten Anfragen sind in diesem Bericht behandelt (siehe insbesondere 5.3, 9.1, 9.5, 10.1, 10.2, 11.1, 12.2, 12.3, 19.).

4. Anlassunabhängige Überprüfungen bei Anbietern von Telediensten

§ 8 Teledienstedatenschutzgesetz (TDDSG) gibt den Aufsichtsbehörden die Möglichkeit, anlassunabhängige Kontrollen bei Teledienstеanbietern durchzuführen.

Aufgrund dieser Rechtsgrundlage hat das Regierungspräsidium Darmstadt sechs Teledienstеanbieter vor Ort überprüft.
Im Vordergrund stand dabei die Information über die Bestimmungen des TDDSG und auch des Mediendienstestaatsvertrages (da die Abgrenzung zwischen Tele- und Mediendiensten teilweise zweifelhaft ist).

Folgende Defizite wurden am häufigsten festgestellt:

- Verarbeitung von Bestandsdaten über die in § 5 Abs. 1 TDDSG zugelassenen Zwecke hinaus (ohne Einwilligung),
- Verarbeitung von Nutzungsdaten über die in § 6 TDDSG zugelassenen Zwecke hinaus (ohne Einwilligung),
- Grundsatz der Datensparsamkeit (§ 3 Abs. 4 TDDSG) nicht hinreichend beachtet.

5. Datenverarbeitung bei Banken

5.1 Fusion von Banken und Ausgliederung von Geschäftsbereichen

Um sich den Anforderungen des globalen Wettbewerbs zu stellen, nehmen Banken - wie andere Unternehmen auch - Fusionen oder Umstrukturierungen vor, die nach Maßgabe des Umwandlungsgesetzes (UmwG) vollzogen werden.

Eine Bank (im Folgenden: Bank A) gliederte den Teilbetrieb "Privat- und Geschäftskunden" nach § 123 Abs. 3 Nr. 1 UmwG auf eine andere Bank (im Folgenden: Bank B) aus.

Von der Ausgliederung waren mehrere Millionen Kundenbeziehungen betroffen. Lediglich die Kundenbeziehungen zu besonders vermögenden Privat- und Geschäftskunden (mit einem ausgeprägten Interesse an Vermögensanla-

ge- und Vorsorgeprodukten) verblieben bei der Bank A. Diese gehören zum Geschäftsbereich "Private Banking", der bereits vor der Ausgliederung intern vom Geschäftsbereich "Privat- und Geschäftskunden" unterschieden wurde, da sich unterschiedliche Bedarfsbündel auf der Kundenseite herausgebildet hatten.

Die Ausgliederung umfasste auch sämtliche Arbeitsverhältnisse derjenigen Mitarbeiter, welche in dem Teilbetrieb "Privat- und Geschäftskunden" beschäftigt waren, sowie eine Vielzahl weiterer Vertrags- und Rechtsverhältnisse.

Aufgrund zweier Beschwerden befasste sich die Aufsichtsbehörde mit der grundsätzlichen Frage, wie Fusionen und Ausgliederungen etc. nach dem Umwandlungsgesetz datenschutzrechtlich zu bewerten sind.

a) Verschmelzung von Unternehmen (Fusion)

Verschmelzungen i.S.d. § 2 UmwG bzw. die Registereintragungen bewirken eine Gesamtrechtsnachfolge (§ 20 UmwG).

Der Begriff der "Übermittlung" i.S.d. § 3 Abs. 5 Nr. 3 BDSG ist sehr weit gefasst, sodass zu überlegen ist, ob der Umwandlungsvertrag in Verbindung mit der beantragten (und erfolgten) Registereintragung als Übermittlung zu bewerten ist.
Hiergegen spricht jedoch, dass der Vorgang der Verschmelzung - sei es nun bei der Verschmelzung durch Neugründung oder bei der Verschmelzung durch Aufnahme - nicht dadurch gekennzeichnet ist, dass Daten vom Vertragspartner des Kunden an einen "Dritten" i.S.d. § 3 Abs. 9 BDSG gelangen, sondern dass sich die rechtliche Identität des Vertragspartners ändert.
Unter welchen Voraussetzungen Änderungen der rechtlichen Identität von Unternehmen und damit aufgrund der Gesamtrechtsnachfolge ein Wechsel bzw. eine Veränderung des Vertragspartners zulässig sind, ist eine dem BDSG vorgelagerte Frage. Das BDSG regelt nur, dass sich sowohl vor als auch nach der Umwandlung die Datenverarbeitung des Kredit-
institutes nach § 28 BDSG richten muss.
Wenn man anderer Auffassung wäre, würde dies bedeuten, dass der Abschluss von Verschmelzungsverträgen von sehr diffizilen Abwägungen nach §§ 28 ff. BDSG hinsichtlich aller Daten oder - im Falle von Bankverträgen - von den Einwilligungen aller betroffenen Kunden abhängig wäre. Damit würde man § 20 UmwG und das UmwG aushebeln. Eine sachgerechte Auslegung sowohl des BDSG als auch des UmwG kann daher nur von zwei unterschiedlichen Regelungsmaterien ausgehen, die sich nicht überschneiden, sondern eher in einer Art Stufenverhältnis zueinander stehen: Zuerst ist nach Maßgabe des UmwG zu entscheiden, ob die Verschmelzung überhaupt zulässig ist. Danach erst ist das BDSG maßgeblich für die Datenverarbeitung durch das "neue" Unternehmen.
Im Übrigen lässt sich die datenschutzrechtliche Irrelevanz von Verschmelzungen auch aus § 132 UmwG ableiten: In § 132 UmwG hat der Gesetzgeber die Gestaltungsfreiheit für den Abschluss von Umwandlungsverträgen durch die Bezugnahme auf Normen außerhalb des Umwandlungsgesetzes begrenzt. Dies hat er jedoch nur für ganz spezielle Umwandlungsarten getan.
Unabhängig davon, ob das Bundesdatenschutzgesetz tatsächlich zu den nach 132 UmwG zu beachtenden Schranken gehört (siehe nachfolgend unter b), führt zumindest der Umkehrschluss aus § 132 UmwG dazu, dass das Bundesdatenschutzgesetz jedenfalls beim Abschluss und Vollzug sonstiger Umwandlungsverträge unbeachtlich sein muss.
Im Ergebnis ist das BDSG für die Verschmelzung von Unternehmen nicht anwendbar.

Die Aufsichtsbehörde teilt damit die in den Hinweisen Nr. 38 des Innenministeriums Baden-Württemberg zum Datenschutz für die private Wirtschaft (Staatsanzeiger für Baden-Württemberg 2000, vom 18. Januar 2000, [Punkt A.3.]) vertretene Rechtsauffassung.

b) Aufspaltung, Abspaltung und Ausgliederung

Spezielle Problematik des § 132 UmwG

Bei Ausgliederungen, Aufspaltungen und Abspaltungen i.S.d. § 123 UmwG bewirkt die Registereintragung der entsprechenden Verträge eine partielle Gesamtrechtsnachfolge nach § 131 UmwG. Für die genannten Umwandlungsarten gilt § 132 UmwG. Danach bleiben allgemeine Vorschriften, welche die Übertragbarkeit eines bestimmten Gegenstandes ausschließen oder an bestimmte Voraussetzungen knüpfen oder nach denen die Übertragbarkeit eines bestimmten Gegenstandes einer staatlichen Genehmigung bedarf, durch die Wirkungen der Eintragung nach § 131 UmwG [= partielle Gesamtrechtsnachfolge] unberührt. § 399 des Bürgerlichen Gesetzbuches steht der Aufspaltung nicht entgegen.

Nach dem Zweck des § 132 UmwG sollen sich rechtliche Schranken, die einer Einzelrechtsnachfolge entgegenstehen, auch auf die Wirksamkeit der Gesamtrechtnachfolge auswirken. Der Gesetzgeber wollte damit der Gefahr, dass die speziellen Formen der Umwandlung nach § 123 UmwG nur gewählt werden, um die für die Einzelübertragung geltenden Schranken zu umgehen, entgegenwirken (Teichmann in Lutter (Hrsg.), UmwG, § 132 Rn. 2,3).

Es stellt sich daher die Frage, ob das BDSG einer Einzelrechtsnachfolge entgegenstünde.

Hierbei ist nicht maßgeblich, ob die Kundendaten als eigenständiges Vermögensgut veräußert werden können, sondern es kommt darauf an, ob das BDSG der Einzel-Übertragung eines Kundenvertrages entgegenstünde.

Denn wenn ein Kundenvertrag wirksam übergeht, dann darf der neue Vertragspartner selbstverständlich alle vom alten Vertragspartner im Rahmen des Vertragsverhältnisses zulässigerweise gespeicherten Daten weiter nutzen und verarbeiten.

Die Einzelübertragung der Rechte und Pflichten aus den einzelnen Bankverträgen erfordert zivilrechtlich zumindest eine Schuldübernahme, welche nach §§ 414, 415 BGB der Einwilligung bzw. Genehmigung des Gläubigers (Bankkunden) bedarf. Die im BGB nicht explizit geregelte Übertragung einer ganzen Vertragsposition (hier also des Bankvertrages mit den Kunden) ist nach der Rechtsprechung nur nach Mitwirkung/Zustimmung aller Beteiligten, also auch des Kunden zulässig.
In der Praxis wird sich daher die Frage, ob der Abschluss entsprechender (auf die Schuld- bzw. Vertragsübernahme gerichteter) Vereinbarungen und die in deren Vollzug erfolgende Datenweitergabe als Übermittlungen zu bewerten sind, gar nicht stellen.

Hiervon zu unterscheiden sind freilich die Fälle, bei denen Kundendaten nicht im Gefolge einer zivilrechtlich wirksamen Schuld- bzw. Vertragsübernahme, sondern unabhängig oder im Vorgriff auf eine solche (bzw. im Hinblick auf eine wegen Fehlens der Einwilligung/Genehmigung des Kunden noch schwebend unwirksame Vertragsübernahme) übertragen werden. In diesen Fällen läge zweifellos eine Übermittlung vor.

Die Abtretung einer Forderung wird ebenfalls als Übermittlung bewertet (vgl. Bergmann/Möhrle/Herb, BDSG, § 28 Rn. 1109 für die Abtretung ärztlicher Honorarforderungen).
Dies könnte ein Argument sein, dann auch die Schuldübernahme und die komplette Vertragsübernahme als Übermittlung zu bewerten (bzw. genauer den Gesamtvorgang der Vereinbarung nebst Vollzug).

Zwingend erscheint dies jedoch nicht.
Vielmehr könnte man durchaus das Verhältnis des BDSG zu den zivilrechtlichen Regelungen des BGB und der daraus entwickelten Rechtsprechung über die Übertragung von Vertragsverhältnissen als eine Art Stufenverhältnis ansehen (vgl. oben a):
Die für die Verarbeitung von Kundendaten zentrale Norm des § 28 Abs. 1 Nr. 1 BDSG knüpft an das Bestehen eines Vertragsverhältnisses an, dessen Zustandekommen wird nicht geregelt. (Der Abschluss eines Vertrages kann nicht als Übermittlung gewertet werden.) Demzufolge ist fraglich, ob die Übertragung von Verträgen unter den Begriff der Übermittlung fallen kann. Wie bereits erwähnt, ist die Frage aber jedenfalls in der Praxis nicht (bzw. allenfalls im Hinblick auf die Form der zivilrechtlich oh-

nehin erforderlichen Einwilligung/Genehmigung) relevant und von der Aufsichtsbehörde nicht vertieft worden, denn auch im Hinblick auf § 132 UmwG kann die Frage wohl letztlich dahingestellt bleiben:
Würde man § 132 UmwG wörtlich auslegen und anwenden, dann würde bereits § 415 BGB hinsichtlich der Kundenbeziehungen der Wirksamkeit der partiellen Gesamtrechtsnachfolge entgegenstehen, denn § 415 BGB enthält eine Voraussetzung für die Übertragbarkeit von Schulden, nämlich die Einwilligung/Genehmigung der Kunden. (So wohl Teichmann a.a.O., Rn. 10.).
Folglich würde die Übertragung der Kundenbeziehungen bereits aus diesem Grund scheitern (ohne dass es auf § 4 BDSG ankäme!).

In der Kommentierung zum UmwG wird jedoch die Auffassung vertreten, dass § 415 BGB nicht gelte. Dies beruht auf der grundsätzlichen Kritik an § 132 UmwG:

Danach wird es zwar im Ausgangspunkt als verständlich betrachtet, dass der Gesetzgeber unter dem Blickwinkel der "Umgehungsgefahr" die Kriterien für die Grenzen bei der partiellen Gesamtrechtsnachfolge aus dem Recht der Einzelübertragung entwickelt hat. Gleichzeitig wird dieser Ansatz jedoch zum einen gerade wegen seiner Ergebnisse, zum anderen aber auch grundsätzlich kritisiert. Nähme man § 132 wörtlich, so wäre eine Abspaltung oder eine Ausgliederung komplexer Vermögenseinheiten, für die die Rechtsinstitute gerade schaffen wurden, faktisch nicht möglich.
Die Kommentierung kommt so unter anderem im Wege der teleologischen Reduktion zu der Auslegung, dass bei der Übertragung von Vertragspositionen (bzw. der Schuldübernahme) § 415 BGB nicht gelte. Verträge gehen, wenn dies im Spaltungsvertrag so vorgesehen ist, im Ganzen, also mit ihren Ansprüchen, Rechten und Verbindlichkeiten auf den übernehmenden Rechtsträger über (Teichmann a.a.O., Rn. 12 - 14, 22).

Wenn Verträge wirksam übergehen, darf der neue Vertragspartner auch die Vertragsdaten erhalten und verarbeiten.

Selbst wenn man den Abschluss von Vereinbarungen über die Vertragsübernahmen (und den im Vollzug erfolgenden Datentransfer) als Übermittlung i.S.d. BDSG bewerten würde, so kann man im Wege der einschränkenden Auslegung des § 132 UmwG gleichwohl zu dem Ergebnis gelangen, dass das BDSG ebenso wenig einschlägig ist wie § 415 BGB:

Bei der teleologischen Auslegung des § 123 UmwG ist eine Interessenabwägung vorzunehmen. Einzubeziehen in diese Interessenabwägung ist die Zielsetzung des Gesetzes, notwendige oder auch nützliche Umstrukturierungen von Unternehmen gegenüber Einzelrechtsnachfolgen zu erleichtern oder überhaupt erst möglich zu machen. Dabei kann danach differenziert werden, ob bei dem Spaltungsvorgang ganze Betriebe bzw. Betriebsteile übergehen sollen, denn der Zweck des Gesetzes ist auf die Erleichterung des Transfers von Betrieben und Betriebsteilen gerichtet (Teichmann, a.a.O., Rn. 13).
Im konkreten Fall liegt eindeutig die Ausgliederung eines ganzen Betriebsteiles vor.

Wenn schon einer kompletten Verschmelzung der Bank A mit der Bank B, bei der sämtliche Kundenbeziehungen (nebst Daten) übergehen würden, die datenschutzrechtlichen Bestimmungen nicht entgegenstünden (siehe oben angeführt), dann ist nicht verständlich, warum bei der Übertragung der überwiegenden Zahl von (Privat-)Kundenbeziehungen das BDSG entgegenstehen sollte.

Im Ergebnis hielt die Aufsichtsbehörde daher die von den Banken vertretene Auffassung, dass für die Ausgliederung auf die Bank B keine Einwilligungen nach § 4 BDSG erforderlich gewesen seien und die im Zusammenhang mit der Vertragsbeziehung zulässigerweise gespeicherten Daten auch zulässig "übertragen" worden seien, für zutreffend.

Da aber die Auslegung des UmwG insgesamt mit Unsicherheiten behaftet ist, wird die wissenschaftliche Diskussion der Gesellschaftsrechtler zur Auslegung des UmwG weiter zu verfolgen sein.

5.2 Zweckgebundenheit eines Treuhänderdatenbestandes

Ein Treuhänder erhielt von Emissionsbanken Daten von Aktienkäufern für einen exakt beschriebenen treuhänderischen Zweck. Private Anleger sollten die Neuemission zu einem günstigeren Preis erhalten; für den Fall der Inanspruchnahme der Vergünstigungen würde der Treuhänder den vollständigen Namen, die Anschrift und das Geburtsdatum des betreffenden Aktienanlegers erhalten.

Die Aufgabe des Treuhänders bestand darin, die Bedingungen für die Inanspruchnahme der Vergünstigungen bei der Zuteilung zu überprüfen. Nach Abschluss dieser Tätigkeit (und einer vorher festgelegten zeitlichen Frist) waren die Daten beim Treuhänder zu löschen. Der Aktienkäufer wurde bereits mit dem Kaufantrag über diese Kontrollmechanismen informiert.

Nach der erfolgreichen Aktienemission meldete das nunmehr an der Börse notierte Unternehmen einen weitergehenden Kontrollbedarf an, um Missbräuche von einzelnen (Depot-)Banken auszuschließen. Für diesen - durchaus sinnvollen Zweck - hätte der vorhergehende treuhänderische Datenbestand - entgegen den vertraglichen Zusagen gegenüber den Aktienkäufern und den vorherigen vertraglichen Vereinbarungen mit dem Treuhänder - länger aufbewahrt und genutzt werden müssen.

Es gab aus Sicht der Aufsichtsbehörde jedoch keine Möglichkeit, den Adressdatenbestand der Aktienkäufer über den vertraglich zugesicherten Zeitraum hinaus aufzubewahren. Eine Änderung des Kontrollzweckes war - entsprechend den Regelungen von § 28 Abs. 1 Nr. 1 und 2 BDSG - ebenso nicht möglich; der weitere Zweck hätte schon bei der Emission genannt werden müssen.

Im Übrigen waren Betrugsfälle eher unwahrscheinlich, da bei einem Betrug im Einzelfall immer die Zusammenarbeit des privaten Aktienkäufers mit der (Depot-)Bank erforderlich gewesen wäre.

Aufgrund dieser Hinweise durch die Aufsichtsbehörde löschte der Treuhänder die Daten und wahrte damit den Vertrauensschutz der Aktienkäufer in die vertraglichen Vereinbarungen.

5.3 Übertragung von Dienstleistungen

Auftragsdatenverarbeitung oder Funktionsübertragung? - Diese Frage hatte sich der Datenschutzbeauftragte einer Bank (im Folgenden: Bank A) zu stellen, als diese beabsichtigte, die bisher über eine Zweigstelle abgewickelten Dienstleistungen "Order Discount und Betrieb einer Homebanking-Hotline" von einer anderen Bank (im Folgenden: Bank B) durchführen zu lassen. Die Bank B ist ein Tochterunternehmen und sollte die Dienstleistungen im Wesentlichen in Form eines Callcenters erbringen.

Eine Funktionsübertragung, also Übermittlung, wäre nur mit Einwilligung der Kunden möglich gewesen.

Die vom Datenschutzbeauftragten um Beratung gebetene Aufsichtsbehörde kam in Übereinstimmung mit der für das Tochterunternehmen zuständigen Aufsichtsbehörde zu der Bewertung, dass eine Auftragsdatenverarbeitung vorliegt.

Folgende Aspekte waren maßgeblich:

- Die Bank B ist nicht berechtigt, Tele- und Hombebanking-Verträge bzw. - als Zusatz - Order-Discount-Verträge für die Bank A abzuschließen. Die Verträge werden ausschließlich in der Bank A und deren Filialen in Schriftform abgeschlossen.
- Die Dienstleistung der Bank B umfasst nur die Abwicklung von Routineangelegenheiten ohne (echten) Beratungsbedarf.

  So erfolgt beim Order Discount keine Aufklärung über die mit einzelnen Wertpapiergeschäften verbundenen Risiken und auch keine sonstige Beratung. Darauf wird der Kunde bereits im Vertrag ausdrücklich hingewiesen. Die Zuständigkeit für die Konto- und Depotführung einschließlich der Wertpapierabrechnung verbleibt bei der Bank A.

- Die Bank A hat der Bank B genaue Vorgaben gemacht, wie zu verfahren ist. Die Bank B hat keinen eigenen Entscheidungsspielraum. Beispielsweise dürfen Dispositionen im Rahmen des Order Discount nur innerhalb der von der Bank A vorgegebenen individuellen Betragsgrenzen vorgenommen werden. Bei der Homebanking-Hotline dürfen grundsätzlich nur Fragen zu technischen und funktionellen Fragestellungen der Softwareprodukte beantwortet werden. Bei Anfragen, welche die persönliche Geheimzahl etc. betreffen, ist ein Mitarbeiter der Bank A hinzuzuziehen.

5.4 Markt- und Meinungsforschung bei Banken

Banken sind aus Eigen- und aus Kundeninteresse an den Wünschen ihrer Kunden interessiert. Im konkreten Fall sollte die Kundenzufriedenheit erfragt werden, um gegebenenfalls eine Verbesserung des Services herbeizuführen.

Eine Befragung der Kunden könnte auch von einer eigenen Marktforschungsabteilung durch die Bank durchgeführt werden. Sinnvoller und kostengünstiger wird dies aber von einem spezialisierten Marktforschungsunternehmen erledigt. Für den Kunden hat dies den Vorteil, dass er (anonym für die Bank) deutliche Kritik, z.B. über die Kreditsachbearbeitung äußern kann, ohne persönliche Nachteile (z.B. wegen einer Informationsweitergabe von Bankkollege zu Bankkollege) befürchten zu müssen.
Für die Bank ist es aber wichtig, gerade diese (berechtigte) Kritik des Kunden zu erfahren.

Die Adress- bzw. Telefonnummernweitergabe der Bank an das Marktforschungsunternehmen wurde von der Aufsichtsbehörde als unkritisch bewertet, da keine weiteren Kundendaten herausgegeben wurden und Deckadressen eventuelle Missbräuche offen legen. Darüber hinaus hatte die Bank vorab in einem Schreiben die Kunden über die Befragung ausführlich informiert; Widersprüche von Kunden wurden beachtet. Sowohl die Durchführung der Befragung als auch die Auswertung der Ergebnisse wurde von der Bank bestimmt. Mit dieser eindeutigen Auftragsdatenverarbeitung wurde nicht gegen das Bankgeheimnis verstoßen.

In Anbetracht dessen, dass bei der strafbaren Weitergabe von Kundendaten durch ein Marktforschungsinstitut dessen Existenz auf dem Spiel steht und der Auftraggeber das Verhalten der Marktforscher zusätzlich kontrolliert, sind die Daten in einem seriösen Marktforschungsunternehmen ebenso sicher wie in der Bank selbst.

Der Ehrenkodex der Marktforschungsunternehmen verhindert in der Regel, dass die Befragungsergebnisse personenbezogen an den Auftraggeber übergeben werden.
In anderem Zusammenhang wurde in der Vergangenheit von anderen Auftraggebern allerdings schon massiv versucht, die Befragungsdaten personenbezogen zu erlangen. Auf Befragen teilte die Aufsichtsbehörde den Marktforschungsunternehmen jeweils mit, dass eine anonyme Kundenbefragung aus Datenschutzgründen auch anonym bleiben muss.
Im Regelfall sind die Marktforschungsunternehmen hier sehr auf ihren Ruf bedacht und betrachten die Arbeit der Aufsichtsbehörde in diesem Zusammenhang als Unterstützung.

Es ist deshalb davon auszugehen, dass bei der Weitergabe von Kundenadressen bzw. Telefonnummern durch eine Bank für eigene Marktforschungszwecke keine schutzwürdigen Belange der betroffenen Kunden beeinträchtigt werden, sofern die genannten Voraussetzungen erfüllt sind.

5.5 Ausdruck von Bankleitzahl und Kontonummer im Kontoauszug

Bei Überweisungen kann es für den Überweisenden sinnvoll sein, wenn für ihn im eigenen Kontoauszug nochmals die Kontonummer und die Bankleitzahl des Empfängers aufgeführt wird. Dem Kontoauszug kommt häufig eine Beweis- oder Belegfunktion zu; in zahlreichen Fällen existiert bereits kein Überweisungsbeleg mehr. Die ausschließliche Angabe des Empfängernamens und des Verwendungszweckes zum Nachweis von Zahlungen kann im Einzelfall nicht ausreichend sein.
Detaillierte Angaben in den Kontoauszügen der überweisenden Kunden stellen also einen nützlichen Bankservice dar.

Für den Zahlungsempfänger ist es jedoch in der Regel nicht erforderlich, Kenntnis von der Kontonummer und der Bankleitzahl des Überweisenden zu erlangen. Der Absendername, Verwendungszweck und Betrag reicht für die Zuordnung der Zahlung aus. In Ausnahmefällen kann die Bank fehlgeleitete Zahlungen - in Kenntnis der vollständigen Überweisungsdaten - an den Urheber zurück überweisen.

Da für den Überweisungsempfänger mithin kein Erfordernis besteht und damit kein berechtigtes Interesse an den Bankleitzahl- und Kontonummerdaten des Überweisenden vorliegt, ist diese Datenübermittlung einzustellen.

Die betroffene Genossenschaftsbank ließ die Kontoausdrucke standardisiert bei einem großen genossenschaftlichen Rechenzentrum außerhalb Hessens erstellen. Da die Beanstandung jedoch erstmals überhaupt vorgebracht wurde, mussten die Programme geändert werden. Je nach der von den Banken gewünschten Gestaltungsweise lässt sich nunmehr der Ausdruck (über Parameter gesteuert) vollständig oder um Bankleitzahl und Kontonummer des Überweisenden verkürzt erstellen. Zwischenzeitlich wurden vergleichbare Beanstandungen auch von der Berliner Aufsichtsbehörde bekannt; so ist wohl mittelfristig mit einer grundsätzlichen Verbesserung aus datenschutzrecht-
licher Sicht zu rechnen.

Es handelt sich hierbei um keine überzogenen Anforderungen der Datenschützer; die Kontonummer eines Betroffenen und seine Bankverbindung sind schützenswert. In Einzelfällen wird aus Kreisen der Wirtschaft sogar empfohlen, dass Export-Unternehmen auf dem Geschäftsbriefbogen Kontonummer und Bank nicht erwähnen, da es beispielsweise in Russland zu Missbrauchsfällen auf Grund solcher Angaben gekommen ist.

5.6 Automatisches Hinzufügen der Empfänger-Anschrift auf den Kontoauszug des Überweisenden

Eine Betroffene äußerte ihre Verwunderung darüber, dass ihre Anschrift auf dem Kontoauszug des Absenders einer Überweisung erschien, obwohl diesem ihre Anschrift bis dahin unbekannt war. Es stellte sich heraus, dass die Bank generell - wenn der Empfänger Kunde der Bank war - die Anschrift dem Kontoauszug des Absenders hinzufügte. Die Bank begründete die Vorgehensweise damit, dass so bei einer Fehlüberweisung eine unmittelbare Kontaktaufnahme zwischen den beteiligten Parteien ermöglicht wird. Dies sei schließlich im Interesse der Kunden. Eine Erforderlichkeit war jedoch nicht gegeben, sodass keine Rechtsgrundlage nach § 28 Abs. 1 Nr. 1, 2 bzw. Abs. 2 Nr. 1 a BDSG bestand.

Die Bank hat dies eingesehen und ihr System verändert, sodass die Übermittlung künftig unterbleibt.

5.7 Abfrage und Speicherung der Passnummer für die Erfüllung des Geldwäschegesetzes

Die Erkenntnis, dass das Geldwäschegesetz und das Bundesdatenschutzgesetz in einem gegenseitigen Spannungsverhältnis stehen, ist nicht neu.

Die Kreditinstitute und Kreditkartenunternehmen sind gehalten, nach § 2 Abs. 1 in Verbindung mit § 1 Abs. 5 Geldwäschegesetz (GwG) den Betroffenen unter anderem mit der Nummer des Personalausweises oder Reisepasses zu identifizieren. Vergleichbares fordert auch § 103 Abgabenordnung. Diese Identifizierungspflicht bzw. die diesbezügliche Aufzeichnungspflicht nach § 9 Abs. 1 GwG wird vom Bundesaufsichtsamt für das Kreditwesen dahingehend ausgelegt, dass diese Nummern auch gespeichert werden müssen.

Der Vorschlag, sich bei der Erfassung der Personalausweisnummer bzw. Passnummer auf Teile dieser Nummern zum Nachweis der Identifizierung zu beschränken, wurde vom Bundesaufsichtsamt für das Kreditwesen nicht akzeptiert.

Wenn die vollständige Ausweisnummer einmal gespeichert ist, lässt sie sich jederzeit entgegen den Vorschriften von § 4 Abs. 2 u. 3 des Personalausweis-

gesetzes nutzen. Eine Einhaltung dieser und vergleichbarer Vorschriften des Passgesetzes lässt sich nicht sicherstellen.

Heutige Computersysteme ermöglichen in der Regel jederzeit eine gezielte Auswertung der Seriennummern von gespeicherten Personalausweisen bzw. Pässen.

Derartiges kann bei Banken mit zahlreichen Filialen (ohne einheitliche Kundennummer) zur Feststellung des Gesamtobliegens bzw. Gesamtvermögens eines Kunden durchaus von Interesse sein.

Die Aufsichtsbehörden können hier nur darauf hinweisen, dass die Speicherung von Ausweis-/Passnummer eindeutig zweckgebunden ist und andere Nutzungen datenschutzrechtlich unzulässig sind.

5.8 Unzulässige Datenübermittlung im Zusammenhang mit einer Erbschaft

Eine Bank hatte bei einer Erbauseinandersetzung Kontoinformationen der Verstorbenen an die Erben übermittelt. Diese Informationen waren für die Erbberechtigten erforderlich, um ihre Ansprüche geltend machen zu können.

Im Beschwerdefall wurden aber auch die gesamten Kontodaten einer Erbin bei der gleichen Bank an weitere Erben übermittelt.

Es mag sein, dass hieran für die übrigen Erben ein gewisses Interesse bestand, weil bei strittigen Erbauseinandersetzungen häufig der Verdacht einer vorherigen Bereicherung geäußert wird. Die Übermittlung der Kontodaten der Erbin war trotzdem als unzulässig zu bewerten. Eventuelle weiter gehende Informationsansprüche hätten die betroffenen Erben begründen und gerichtlich durchsetzen müssen.

Die betroffene Bank bezeichnete die Übermittlung der Kontodaten der Erbin an weitere Erben als Büro-Versehen. Es ist davon auszugehen, dass sich zumindest bei dieser Bank der Fall nicht wiederholen wird.

5.9 Depot- und Kontonummer im Adressfeld sichtbar

Mitarbeiter eines Unternehmens erhielten Aktionärsmitteilungen (ihres Arbeitgebers) von einer Großbank. Bei diesen Mitteilungen war im Adressfeld sowohl die Kontonummer als auch die Depotnummer sichtbar.

Der Betroffene glaubte, dass die Bank wenig professionell gehandelt und seine Konto- und Depotnummer damit unbefugten Dritten zur Kenntnis gegeben hatte.

Es stellte sich jedoch heraus, dass der Arbeitgeber das Layout des Briefes vollständig erstellt hatte und die Bank über einen Dienstleister nur den Versand erledigte.

Damit derartige Ereignisse sich nicht wiederholen, wurde mit der Bank vereinbart, bei solchen Sendungen für Dritte die Gestaltung des Layouts unter Datenschutzaspekten zu kontrollieren bzw. den Auftraggeber entsprechend zu beraten.

5.10 Datenerhebung beim Auto-Leasing

Mit großer Verblüffung reagierte der Kunde eines Autohauses, der beim Abschluss eines Leasing-Vertrages befragt wurde, ob er denn Wehr- oder Zivildienst abgeleistet habe oder ob er vom Dienst freigestellt gewesen sei. Auf Nachfrage wurde ihm vom Verkaufspersonal erklärt, dass diese Angaben schon immer so vom EDV-System der angeschlossenen Leasing-Bank verlangt würden. Auch auf dem Antragsformular sei schließlich ein entsprechendes Feld vorhanden, das auszufüllen sei. Zu welchem Zweck diese Information im Rahmen der Leasing-Vereinbarung benötigt wird und welche Funktion diese Frage bei Frauen haben könnte, vermochten die Mitarbeiter des Autohauses allerdings auch nicht zu sagen. Da der Kunde befürchtete, dass hier Männer und Soldaten beim Auto-Leasing bevorzugt werden sollten, bat er die Aufsichtsbehörde um Prüfung der Zulässigkeit dieser Datenerhebung.

Bei den Nachforschungen der Aufsichtsbehörde stellte sich jedoch schnell heraus, dass es sich bei dem fraglichen Sachverhalt um einen Software-Fehler des von der Bank und dem Vertragshändler benutzten Point-of-Sale-Systems handelte, das den Verkäufer bei der Finanzkalkulation und der Erfassung der für die Kreditentscheidung erforderlichen Daten unterstützt. Zur Absicherung des kreditorischen Risikos ist es bei männlichen Personen unter 26 Jahren durchaus zulässig nachzufragen, ob durch die eventuell noch ausstehende Einberufung zum Wehr- oder Zivildienst eine Unterbrechung der vereinbarten Zahlungsweise entstehen kann. Aufgrund der Prüfung durch die Aufsichtsbehörde stellte sich heraus, dass in einigen Einzelfällen systemseitig diese Frage auch älteren Männern und Frauen gestellt wurde. Die Bank hat diesen Mangel umgehend durch den Austausch der betroffenen Systeme behoben.

Die Datenschutzaufsichtsbehörde hat die unzulässige Datenerhebung gegenüber dem Autohaus beanstandet und dieses aufgefordert, seine Mitarbeiter künftig besser zu schulen sowie den (vorhandenen) betrieblichen Datenschutzbeauftragten umfassender in die Bearbeitung datenschutzrelevanter Vorgänge einzubinden.

6. Schufa

6.1 Interpretation von Score-Werten

Die Score-Werte der Schufa geben bei unterschiedlichen Anlässen Grund zur Klage. Score-Verfahren erstellen mit statistisch-mathematischen Methoden Prognosen über das zukünftige Verhalten von Personengruppen und drücken diese in einer Punktzahl (Score) aus. Dabei handelt es sich um eine anonymisierte Auswertung aller im Schufa-Datenbestand gespeicherten Daten, auf deren Grundlage eine Wahrscheinlichkeit des Eintretens von Risiken prognostiziert wird, die z.B. mit einer Kontoeröffnung oder der Einräumung eines Kredites verbunden sind. Diese Wahrscheinlichkeitsaussage gilt nicht für
eine konkrete Person, sondern nur für Gruppen von Personen mit gleichem Datenprofil. Aufgrund der Auswertung einer Vielzahl gleichartiger Datensätze soll es möglich sein, vorherzusagen, dass ein Kreditverhältnis ähnlich verlaufen wird, wie in der Vergangenheit die Kreditverhältnisse der herangezogenen Vergleichspersonen.
Weder die Schufa noch der Schufa-Anschlusspartner (Abfrager) gibt dem Betroffenen in der Regel Auskunft über die Höhe des Score-Wertes.

Die Schufa begründet dies damit, dass der Score-Wert eine wechselnde Größe sei und bei ihr nicht gespeichert werde, welcher Wert dem Betroffenen im Zeitpunkt der Abfrage durch den Anschlusspartner zugeordnet wurde.

Ein Betroffener hatte bei der Schufa einen Score-Wert mit einem Ausfallrisiko von 10 bis 12,5 v.H., was dazu führte, dass er eine gewünschte Lieferung bei einem Versandhändler nicht erhielt. Obwohl der Betroffene keinerlei Negativdaten bei den Schufa-Eintragungen aufwies, wurde ihm das gesamte Gruppenrisiko zugeordnet.

Der Lieferant stützte seine negative Entscheidung allein auf den Score-Wert der Schufa und lehnte damit (quasi automatisiert) eine Geschäftsverbindung ab. Derartige automatisierte Einzelentscheidungen sind nach Art. 15 der EG-Datenschutzrichtlinie unzulässig.

Die Annahme und Vorgabe der Schufa, dass der Score-Wert kein alleiniges Entscheidungskriterium ist, entspricht jedenfalls im konkreten Fall nicht der Realität. Der Versandhändler hatte auch keine weiteren Informationen der Schufa (wie z.B. die Banken), die den Score-Wert relativieren könnten. Lediglich bei Altkunden wäre dies weniger problematisch, weil der Händler hier auch eigene Kenntnisse aus der Geschäftsbeziehung hat.

Da die EG-Richtlinie noch nicht in deutsches Recht umgesetzt wurde und für den Lieferanten kein Kontrahierungszwang besteht, konnte der Lieferant nicht zu einer anderen Entscheidung bewegt werden.

In diesem Zusammenhang wurde offensichtlich, dass die jetzige Schufa-Einwilligungsklausel nicht ausreicht. Für den Betroffenen war zum Zeitpunkt der Einwilligung in die Übermittlung positiver Vertragsdaten nicht erkennbar, dass sich auch positive Daten im Gruppenvergleich des Scorings für ihn negativ auswirken können. Ein Hinweis in der Schufa-Einwilligung, dass ein Score-Wert übermittelt wird - wie er künftig vorgesehen ist -, ist sehr zu begrüßen, genügt aber nicht.
Der Betroffene muss eine Vorstellung davon haben, wie der Score-Wert zustande kommt.

Ein Merkblatt mit Hintergrundinformationen muss zumindest allgemeine Angaben über die Kriterien (Faktoren) des Score-Wertes enthalten. Der Betroffene muss darüber hinaus auch in jedem Fall beim angeschlossenen Unternehmen Auskunft über den Score-Wert erhalten, der bei der Kreditentscheidung berücksichtigt worden ist, damit er seinen Standpunkt geltend machen kann (vgl. Art. 15 Abs. 2a der EG-Richtlinie).

Die Forderungen der Aufsichtsbehörden werden zurzeit mit der Kreditwirtschaft und der Schufa intensiv erörtert.

6.2 Personenverwechslung bei Zwillingen

Die Datenspeicherung bei der Schufa ist ein Massengeschäft mit relativ geringer Fehlerquote. Menschliche Fehler können jedoch nicht ausgeschlossen werden. Verwechslungen von Vater und Sohn mit gleichem Vornamen sind schon - trotz des unterschiedlichen Geburtsdatums - bei einer identischen Wohnadresse vorgekommen.

Die neueste Verwechslung betraf Zwillinge, die nur über die unterschiedlichen Vornamen auseinander gehalten werden konnten. Die Zwillinge erhielten durch die fehlerhafte Bearbeitung bei der Schufa eine gemeinsame Identität mit einem einzigen Vornamen. Der Vorname gehörte ausgerechnet zu dem Zwilling, welcher einen negativen Eintrag erhielt.

Ein Telekommunikationsanbieter, bei dem der andere Zwilling einen Mobilfunkvertrag abgeschlossen hatte, erhielt daraufhin eine Mitteilung über den Negativeintrag. Dies führte zur Kündigung des Dienstleistungsvertrages.

Der Empfänger der Negativnachricht hatte hierbei nicht die unterschiedlichen Vornamen berücksichtigt, weil Nachname und Geburtsdatum übereinstimmten. Der Empfänger von Schufa-Nachmeldungen ist jedoch - entsprechend den technischen Anweisungen der Schufa - verpflichtet, die Personenidentität zu überprüfen. Eine Überprüfung hätte zu einer Aufdeckung der fehlerhaften Schufa-Datenspeicherung und der fehlerhaften Datenübermittlung der Schufa geführt.

Dieser Fall bestätigt frühere Erfahrungen, dass (Nach-)Meldungen beim Schufa-Anschlusspartner nicht ausreichend geprüft werden. Beispielsweise wurden Kunden einfach abgewiesen, weil eine (zeit-)aufwendige Identitätsprüfung als nicht lohnend erschien.

Das Schufa-System erhält seine Qualitäten aber unter anderem durch ständige Kontrollen seiner Anschlusspartner.

7. Auskunfteien

7.1 Speicherung und Übermittlung unrichtiger Daten

Zum betroffenen Unternehmen waren - bis auf wenige Ausnahmen - fast nur falsche Daten gespeichert und wurden auch in dieser Form von der Auskunftei an Anfrager übermittelt.

Hier wurde wieder einmal dokumentiert, dass der Wert einer Auskunft mit der Qualität der Recherche durch die Wirtschaftsauskunfteien steht und fällt.

Erst nach mehrmaligen Änderungen (und jeweiligen Benachrichtigungen der Auskunftsempfänger) gelang es, die Datenspeicherung der Realität anzupassen.

Die betroffene Auskunftei hat mit personellen Maßnahmen gegenüber ihrem unzuverlässigen Rechercheur eine Wiederholung dieses Vorfalles verhindert.

Für Unternehmen kann dieses Ereignis nur bedeuten, dass es wichtig ist, die eigene Kreditbeurteilung durch Selbstauskünfte zu kontrollieren. Juristische Personen - falls es keine Ein-Personen-Gesellschaften sind - können jedoch keine Auskünfte nach § 34 BDSG fordern. In der Regel werden Selbst-Auskünfte über juristische Personen aber freiwillig zur Qualitätskontrolle erteilt.

7.2 Fragwürdige Recherche-Methoden

Ausgangspunkt für eine Recherche ist häufig eine telefonische Befragung des Betroffenen selbst.

Eine Betroffene beschwerte sich darüber, dass sie bei der Selbstbefragung telefonisch erheblich unter Druck gesetzt worden sei. Dies war offensichtlich nicht das einzige Ereignis dieser Art, da die Auskunftei bereits 1997 der Betroffenen die Zusage gegeben hatte, weitere Kontakte zu unterlassen.

Vom betroffenen Rechercheur wurden telefonische Pressionen bestritten, vor allem behauptete er, bei seiner neuen Recherche nicht gewusst zu haben, dass die Betroffene die neue Geschäftsführerin und Eigentümerin des recherchierten Unternehmens sei. Zumindest in diesem Punkt waren die Behauptungen des Rechercheurs offensichtlich unwahr, weil ein der Recherche zugrunde liegendes Werbeschreiben von der Betroffenen unterschrieben war und sie in der Fußnote als Inhaberin bezeichnet wurde.

Der Datenschutzbeauftragte wurde aufgefordert, die Tätigkeit des verursachenden Rechercheurs verstärkt zu kontrollieren.

Betroffenen ist - sollten derartige Übergriffe von Rechercheuren tatsächlich vorkommen - zu empfehlen, nur schriftliche Auskünfte zu erteilen oder Auskünfte zu verweigern. Bei einer schriftlichen Selbstauskunft ist auch die Beweislage in jeder Hinsicht vorteilhafter.

7.3 Benachrichtigung nach § 33 BDSG mit Werbung verknüpft

Werden erstmals personenbezogene Daten für eigene Zwecke gespeichert, ist der Betroffene von der Speicherung und der Art der Daten zu benachrichtigen. Diese Vorschrift soll der Transparenz der Datenverarbeitung für den Betroffenen dienen. Wenn jedoch öffentlich verfügbare Adressdaten (z.B. aus Telefonbüchern) zu Werbezwecken gespeichert werden, ist der Sinn einer gesonderten Benachrichtigung für die betroffenen Unternehmen kaum nachvollziehbar. In diesen Fällen wird von der Aufsichtsbehörde toleriert, dass die Benachrichtigung der Werbung beigefügt ist.

Im vorliegenden Fall handelte es sich jedoch um nicht ohne weiteres öffentlich verfügbare Anlegerdaten, die längerfristig gespeichert und zu Werbezwecken genutzt werden sollten. Die kreative Geschäftsidee, mit der Benachrichtigung nach § 33 BDSG den Aufmerksamkeitswert der Werbung zu erhöhen, wurde von der Aufsichtsbehörde missbilligt. Schriftliche Werbung wird zu einem hohen Prozentsatz ungelesen in den Papierkorb geworfen. Es ist zu befürchten, dass dann die gesetzlich vorgeschriebene Benachrichtigung gleichzeitig ungelesen als vermeintliche Werbung mit entsorgt wird.
Als Kompromiss - separate Portokosten für Benachrichtigungen haben einen hohen Abschreckungsfaktor - ist es nach Meinung der Aufsichtsbehörde akzeptabel, wenn in einem beigefügten separaten Schreiben benachrichtigt wird. Sinnvollerweise sollte dabei - auch ohne gesetzliches Erfordernis - auf das Widerspruchsrecht nach § 28 Abs. 3 BDSG hingewiesen werden. Dieser zusätzliche Hinweis spart dem Unternehmen - wenn es auch selten geglaubt wird - Geld, weil unerwünschte Werbung auch ein Kostenfaktor ist und im Ergebnis negative Imageeffekte erzeugt.

8. Kreditkartenunternehmen

8.1 Datenverarbeitung im Zusammenhang mit Corporate Travel (und Corporate Card)

Ein Kreditkartenunternehmen bietet auch Reisedienstleistungen für Firmen an, d.h. die Firmen übertragen die Buchung und Abwicklung ihrer Geschäftsreisen auf das Kreditkarten- bzw. Reisebürounternehmen mit dem Ziel, einen optimalen Service zu erhalten und Reise- sowie Verwaltungskosten zu reduzieren.
Die Geschäftsreisenden (d.h. die Mitarbeiter der betreffenden Firmen) können so ihre Buchungen unmittelbar über das Kreditkartenunternehmen vornehmen.

Wenngleich im Rahmen des Corporate Travel grundsätzlich nur eine Vertragsbeziehung (Dienstleistungsvertrag) zwischen dem Kreditkartenunternehmen und den Firmen besteht, so werden doch eine Vielzahl personenbezogener Daten der Arbeitnehmer bzw. Angestellten verarbeitet.
Hierüber informierte ein von dem Kreditkartenunternehmen herausgegebenes und an die Geschäftsreisenden verteiltes Datenschutz-Faltblatt.
Dieses war Anlass für mehrere Eingaben und führte zu Diskussionen, die mit Konkurrenzunternehmen möglicherweise erst noch zu führen sein werden.
Die Aufsichtsbehörde bewertete die Datenverarbeitungen durch das Kreditkartenunternehmen nicht als Auftragsdatenverarbeitung i.S.d. § 11 BDSG, sondern als eigenständige Datenverarbeitung, für welche das Kreditkartenunternehmen verantwortlich ist.

Ein Teil der Eingaben bezog sich auf die als "Reiseprofil" erfassten Daten und die werbliche Nutzung.
Die Geschäftsreisenden haben die Möglichkeit, in einem Formular ihre Präferenzen und Wünsche hinsichtlich der Reisebuchungen mitzuteilen, beispielsweise, welche Hotelkette und -kategorie oder welche Mahlzeit im Flugzeug (Standardmenü oder vegetarisch) bevorzugt wird.
Die Erfassung dieses "persönlichen Reiseprofils" soll dazu dienen, die Reisen noch schneller organisieren zu können. Durch die Hinterlegung der Daten im START/Amadeus-Buchungssystem muss der Reisende nicht jedes Mal bei einer Buchung seine Daten neu mitteilen. Sein Reiseprofil wird abgerufen und die Kerninformationen für seine Buchung sind automatisch vorhanden.

Da in dem Formular auf die Datenweitergabe an "ein von Dritten betriebenes Computer-Reservierungssystem" ausdrücklich hingewiesen wurde und die Datenerfassung auf freiwilliger Basis erfolgt sowie die Daten (derzeit) ausschließlich für die Geschäftsreiseplanung verwendet werden, hatte die Aufsichtsbehörde im Grundsatz keine Bedenken.

Im oben genannten Datenschutz-Faltblatt war jedoch auch von einer Verwendung für Berichte an den Arbeitgeber und - unter Hinweis auf das Widerspruchsrecht - von einer (künftigen?) werblichen Datennutzung die Rede, wobei der Umfang nicht ganz klar war.
Insbesondere im Hinblick darauf, dass die Betroffenen von ihrem Arbeitgeber zur Inanspruchnahme der Reisebüro-Dienstleistungen und damit zur Preisgabe personenbezogener Daten an das Unternehmen gezwungen werden, sind im Hinblick auf die schutzwürdigen Belange hohe Anforderungen, insbesondere an die Transparenz, zu stellen.

Die Aufsichtsbehörde vertrat daher die Auffassung, dass die im Faltblatt enthaltenen (und sehr zu begrüßenden) Ansätze verbessert werden sollten:
Bereits in dem Reiseprofil-Formular sollte explizit darauf hingewiesen werden, dass die Angaben freiwillig sind und zu welchem Zweck sie verwendet werden.

Hinsichtlich einer etwaigen werblichen Nutzung müsste auf dem Reiseprofil-Formular eine Einwilligung eingeholt werden oder eine klare Widerspruchs-(opt-out)-Möglichkeit durch Ankreuzen vorgesehen werden.
Eine Einwilligung wäre unerlässlich, wenn Daten aus dem Reiseprofil mit Daten aus der Nutzung der Corporate Card und mit den Daten aus der Nutzung der gegebenenfalls vorhandenen privaten Karte verknüpft würden. Dies war jedoch im konkreten Fall gemäß Auskunft der betrieblichen Datenschutzbeauftragten nicht der Fall und ist auch nicht beabsichtigt.
Wenn im Dienstleistungsvertrag zwischen Arbeitgeber und dem Kreditkarten- bzw. Reisebürounternehmen die werbliche Nutzung ausgeschlossen wurde bzw. die Datennutzung ausdrücklich auf die Erbringung der Reisedienstleistung beschränkt wurde, hat dies Vorrang, d.h. eine werbliche Nutzung der Daten der Reisenden scheidet von vornherein aus.

Gegenstand einer Eingabe bzw. Anfrage war des Weiteren die Frage, inwieweit es zulässig ist, dass das Kreditkartenunternehmen Daten über das Reiseverhalten der Mitarbeiter und Auswertungen an den Arbeitgeber liefert. Die Datenschutzbeauftragte des Kreditkartenunternehmens richtete außerdem selbst die Anfrage an die Aufsichtsbehörde, ob es zulässig sei, "Rohdaten" an die Arbeitgeber zu liefern, sodass diese selbst personenbezogene Auswertungen vornehmen können. Derzeit werden keine Rohdaten geliefert, vielmehr werden im Wesentlichen statistische Auswertungen erstellt.

Die Aufsichtsbehörde differenzierte bei ihrer Bewertung zwischen folgenden Fallgruppen:

a)
Die Buchungen werden über Corporate Travel vorgenommen, die Bezahlung erfolgt mittels einer persönlichen Kreditkarte des Geschäftsreisenden oder durch ein anderes Zahlungsmittel, jedenfalls nicht über eine Reisestellenkarte (siehe hierzu nachfolgend b) oder über eine vom Kreditkartenunternehmen herausgegebene Corporate Card (siehe hierzu nachfolgend c).

Da es sich um Geschäftsreisen handelt, bestehen keine Bedenken, wenn der Arbeitgeber Daten über den Verlauf der Reisen erhält (Reiseziel, Reisedatum, Fluglinie, Flugpreis, Name des Reisenden und gegebenenfalls weitere Daten) - also solche Daten, die der Reisende ohnehin regelmäßig in Reiseantrags- und Reisekostenerstattungsformularen anzugeben hat (bzw. hätte).

Hier muss nur klar sein, dass sich diese Buchungsdaten tatsächlich auf Geschäftsreisen beziehen. Der Arbeitgeber muss also gegenüber seinen Mitarbeitern klarstellen, dass die Corporate-Travel-Dienstleistung entweder ausschließlich für Geschäftsreisen in Anspruch genommen werden darf oder - wenn eine Nutzung für private Zwecke akzeptiert wird - dass der Reisende diese Buchungen entsprechend deklariert, da ansonsten sämtliche Buchungsdaten an den Arbeitgeber gegeben werden.

Interessanter als die reinen Buchungsdaten sind für die Arbeitgeber weitere Analyse- und Bewertungsdaten, die Einsparpotenziale aufzeigen und die Möglichkeit geben, die Einhaltung ihrer Reiserichtlinien zu überprüfen.
Das Kreditkartenunternehmen erbringt auf diese Weise Controlling-Leistungen. So kann detailliert aufgezeigt werden, welches der günstigste Tarif für einen Flug gewesen wäre und warum dieser nicht gewährt werden konnte: Beispielsweise wegen zu später Buchung oder weil der Reisende eine bestimmte Fluggesellschaft gewählt hat, um Vielflieger-Bonuspunkte zu erhalten.
Wenn diese Daten als Rohdaten geliefert werden, könnte der Arbeitgeber durch eine individuelle Reiseverhaltensanalyse auch gezielt auswerten, welche "Mehrkosten" ein bestimmter Mitarbeiter verursacht hat.

Sicherlich besteht hieran ein legitimes Interesse des Arbeitgebers. Die Fairness gegenüber den Mitarbeitern gebietet es jedoch, dass solche Auswertungen bzw. die Ableitung konkreter Verhaltensvorwürfe aus den Auswertungen nur erfolgen, wenn der Mitarbeiter auch weiß, wie er sich korrekt zu verhalten hat und dass er insoweit kontrolliert wird.

Primär besteht hier die Verantwortung der Arbeitgeber. Die Datenschutzbeauftragten von Unternehmen, welche Corporate-Travel-Dienstleistungsverträge mit einem Reisebürounternehmen abschließen, sind daher aufgerufen, von vornherein mitzuwirken, damit die schutzwürdigen Belange der Mitarbeiter berücksichtigt werden.

Darüber hinaus ist auch das Kreditkarten- bzw. Reisebürounternehmen als übermittelnde Stelle nicht frei von jeder Verantwortung.

Die Aufsichtsbehörde hält die Übermittlung von "Analyse- und Bewertungsdaten" als Rohdaten nur für zulässig, wenn

- entsprechend konkrete Reiserichtlinien existieren und diese dem Mitarbeiter bekannt sind,
- sichergestellt ist, dass dem Mitarbeiter in der konkreten Buchungssituation bewusst ist bzw. dass er wissen kann, dass er gegebenenfalls gegen die Richtlinien verstößt (dies setzt voraus, dass er von den Reisebüro-

Mitarbeitern informiert wird, dass es beispielsweise einen günstigeren Flug gibt, wenn er eine andere Route wählt), und

- der Mitarbeiter darüber informiert wird, dass das Reisebürounternehmen umfassende Daten liefert, damit der Arbeitgeber die Einhaltung der Reiserichtlinien kontrollieren kann.

Das Kreditkarten- bzw. Reisebürounternehmen sollte sich daher vom Arbeitgeber versichern lassen, dass entsprechende Reiserichtlinien existieren und dass die Mitarbeiter die oben genannten Informationen erhalten haben.

Außerdem wurde dem Kreditkartenunternehmen empfohlen, den mit der Erstellung des Datenschutz-Faltblattes eingeschlagenen Weg fortzusetzen und selbst präzisere Informationen zu liefern.

Wenn die oben genannten Voraussetzungen nicht erfüllt sind, ist die Übermittlung von "Analyse- und Bewertungsdaten" (als Rohdaten) zumindest sehr problematisch. Es dürften dann grundsätzlich nur statistische Auswertungen geliefert werden.

b)
Die Buchungen werden über Corporate Travel vorgenommen, und zwischen dem Arbeitgeber und dem Kreditkarten- bzw. Reisebürounternehmen besteht eine Vereinbarung, dass die Buchungen über eine "Reisestellenkarte" (Business Travel Account = BTA) beglichen werden. Alle Reisen der Mitarbeiter werden über diese Karte abgerechnet, die für diese Firma eingerichtet wurde. Die volle Haftung liegt beim Arbeitgeber.

Hier steht außer Frage, dass der Arbeitgeber sämtliche Buchungs- bzw. Abrechnungsdaten erhalten darf und muss.

Soweit über die Abrechnungs-(Buchungs-)Daten hinaus auch weitere "Analyse- und Bewertungsdaten" als Rohdaten geliefert werden, gelten die obigen Ausführungen unter a) entsprechend.

c)
Es besteht nicht nur ein Corporate-Travel-Dienstleistungsvertrag, sondern auch eine Rahmenvereinbarung zwischen dem Arbeitgeber und dem Kreditkartenunternehmen über die Ausgabe von Corporate Cards an die Mitarbeiter. Die Bezahlung sämtlicher Reiseleistungen kann mit der Corporate Card erfolgen. Zwischen den einzelnen Mitarbeitern und dem Kreditkartenunternehmen bestehen separate Kreditkartenverträge, wobei es hinsichtlich der Haftung verschiedene Ausgestaltungsmöglichkeiten gibt:
In einer Variante verpflichten sich Arbeitgeber und Arbeitnehmer zu gesamtschuldnerischer Haftung für die Forderungen aus der Corporate Card.
In der anderen Variante ist der Arbeitnehmer allein für diese Forderungen haftbar.
Unabhängig davon kann die Abrechnung der Forderungen aus der Corporate Card entweder allein über den Arbeitgeber oder anteilig über Arbeitgeber und Arbeitnehmer sowie allein über den Arbeitnehmer erfolgen.

In allen Fällen ist dem Arbeitgeber ein zumindest teilweise berechtigtes Interesse an der Auswertung der Mitarbeiterreisen im Rahmen des § 28 Abs. 2 Nr. 1 a) BDSG zuzugestehen.

Unproblematisch erscheinen die Fälle, in denen der Arbeitnehmer von vornherein Kenntnis davon hat, dass die auf ihn ausgestellte Corporate Card ausschließlich zu dienstlichen Zwecken eingesetzt werden darf (ausdrückliches vorheriges Verbot der privaten Nutzung).
Beim rechtmäßigen Gebrauch der Karte enthalten die Übermittlungen in diesen Fällen dann nur dienstlich getätigte Ausgaben.
Daher können die Buchungs- und Abrechnungsdaten der über Corporate Travel gebuchten und zugleich mit der Corporate Card beglichenen Leistungen an den Arbeitgeber übermittelt werden.
Darüber hinaus können auch die Daten über solche "Reiseleistungen" übermittelt werden, die nicht zuvor über Corporate Travel gebucht wurden, beispielsweise Restaurantbesuche.

In den übrigen Fällen, in denen eine private Nutzung der Corporate Card nicht von vornherein ausgeschlossen wird, ist zu differenzieren.

Haftet der Arbeitgeber gemeinsam mit dem Arbeitnehmer gesamtschuldnerisch, so besteht auch dann ein berechtigtes Interesse an der Kenntnisnahme des gesamten Forderungsumfangs. Dabei muss der Arbeitnehmer jedoch vorab ausdrücklich Kenntnis von dem Umstand erlangen, dass dem Arbeitgeber alle mit der Corporate Card getätigten Ausgaben übermittelt werden.

Im Fall der alleinigen Haftung des Arbeitnehmers für alle mit der Corporate Card getätigten Ausgaben müssen sich die Übermittlungen an den Arbeitgeber auf die Ausgaben beschränken, die eindeutig dem dienstlichen Zweck zugeordnet werden können. Dies kann nur bei den über Corporate Travel gebuchten Leistungen (nach Maßgabe der obigen Ausführungen unter a) der Fall sein.

Hinsichtlich der (zusätzlichen) Übermittlung von Analyse- und Bewertungsdaten gelten die obigen Ausführungen unter a) entsprechend.

Der Arbeitnehmer ist mit Ausstellung der Corporate Card und Abschluss des für ihn gültigen Kartenvertrages über die jeweiligen Übermittlungsbedingungen in Kenntnis zu setzen.

8.2 Erhebung von Daten für die Corporate Card

Wie bereits unter 7.1 ausgeführt, schließen Unternehmen oftmals Rahmenvereinbarungen mit Kreditkartenunternehmen ab, aufgrund derer die Mitarbeiter dann zu besonderen Konditionen einen Kreditkartenvertrag (so genannte Corporate Card) abschließen können.

Hier stellt sich dann die Frage, in welchem Umfang das Kreditkartenunternehmen Daten über den Mitarbeiter erheben darf.

Eine pauschale Ermächtigungsklausel in den Allgemeinen Geschäftsbedingungen des Corporate-Card-Vertrages, "bankübliche Arbeitgeberauskünfte" einzuholen, ist unwirksam.

Abgesehen davon, dass die erforderliche Hervorhebung im äußeren Erscheinungsbild fehlt und das Unterschriftserfordernis nicht erfüllt ist (§ 4 Abs. 2 BDSG), wenn die Klausel nur in den Allgemeinen Geschäftsbedingungen enthalten ist, mangelt es auch an der erforderlichen Bestimmtheit:

Der Begriff der "banküblichen" Auskünfte entsprechend dem gemeinsamen Kommuniqué der Datenschutzaufsichtsbehörden und den Vertretern des Bankgewerbes zum Bankauskunftsverfahren, dürfte zur Eingrenzung von Arbeitgeberauskünften kaum geeignet sein.

Das Kreditkartenunternehmen versicherte zwar, dass es von der Auskunftsklausel, die auch in den "normalen" Kartenanträgen enthalten ist, nur in besonderen Einzelfällen Gebrauch mache, wenn die vorhandenen Angaben nicht plausibel seien und für eine Bonitätsbewertung nicht reichen.

Dabei verwies das Unternehmen darauf, dass es bei seinen Karten kein Ausgabelimit gibt und dass der Kartenherausgeber keine Bank sei, sodass keinerlei Erkenntnisse über die Einkommens- und Vermögenssituation vorlägen.

Bei Corporate-Card-Anträgen seien bislang noch keine Arbeitgeberauskünfte für die Kreditwürdigkeitsprüfung eingeholt worden. Nach Auffassung der Aufsichtsbehörde sollte in den Sonderfällen, in denen eine Arbeitgeberauskunft benötigt wird, eine separate konkrete Einwilligung eingeholt werden. Zumindest müsste die Klausel präzisiert werden.

Darüber hinaus ist die besondere Situation bei der Corporate Card zu berücksichtigen:

Für den betroffenen Arbeitnehmer kann unter Umständen eine gewisse Zwangssituation gegeben sein, die Karte zu beantragen und für Geschäftsreisen zu nutzen, wenn er Nachteile vermeiden will (eventuell müsste er selbst in Vorlage treten - währenddessen bei der Corporate Card dies wegen eines längeren Zahlungsziels gegebenenfalls entfällt).

Von daher ist das Problem der Freiwilligkeit von Einwilligungserklärungen besonders kritisch zu bewerten.

Wenn ein Antrag nicht vollständig ausgefüllt ist, der Antragsteller nicht erreichbar ist, aber die Karte in Kürze benötigt wird, wären Rückfragen beim Arbeitgeber zu allgemeinen Angaben wie der Firmenzugehörigkeit, Abteilung, Kostenstelle etc. zulässig - eventuell sogar ohne Einwilligung.

Weitergehende Auskünfte zur Kreditwürdigkeitsprüfung sind nicht gerechtfertigt, wenn in dem Rahmenvertrag mit dem Arbeitgeber dessen gesamtschuldnerische (Mit-)Haftung vereinbart wurde, da dann das Ausfallrisiko für das Kreditkartenunternehmen gering ist.

Wenn keine gesamtschuldnerische Haftung vereinbart wurde, besteht zwar ein Risiko für das Kreditkartenunternehmen, aber je stärker eventuell der faktische Zwang zur Beantragung einer Corporate Card ist, desto gewichtiger sind die schutzwürdigen Belange der Arbeitnehmer bzgl. einer Offenbarung ihrer Daten gegenüber dem Kreditkartenunternehmen.

Hier sind daher auch die Datenschutzbeauftragten der Unternehmen, welche Rahmenvereinbarungen abschließen, gefordert, sachgerechte Lösungen mit dem Kreditkartenunternehmen zu finden.

Im konkreten Fall konnte der Datenschutzbeauftragte mit Unterstützung der Aufsichtsbehörde und im Zusammenwirken mit der Datenschutzbeauftragten des Kreditkartenunternehmens erreichen, dass die Kartenantragsformulare für die Mitarbeiter des Unternehmens entsprechend abgeändert wurden (d.h. lediglich in dringenden Fällen erfolgen Rückfragen beim Arbeitgeber bezüglich Angaben zur Person).

8.3 Datenerhebung bei Kreditkarten

Neben dem Problem des Volumens der Datenerhebung sind die Verfahrensabläufe für die Kreditkartenkunden teilweise wenig nachvollziehbar.

In einem Beschwerdefall waren bei der Herausgabe und laufenden Abwicklung der Karte insgesamt drei Unternehmen beteiligt. Eine Bank gab gemeinsam mit einem weiteren (vor allem auf Privatkunden spezialisierten) Unternehmen eine Kreditkarte heraus (Cobranding).
Der Kunde unterhielt damit Geschäftsbeziehungen zu zwei Unternehmen, wobei die Nichtbank von dem Kunden nur nähere Kenntnisse erlangte, wenn er bei ihr Dienstleistungen direkt mit seiner neuen Kreditkarte bezahlte.
Für den Betroffenen überraschend war, dass auch die Bank selbst von ihm keine nähere Kenntnis hatte. Die gesamte Abwicklung der Kreditkarte (processing), einschließlich der Bonitätsprüfung, geschah bei einem darauf spezialisierten Dienstleister.
Der Betroffene war zwar bereit, sich gegenüber einer Bank bezüglich seiner Vermögensverhältnisse zu offenbaren, dieses Vertrauen erstreckte sich jedoch nicht auf einen anonymen Dienstleister. Da der Kartenkunde aber bereits im Kartenantrag auf den Dienstleister hingewiesen wurde, war die geschilderte Arbeitsweise im Grundsatz nicht zu beanstanden.
Es wäre jedoch wünschenswert, wenn für die Kartenkunden die Informationsflüsse und die Rollenverteilung der beteiligten Unternehmen transparenter gestaltet würden.
Da der Dienstleister eigenständig Bonitätskontrollen durchführt und über die Herausgabe der Karten entscheidet, liegt keine Auftragsdatenerarbeitung, sondern eine Funktionsübertragung vor.
Daher sollte im Briefkopf von Schreiben des Dienstleisters nicht nur das Cobranding Unternehmen, sondern sinnvollerweise auch der Dienstleister genannt werden.

9. Neue Medien, Internet-Provider

9.1 Einsatz von Cookies zur Profilbildung

Die Abstimmung der Angebote und Werbung auf einen bestimmten Kunden wird immer wichtiger - so lautet das Credo der Marketingfachleute.

Dies gilt selbstverständlich auch für Angebote und Werbung im Internet. Internet-Unternehmen sind daher sehr daran interessiert, das Verhalten der

Internet-Nutzer zu verfolgen und zu analysieren, entsprechende Daten zu sammeln und hieraus Profile zu erstellen.

Ein in den USA ansässiges Unternehmen verfügt dort über mehr als 30 Millionen Profile von Web-Nutzern. Es ist in den USA ein führender Anbieter von Produkten und Dienstleistungen, die es Online-Publishern, Werbungstreibenden und Händlern ermöglichen, zielgerichtete Online-Werbung, Inhalte und e-Commerce-Angebote auszuliefern und ihre Wirksamkeit zu messen. Mit der Gründung einer Niederlassung im Rhein-Main-Gebiet soll das Unternehmenskonzept auch in Deutschland umgesetzt werden. Daher wurde die Aufsichtsbehörde um eine datenschutzrechtliche Bewertung gebeten.

Das Unternehmenskonzept wurde wie folgt erläutert:

- Datenerhebung und Aufbau der Datenbank beim Unternehmen (im Folgenden: Unternehmen X)

  Sobald ein Internetnutzer eine Web Site eines Vertragspartners des Unternehmens X (im Folgenden: Anbieter) aufruft, werden zwei Cookies gesetzt: Das Unternehmen X setzt ein Cookie und der Anbieter setzt ein Cookie. Bei Cookies handelt es sich um kleine Dateien, die auf den Rechnern der Nutzer abgelegt werden und beispielsweise der Erstellung von Nutzerprofilen dienen.
  Die vom Unternehmen X und den Anbietern gesetzten Cookies enthalten nur Identifikationsschlüssel (ID).

  Jeder Anbieter setzt sein eigenes Cookie für jede Web Site.

  Das Unternehmen X kann das Cookie des Anbieters nicht direkt lesen. Stattdessen sendet der Anbieter sein (Identifikations-)Cookie zum Unternehmen X, sodass dieses eine sichere Kreuzreferenz (cross reference) zwischen dem Cookie des Anbieters und dem eigenen Cookie herstellen kann. Der Anbieter hat keinen Zugang zum Cookie des Unternehmens X. Der Anbieter kann auch nicht sehen, ob und welche Web Sites anderer Anbieter der Internet-Surfer besucht hat. Diese Technik wird als "dual-blind-identification" bezeichnet.

  Von der eigenen Software gesteuert, erhält das Unternehmen X das eigene Cookie (d.h. die Identifikation), die IP-Adresse des Besuchers, die URL der besuchten Webseite, Datum und Zeit(-dauer) des Besuchs sowie Angaben zum Betriebssystem (z.B. Windows 95) und die Version des genutzten Browsers (z.B. welche Explorerversion) - so genannte Klickstromdaten.

  Die IP-Adresse wird verwendet, um den Domaintyp und - soweit möglich - die geographische Region zu ermitteln.
  Jeder URL, also jeder Webseite, sind ein oder mehrere Interessen zugeordnet. Üblicherweise kategorisiert der Anbieter seine Seiten selbst (z.B. "Verbraucherelektronik" mit den Unterkategorien "camcorders", "Home Audio" etc.).
  Nach dieser Auswertung werden die IP-Adresse und die URL gelöscht.

  Der Verlauf der Interessen - entsprechend dem Besuch betreffender Webseiten - wird gemäß eines zum Patent angemeldeten Algorithmus aggregiert, der die Dauer, die Häufigkeit, die wiederkehrenden Interessen sowie die Zeitspanne, seit dem ein bestimmtes Interesse als Letztes gezeigt wurde, einbezieht.

  Das Unternehmen X sammelt auch eine Reihe demographischer Daten (Altersspanne, Geschlecht, geographische Lage [bis zur Stadt, nicht Straße], Vorhandensein von Kindern, Ausbildung, Einkommensspanne und Beruf).
  Teilweise werden diese automatisiert aus den Interessen ermittelt bzw. einfach als statistische Annahme zugeordnet (z.B. Besucher, die Fußball-Sites besuchen, sind meist Männer) - die Daten werden also aus den Klickstromdaten abgeleitet.
  Einige Anbieter sammeln solche Informationen aber auch durch Umfragen und Registrierungsformulare (Bestellformulare oder Ähnliches).
  Hieraus werden die oben genannten demographischen Daten mit Hilfe des Cookies des Kunden als Identifikation und entsprechend dem oben

beschriebenen cross-reference-Verfahrens an das Unternehmen X übermittelt und dem jeweiligen Nutzer zugeordnet.

Ferner erhält das Unternehmen X in den USA von dortigen Anbietern auch Daten aus Suchabfragen.

- Nutzung der Datenbank durch Kunden des Unternehmens X (Anbieter)

  Die Datenbank und spezielle Softwareprodukte des Unternehmens X ermöglichen es, Werbeeinblendungen im Internet genau auf das gespeicherte Interessenprofil des jeweiligen Nutzers (bzw. der Rechner-Nutzer) zuzuschneiden.
  Dabei kann die Werbung sowohl als vollseitige Werbung (Ad-Break) als auch als Bannerwerbung geschaltet werden.
  Ebenso kann die Produktdarstellung im Internet genau auf das jeweilige Interessensprofil ausgerichtet werden.

  Entsprechend dem in den USA verwirklichten Konzept sollten die Profile komplett den Anbietern übermittelt werden (zum Zwecke der dortigen Weiterverarbeitung während einer Websession - lediglich das dauerhafte Speichern war vertraglich verboten).

  Schließlich kündigte das Unternehmen X jedoch Änderungen am Geschäftsmodell an:

  Die Nutzung der Profile soll ausschließlich auf das Aussenden von Werbung beschränkt werden. Die Profile sollen den Anbietern nicht mehr übermittelt werden, sondern ausschließlich zentral im Server des Unternehmens X gespeichert werden.
  Profilbasierte Werbung soll alleine durch den zentralen Server des Unternehmens X ausgeliefert werden.
  Die Profildaten sollen in einer sicheren Umgebung gehalten werden.

  Bei dieser geplanten Neukonzeption würde voraussichtlich nur ein Cookie pro Web-Nutzer gesetzt werden (d.h. das Cookie des Unternehmen X). Genaueres wird noch zu klären sein.

Wegen der grundsätzlichen Bedeutung der Angelegenheit wurde diese auf Initiative der Aufsichtsbehörde in der von den obersten Aufsichtsbehörden für den Datenschutz gebildeten Arbeitsgruppe "Telekommunikation, Tele- und Mediendienste" erörtert.
Auf der Grundlage dieser Diskussion kam die Aufsichtsbehörde zu folgender grundsätzlicher Bewertung:

Die in den Cookies enthaltenen Identifikationsschlüssel sind Pseudonyme.

Auch bei den durch die Anbieter von den Nutzern erhobenen und an das Unternehmen X übermittelten IP-Nummern handelt es sich (zumindest) um Pseudonyme.

Die bei dem Unternehmen X gespeicherten Nutzungsprofile sind somit (zumindest) pseudonyme Profile.

Der Begriff "Pseudonym" ist nur in § 4 Abs. 4 Teledienstedatenschutzgesetz (TDDSG) und § 7 TDDSG (sowie in den gleich lautenden Bestimmungen des § 13 Abs. 4 Mediendienstestaatsvertrag (MDStV) und § 16 Abs. 1 MDStV) erwähnt, aber nicht definiert.

Pseudonyme sind "erfundene Namen" oder Kennzeichen, die aus sich heraus die Identität des Nutzers nicht zu erkennen geben, sondern erst über eine entsprechende Zuordnungsvorschrift (Referenzliste) erschlossen werden können.
Diese Voraussetzungen erfüllen die Cookie-Identifikationsschlüssel und die IP-Nummern.

Da das TDDSG und der MDStV nur für "personenbezogene Daten" gelten (§ 1 Abs. 1 TDDSG und § 12 As. 1 MDStV), stellt sich die Frage, ob beziehungsweise inwieweit für pseudonyme Daten das TDDSG bzw. der MDStV überhaupt gilt.

Wie sich bereits aus dem Umkehrschluss aus § 4 Abs. 4 TDDSG und § 7 TDDSG (bzw. den entsprechenden Regelungen des MDStV) ergibt, geht der Gesetzgeber davon aus, dass bei pseudonymen Nutzungsprofilen der Personenbezug nicht (vollständig) aufgehoben ist.

Allenfalls dann, wenn die Zuordnungsvorschrift überhaupt nicht bzw. nicht auf legalem Wege zugänglich wäre, könnte der Personenbezug entfallen sein. Dies könnte bei vom Betroffenen selbstgenerierten Pseudonymen unter Umständen der Fall sein. Vorliegend trifft dies jedoch nicht zu, wie nachfolgend noch näher erläutert werden wird.

Das TDDSG (bzw. der MDStV) ist daher einschlägig.

Im Einzelnen ergeben sich folgende Anforderungen:

- Unterrichtungspflicht

  Bereits das Setzen der Cookies setzt eine Unterrichtung nach § 3 Abs. 5 Satz 2 TDDSG (bzw. § 12 Abs. 6 Satz 2 MDStV) voraus.
  Bei dem geplanten Einsatz der Cookie-Technik handelt es sich um ein automatisiertes Verfahren, welches es ermöglicht, die gesamten Nutzungsdaten einem Nutzer zuzuordnen und die Erhebung, Verarbeitung und Nutzung personenbezogener Daten vorzubereiten, denn mittels des Identifikationsschlüssels und der IP-Nummer kann unter Umständen ein Personenbezug hergestellt werden.
  Dies gilt zunächst für die Fälle, in denen die Anbieter in ihrem Angebot ein Bestellformular oder ein sonstiges Registrierungsformular vorhalten, mittels derer Name und Anschrift der Nutzer erfasst werden können.
  In diesen Fällen ist die IP-Nummer ebenso eindeutig personenbeziehbar wie für den jeweiligen Provider der Nutzer.
  Aber auch in den Fällen, in denen ein solches Formular nicht vorgesehen ist, besteht eine Unterrichtungspflicht, denn es ist zu berücksichtigen, dass es neben den überwiegend vergebenen dynamischen IP-Nummern auch statische IP-Nummern gibt. Diese können unter Umständen einem Nutzer, also einer natürlichen Person, zugeordnet werden. Da solche eindeutig personenbezogenen IP-Nummern zu einem relevanten Anteil in dem Gesamt-Adressraum der vergebenen IP-Nummern enthalten sind, sind IP-Nummern insgesamt keine anonymen Daten.

  Im Übrigen erfordert jedenfalls eine grundrechtskonforme Auslegung des § 3 Abs. 5 Satz 2 TDDSG im Lichte des Rechts auf informationelle Selbstbestimmung, dass eine Information erfolgt, bevor eine systematische und individuelle Registrierung und Profilbildung mittels Cookies erfolgt.

  Die Unterrichtung muss also erfolgen, bevor ein Cookie gesetzt wird. Das heißt, ein Cookie darf erst gesetzt werden, wenn der Nutzer die Seite, welche die Unterrichtung enthält, verlassen hat.

  Die wesentlichen Informationen müssen im sichtbaren Bereich der Webseite, in deutlich wahrnehmbarer Form unmittelbar eingeblendet werden.
  Zu den Kerninformationen gehört die Angabe, dass das Nutzungsverhalten und gegebenenfalls Daten aus Suchabfragen erfasst werden und zur Profilbildung bei einem Dienstleister verwendet werden. Ferner muss der Verwendungszweck der Profile angegeben werden (Werbung). Außerdem muss ein Hinweis auf weitere Informationsmöglichkeiten enthalten sein ("Info-Button").

  Diese Informationen müssen auch später jederzeit abrufbar sein (§ 3 Abs. 5 Satz 3 TDDSG).

- Gestaltungsmöglichkeit

  Das Erheben der IP-Nummern und Nutzungsdaten durch die Anbieter und die Weiterleitung an das Unternehmen X wäre nach § 3 Abs. 1 TDDSG (bzw. § 12 Abs. 2 MDStV) nur zulässig, wenn hierfür ein Erlaubnistatbestand gegeben wäre.

  § 4 Abs. 4 TDDSG ist hier insoweit kein ausreichender Erlaubnistatbestand. Aus der Gesetzesbegründung ergibt sich, dass mit dieser Vor-

schrift ein Kompromiss zwischen dem Interesse des Nutzers an weitgehender Anonymität seines Konsumentenverhaltens und dem berechtigten Interesse "des Diensteanbieters", die Inanspruchnahme der Teledienste auszuwerten, ermöglicht werden sollte. Die Regelung in § 4 Abs. 4 TDDSG ist daher so zu verstehen, dass nur der jeweilige Anbieter pseudonyme Nutzungsprofile aus der Inanspruchnahme seiner eigenen Dienste erstellen darf. Anbieterübergreifende pseudonyme Profile sollten nicht erlaubt werden. (Gleiches gilt für die gleich lautende Bestimmung im § 13 Abs. 4 MDStV.). Folglich ist im vorliegenden Fall grundsätzlich eine Einwilligung der Nutzer erforderlich.

Allerdings ist zu berücksichtigen, dass der Begriff der pseudonymen Daten vom Gesetzgeber quasi zwischen den Begriff der personenbezogenen Daten und den Begriff der (völlig) anonymen Daten eingeschoben wurde. Wenngleich pseudonyme Daten - wie oben ausgeführt - im Grundsatz als ein Unterfall der personenbezogenen Daten zu bewerten sind, so sind sie doch nicht völlig identisch mit diesen.

Eine sachgerechte Auslegung des TDDSG bzw. des MDStV kann daher eine Differenzierung rechtfertigen.

Bei einer hinreichend starken Pseudonymisierung, d.h. wenn die Möglichkeit und Wahrscheinlichkeit, dass die Daten einer bestimmten Person zugeordnet werden können, gering ist, genügt eine Widerspruchsmöglichkeit ("opt-out").

Soweit also im konkreten Fall der jeweilige Anbieter keine Erhebung von Adressdaten der Nutzer durch Formulare etc. vorsieht und auch das Unternehmen X durch organisatorische Vorkehrungen sicherstellt, dass kein Personenbezug hergestellt wird, reicht ein opt-out.
Auf diese Möglichkeit muss jedoch deutlich hingewiesen werden, und die Ausübung muss leicht und unmittelbar möglich sein. Das opt-out muss jederzeit, also auch nachträglich (nach dem Setzen des Cookies), möglich sein.
Deshalb muss mit dem Abruf des Inhaltes der Unterrichtung (siehe oben) auch unmittelbar die opt-out-Möglichkeit verfügbar sein.
Wenn der Nutzer von der opt-out-Möglichkeit Gebrauch macht, darf ihm das Angebot grundsätzlich nicht vorenthalten werden (vgl. § 3 Abs. 3 TDDSG, § 12 Abs. 4 MDStV).
Es muss sichergestellt werden, dass keine weiteren Cookies mehr gesetzt werden (z.B. durch ein Sperr-Cookie).
Ferner müssen nach einem opt-out die Profildaten des betreffenden Nutzers in der Datenbank gelöscht werden.

- Auskunftsrecht

  Der Nutzer muss nach § 7 TDDSG (§ 16 Abs. 1 MDStV) die Möglichkeit haben, sein pseudonymes Nutzungsprofil auf Wunsch elektronisch einzusehen.
  Die Auskunft muss in der Weise gewährt werden, dass sich der Nutzer durch sein Auskunftsersuchen nicht gegenüber dem Anbieter oder dem Unternehmen X namentlich identifizieren muss.
  Gleichzeitig soll ein Verfahren bereitgestellt werden, bei dem sichergestellt ist, dass die Auskunft nur den berechtigten Empfänger erreicht.

  Das Unternehmen X versprach, konkrete Vorschläge zur Realisierung dieser Anforderungen zu erarbeiten.

9.2 Zulässigkeit der Veröffentlichung personenbezogener Daten im Internet durch die deutsche Vergabestelle für Internet-Domains DENIC eG

Die DENIC eG in Frankfurt am Main ist die zentrale deutsche Vergabe- und Registraturstelle für Internet-Domains unterhalb der Top Level Domain ".DE" (z.B. "hessen.de" oder "rp-darmstadt.de"). Die DENIC eG betreibt im Rahmen des Domain Name Systems (DNS) den Primary-Nameserver für alle deutschen Internet-Domains. Dieses hierarchische System sorgt dafür, dass weltweit jede Internet-Adresse einmalig und eindeutig ist und stellt somit die Basis jeder Internet-Nutzung dar. Mitglieder der DENIC eG sind deutsche Internet Service Provider, die ihren Kunden unter anderem auch die Registrierung einer eigenen Domain in der Form "www.wunschname.de" und auch

den Speicherplatz für eine entsprechende Homepage im World Wide Web (WWW) auf den Provider-Rechnern anbieten. Die Registrierung der gewünschten Domain der privaten Endkunden bei der DENIC eG erfolgt über die Internet Service Provider, die gegenüber ihren Kunden als günstige Domain-Weiterverkäufer auftreten.
Für die Registrierung einer Domain verlangt die DENIC eG neben den erforderlichen technischen Daten auch die Angabe von Name und Anschrift der antragstellenden Person/Organisation (Domain-Inhaber) sowie die entsprechenden Angaben zum technischen Ansprechpartner und zum administrativen Ansprechpartner (als Adressat für Rückfragen und rechtlich für die Domain verantwortliche Person). Bzgl. des technischen und des administrativen Ansprechpartners wird außerdem die Angabe der Telefonnummer oder alternativ (gegebenenfalls auch zusätzlich) der Telefaxnummer und der E-Mail-Adresse gefordert.

Die Daten zum Domain-Inhaber werden sowohl in der Who-is-Datenbank der DENIC eG gespeichert als auch in der Datenbank des RIPE (Réseaux IP Européen) in Holland, wo alle DNS-Daten für den europäischen Bereich gesammelt werden. Über den so genannten Who-is-Dienst sind die Daten bei beiden Institutionen weltweit abrufbar.

Die kompletten Daten der administrativen und technischen Ansprechpartner sind nur bei RIPE gespeichert, bei DENIC befinden sich nur die Kürzel (NIC-Handle), allerdings sind auch die Namen und Telefonnummern über einen Zeiger auf die RIPE-Datenbank bei DENIC abrufbar.

Bei den Petenten, die sich an die Aufsichtsbehörde gewandt haben, handelt es sich ausschließlich um Privatpersonen, die ein eigenes auf Dauer gerichtetes Angebot im Internet in Form einer WWW-Homepage bereithalten und die Aufsichtsbehörde um Überprüfung der Zulässigkeit der Veröffentlichung ihrer Daten durch die DENIC eG im World Wide Web (WWW) baten.

Die Veröffentlichung von Name und Anschrift der Domain-Inhaber bei der DENIC eG ist nicht zu beanstanden, da dies sowohl aus technischen, aber vor allem auch aus rechtlichen Gründen erforderlich ist, um den zuverlässigen Betrieb des Netzes in Deutschland sicherzustellen. So bietet die Preisgabe von Name und Anschrift der Domaininhaber z.B. Anknüpfungspunkte für Fragen des Namens-, Urheber- oder Lizenzrechtes und trägt auch erheblich zur Förderung der Rechtssicherheit i.S.d. Verbraucherschutzes im Internet bei. Zusätzlich ist zu berücksichtigen, dass die Beschwerdeführer als Anbieter von Tele- oder Mediendiensten nach dem MDStV und dem Teledienstegesetz (TDG) ohnehin verpflichtet sind, ein Impressum mit Name und Anschrift auf ihren WWW-Seiten zu führen und deshalb bezüglich dieser Daten kein schutzwürdiges Geheimhaltungsinteresse geltend machen können, soweit sie unter dem registrierten Domain-Namen eine WWW-Site unterhalten.

Für die Veröffentlichung von Telefon- und Telefaxnummern der privaten Domain-Inhaber unter dem Eintrag als administrativer oder technischer Ansprechpartner gilt dies allerdings nicht, da diese Veröffentlichungen für die oben genannten Zwecke nicht erforderlich ist. Auch hat der Gesetzgeber die Impressumspflicht im MDStV und TDG ausdrücklich auf die Angabe von Name und Anschrift begrenzt. Ein Anbieter ist daher nicht verpflichtet, im Impressum seines Tele- oder Mediendienstes eine Telefon- oder Telefaxnummer anzugeben.

Die DENIC eG begründete auf Nachfrage die Veröffentlichung der Telefonnummer damit, dass in Fällen von technischen Fehlfunktionen eine schnelle telefonische Erreichbarkeit der Domain-Eigner zur Fehlerbehebung sichergestellt werden müsse, um die Aufrechterhaltung des Internet-Betriebes in Deutschland zu gewährleisten. Diese Argumentation konnte die Aufsichtsbehörde allerdings nicht überzeugen, da gerade den Privatpersonen, die ihre Domain über einen großen Provider registriert haben, normalerweise keine technischen Möglichkeiten zur Fehlerbehebung zur Verfügung stehen. Diese Privatpersonen haben für ihre Domain oftmals lediglich Speicherplatz bei ihrem Provider angemietet, bei dem der Seiteninhalt auch abgelegt ist. Dort wird auch die technische Infrastruktur für das Internet-Angebot vorgehalten. In der Regel wird daher wohl immer der dahinter stehende technische Dienstleister (Provider) in Anspruch genommen werden müssen, wenn ein eklatanter technischer Fehler behoben werden muss. Es genügt zum Zweck

der Behebung technischer Probleme nach Auffassung der Aufsichtsbehörde also durchaus, lediglich die Telefonnummer des technischen Dienstleisters (Provider) im Eintrag "tech-c" zu veröffentlichen.

Die DENIC hat daher mittlerweile die Anzeige der Telefonnummern der privaten Domain-Inhaber bei der Who-is-Abfrage unterdrückt.
Seit Mitte 1999 bot die DENIC eG zusätzlich die Möglichkeit an, ohne Angabe einer IP-Nummer oder eines Domain-Namens nach Personennamen in der DENIC-Datenbank zu suchen. Als Ergebnis erhalten die Anfrager eine Auflistung sämtlicher Personen des gesuchten Namens, unabhängig von deren Domain. Diese Funktion ist zu Aufrechterhaltung des Internet-Datenverkehrs weder dienlich noch erforderlich, wie die DENIC eG selbst einräumte. Diese Abfragevariante wurde von der DENIC eG nach der Beanstandung durch die Aufsichtsbehörde umgehend eingestellt.

Bis zur Fertigstellung dieses Berichtes waren alle beanstandeten Abfragemöglichkeiten aber noch bei RIPE vorhanden, sodass weiter zu klären sein wird, wie dies abgestellt werden kann. Möglicherweise lässt sich das Problem im Zuge der angekündigten Umstellung des Vergabesystems lösen.

Auch für die Provider besteht rechtlicher Handlungsbedarf. Diese weisen ihre Kunden zum großen Teil nicht oder nur unzureichend auf die Eintragung und Veröffentlichung ihrer Daten bei der DENIC eG hin. Eine informierte Einwilligung (§ 4 Abs. 2 BDSG) in die Übermittlung und anschließende Veröffentlichung der Telefonnummer im WWW liegt den Providern in der Regel auch nicht vor. Oftmals ist lediglich ein kurzer Hinweis im so genannten "Kleingedruckten" der Provider-AGB zu finden, mit dem diese Internet-Anbieter allerdings Ihrer Unterrichtungspflicht nach § 3 Abs. 5 TDDSG nicht im erforderlichen Umfang nachkommen. Ein einfacher Hinweis in den AGB reicht nicht aus. Das führt dazu, dass die DENIC eG vielen Domaininhabern aus dem Privatbereich unbekannt bleibt. Die Betroffenen sind weder über Details der Domain-Vergabe noch über die Veröffentlichungspraxis der DENIC eG informiert. Aus dieser Situation, die im Wesentlichen durch mangelnde Transparenz gekennzeichnet ist, entstehen immer wieder Irritationen, die letztlich zu Eingaben und Beschwerden von Domaininhabern bei der Datenschutzaufsichtsbehörde führen.

Die DENIC eG hat sich bereit erklärt, die Problematik mit den Providern zu diskutieren, damit diese ihrer Unterrichtungspflicht bei Vertragsabschluss mit den Kunden nachkommen. Die Übermittlung der Telefonnummer (oder Telefaxnummer) von privaten Domain-Inhabern an DENIC eG und die Veröffentlichung für die Who-is-Abfrage soll künftig nur noch erfolgen, wenn dem Provider eine ausdrückliche freiwillige Einwilligung des betroffenen Domain-Inhabers bzw. des administrativen Ansprechpartners vorliegt.

Die Aufsichtsbehörde wird die Angelegenheit weiter verfolgen, insbesondere ist es wichtig, dass die neue Verfahrensweise auch bezüglich der RIPE-Datenbank umgesetzt wird.

9.3 Postfach im Impressum und bei der DENIC eG ausreichend?

Der Inhaber einer Homepage, in der er sich engagiert gegen bestimmte gesundheitsschädliche Verhaltensweisen seiner Mitmenschen wendet, hatte über seinen Provider die Registrierung einer eigenen Domain bei der DENIC eG beantragt.

Er beschwerte sich darüber, dass die DENIC eG seine Anschrift mit Straße und Hausnummer veröffentlichen will.
Da er Repressalien von Mitbürgern befürchtet, die mit seiner Kampagne nicht einverstanden sind oder sich angegriffen fühlen, wollte er nur die Veröffentlichung des Postfachs akzeptieren.

Wie oben unter 9.2 ausgeführt, will die DENIC eG mit der Veröffentlichung von Name und Anschrift der Domain-Inhaber ermöglichen, dass rechtliche Schritte, insbesondere bei etwaigen Namens-, Urheber- und Lizenzrechtsfragen, eingeleitet werden können. Die Zielsetzung deckt sich daher teilweise mit der Anbieterkennzeichnungspflicht ("Impressumspflicht"). Soweit diese reicht, besteht jedenfalls kein schutzwürdiges Geheimhaltungsinteresse der Betroffenen.

Daher stellt sich die grundsätzliche Frage nach dem Umfang der Anbieterkennzeichnungspflicht nach § 6 MDStV und § 6 TDG. Beide Vorschriften verlangen die Angabe von Name und Anschrift, ohne den Begriff der "Anschrift" näher zu erläutern.

Dem Zweck der Anbieterkennzeichnungspflicht nach müssen Name und Anschrift geeignet sein, den Nutzer in die Lage zu versetzen, seine Rechte gegenüber dem Anbieter wirksam geltend zu machen. Es muss deshalb eine ladungsfähige Anschrift angegeben werden, weil sonst eine Klageschrift oder ein Antrag auf Erlass einer einstweiligen Verfügung nicht zugestellt werden kann. Daher müssen neben Postleitzahl und Ort die Straße und Hausnummer angegeben werden.

Die Angabe der Postleitzahl hält die Aufsichtsbehörde für unzureichend, da die Vorschriften der Zivilprozessordnung über die Zustellung voraussetzen, dass der Ort der Wohnung (bzw. - falls vorhanden - eines Geschäftslokals) bekannt ist (vgl. §§ 170, 181, 183 Zivilprozessordnung (ZPO)). Selbst eine Ersatzzustellung durch Niederlegung des zu übergebenden Schriftstückes bei der Postanstalt etc. (§ 182 ZPO) setzt voraus, dass eine schriftliche Mitteilung über die Niederlegung am Ort der Zustellung abzugeben ist. Diese Mitteilung hat auch dann unter der Wohnanschrift zu erfolgen, wenn der Adressat ein Postfach unterhält, d.h. die Einlegung in das Postfach würde nicht genügen (Zöller, Zivilprozessordnung, 20. Auflage, § 182 Rdnr. 3; Bay OLG NJW 1963, 600, BSG NJW 1967, 903; BFH NJW 1984, 448).

Der Schutzzweck der Norm erfordert es insbesondere, Rechtsschutzmaßnahmen auch in gerichtlichen Eilverfahren ergreifen zu können. Die Kenntnis nur des Postfachs würde einen schnellen Rechtsschutz erschweren und ist daher unzureichend (ebenso Roßnagel, Recht der Multimedia-Dienste, § 6 MDStV, Rdn. 33).

9.4 Veröffentlichung des Telefonverzeichnisses einer Gemeindeverwaltung im Internet

Ein Bürgermeisterkandidat wollte während des Wahlkampfes die Möglichkeiten und den Nutzen des Internet aufzeigen.

Zu diesem Zweck ließ er sich eine Domain auf den Namen der Gemeinde registrieren und erstellte eine Homepage. Auf dieser veröffentlichte er neben einigen Informationen über seine Person und seine Ziele auch das komplette Telefonverzeichnis der Gemeindeverwaltung mit Namen, Dienst-Telefonnummern und dem Amt (z.B. Hauptamt, Ordnungsamt) bzw. mit der Funktion (z.B. Hauptamtsleiter).

Eine Reihe von Bediensteten beschwerte sich hierüber beim Datenschutzbeauftragten der Gemeinde. Die Veröffentlichung war jedoch weder mit diesem noch mit sonstigen Vertretern der Gemeinde abgestimmt.
Einige betroffene Bedienstete nehmen nur Schreibaufgaben oder sonstige interne Aufgaben wahr, bei denen sie gegenüber den Bürgern nicht in Erscheinung treten.

Für die Bewertung der Zulässigkeit der Veröffentlichung sind weder das TDDSG noch der MDStV maßgeblich, sondern das BDSG, denn es geht hier eindeutig um die Inhaltsebene.
Das BDSG ist einschlägig, da die Veröffentlichung im Internet (HTML-Datei) im Kontext mit der Bewerbung als Bürgermeister erfolgte und somit (auch) beruflichen Zwecken i.S.d. § 1 Abs. 2 Nr. 3 BDSG diente.
Außerdem handelt es sich zumindest um eine "geschäftsmäßige" Datenverarbeitung i.S.d. § 1 Abs. 2 Nr. 3 BDSG, denn sie war auf eine gewisse Dauer gerichtet und nicht auf den rein privaten Bereich begrenzt.
Der Begriff der Geschäftsmäßigkeit in § 1 Abs. 2 Nr. 3 BDSG setzt nicht voraus, dass die Datenverarbeitung gewerblichen oder kommerziellen Zwecken dient.

Wenn eine Kommune die Namen und Dienst-Telefonnummern ihrer Bediensteten im Internet veröffentlichen will, ist dies nach Maßgabe des dann anzuwendenden Landesdatenschutzgesetzes nur zulässig, wenn die dienstliche Funktion es erfordert, dass Bedienstete nach außen auftreten. Jedenfalls bei rein intern wirkenden Verwaltungstätigkeiten (z.B. im Schreibdienst, Botendienst, Registratur, Telefonzentrale) ist die Amtswaltereigenschaft zu

verneinen und damit eine Veröffentlichung nur mit Einwilligung der Betroffenen zulässig (25. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Nr. 8.3; Bayrischer Landesbeauftragter für den Datenschutz, zitiert in DuD 2000, S. 54; Baden-Württembergischer Datenschutzbeauftragter, zitiert in Datenschutz-Berater 1998, Heft 2, S. 9).
Diese Bewertung muss auch bei der Auslegung des § 28 BDSG bzw. des § 29 BDSG, namentlich bei der Frage, ob "schutzwürdige" Belange der Betroffenen einer Veröffentlichung entgegenstehen, berücksichtigt werden, denn andernfalls könnten die für eine Veröffentlichung durch die Kommunen geltenden Schranken ohne weiteres umgangen werden, indem irgendein Externer aus Servicegedanken (oder welchen Gründen heraus auch immer) die Veröffentlichung vornimmt.

Die Aufsichtsbehörde vertrat daher die Auffassung, dass die Veröffentlichung jedenfalls insoweit unzulässig war, als sie Bedienstete betraf, die keine nach außen wirkenden Verwaltungstätigkeiten wahrnehmen.

Dabei war es unerheblich, dass die Gemeinde das komplette Telefonverzeichnis bei einer Gewerbeschau verteilt hatte, denn die Veröffentlichung im Internet hat eine völlig neue Dimension. Sie erreicht weltweit einen ungleich größeren Personenkreis als jede lokal oder regional und auflagenbegrenzte schriftliche Veröffentlichung (vgl. Baden-Württembergischer Datenschutzbeauftragter, a.a.O.).
Grundsätzlich darf eine Veröffentlichung von Telefon- und sonstigen Verzeichnissen öffentlicher Stellen im Internet nur in Abstimmung mit der öffentlichen Stelle (und deren Datenschutzbeauftragten) erfolgen.

Aufgrund der Beanstandung durch die Aufsichtsbehörde nahm der Bürgermeisterkandidat die Daten schließlich aus dem Internet heraus, wenngleich er die Auffassung der Aufsichtsbehörde, insbesondere die Anwendbarkeit des BDSG, in Frage stellte.

9.5 Veröffentlichung von Diabetikern im Internet

Wie bei dem unter 9.4 geschilderten Fall, so steckten auch bei folgendem Fall gute Absichten hinter der Idee, personenbezogene Daten von Mitbürgern ins Internet zu stellen:
Die Mutter eines Diabetikers hatte die Erfahrung gemacht, dass es für Diabetiker oftmals schwer ist, Freunde oder Lebenspartner zu finden. In den in Apotheken kostenlos ausliegenden Zeitschriften befänden sich - so die Aussage der Mutter - häufig Kontaktanzeigen von Diabetikern.

Aus diesen und ähnlichen Quellen hatte die Frau Adressdaten und Telefonnummern von kontaktsuchenden Diabetikern gesammelt und wollte sie in das Internet stellen, um den Betroffenen zu helfen.

Sie bat jedoch zuvor die Aufsichtsbehörde um Auskunft, ob ihr Vorhaben datenschutzrechtlich zulässig sei.

Die Aufsichtsbehörde wies darauf hin, dass schutzwürdige Belange der Betroffenen einer Veröffentlichung entgegenstünden. Wie bereits unter 9.4 ausgeführt, hat eine Veröffentlichung im Internet eine ganz andere Dimension als eine auflagenbegrenzte schriftliche Veröffentlichung. Es kann keinesfalls davon ausgegangen werden, dass alle, die irgendwann einmal in der Apothekenzeitschrift oder ähnlichem eine Anzeige aufgegeben haben, damit einverstanden sind, dass ihr Kontaktgesuch einer unbegrenzten Personenzahl und auf unbegrenzte Zeit bekannt gemacht wird.

Davon abgesehen, war auch nicht ersichtlich, wie die Frau die Benachrichtigungspflicht nach § 33 BDSG erfüllen würde bzw. könnte.

Die Aufsichtsbehörde riet daher zu einer datenschutzgerechten Alternative, nämlich der Einrichtung einer "Kontaktbörse", bei der sich Interessenten auf Grund eigener freiwilliger Entscheidung eintragen lassen können.

10. Aspekte internationaler Datenverarbeitungen

10.1 Datenverarbeitung in Bermuda

Ein in Bermuda ansässiges Unternehmen bietet Datenverarbeitungsdienstleistungen im eCommerce-Bereich an und möchte hierfür Kunden im europäischen Raum und insbesondere im Rhein-Main-Gebiet gewinnen.
Es sah sich daher mit den Restriktionen der EG-Datenschutzrichtlinie konfrontiert, wonach Datenübermittlungen in Länder außerhalb des Geltungsbereiches der Richtlinie nur unter bestimmten Voraussetzungen zulässig sind.
Da es für die Erfüllung von eCommerce-Verträgen zwischen hier ansässigen Unternehmen und ihren Kunden nicht erforderlich ist, dass die Kundendaten nach Bermuda übermittelt werden und somit der Ausnahmetatbestand des Art. 26 Abs. 1 b) der EG-Richtlinie nicht vorliegt, wären Datenübermittlungen nach Bermuda nur zulässig, wenn

- nachgewiesen würde, dass in Bermuda ein angemessenes Datenschutzniveau besteht (Art. 25 der Richtlinie), oder
- etwaige Datenschutzdefizite in Bermuda durch anderweitige Garantien (insbesondere durch vertragliche Regelungen) kompensiert würden (Art. 26 Abs. 2 der Richtlinie), oder
- die Einwilligungen sämtlicher betroffener Personen eingeholt würden (Art. 26 Abs. 1 a) der Richtlinie).

In Bermuda gibt es zwar kein Datenschutzgesetz mit adäquaten Regelungen, aber den Statuten eines Unternehmens kann von den gesetzgebenden Körperschaften Gesetzeskraft verliehen werden.
Diesen Weg hatte das Unternehmen beschritten: Es erließ eine Satzung oder Ähnliches mit sehr umfangreichen Regelungen zum Datenschutz und ließ diese im Gesetzgebungsverfahren als "Privatgesetz" anerkennen bzw. verabschieden.

Die sodann von dem Unternehmen um Bewertung und Bestätigung, dass damit der Nachweis eines angemessenen Datenschutzniveaus erbracht sei, gebetene Aufsichtbehörde unterzog das Regelwerk einer intensiven Prüfung.

Diese orientierte sich an dem von der Gruppe nach Art. 29 der EG-Richtlinie herausgegebenen Arbeitspapier Nr. 12 (= "Workingpaper 12").

Die dort in Kapitel 1 enthaltenen Kriterien beziehen sich auf:

- Inhaltliche Grundsätze
  - Beschränkung der Zweckbestimmung,
  - Datenqualität und -verhältnismäßigkeit,
  - Transparenz,
  - Datensicherheit,
  - Recht auf Zugriff, Berichtigung, Widerspruch,
  - Beschränkung der Weitervermittlung in andere Drittländer;
- Spezielle Anforderungen bei
  - sensiblen Daten,
  - Direktmarketing,
  - automatisierten Einzelentscheidungen;
- Verfahrensrechtliche Mechanismen bzw. Durchsetzungsmechanismen;
- Gewährleistung einer guten Befolgungsrate;
- Unterstützung und Hilfe für einzelne Personen bei der Wahrnehmung ihrer Rechte;
- Gewährleistung angemessener Entschädigung für die geschädigte Partei.

Die Prüfung durch die Aufsichtsbehörde ergab, dass die inhaltlichen Grundsätze und die speziellen Anforderungen im Wesentlichen erfüllt waren.
Die Regelungen der EG-Datenschutzrichtlinie wurden überwiegend wörtlich wiedergegeben und zum Teil durch weitere Detailregelungen präzisiert und sogar zugunsten der Betroffenen verbessert.

Da Art. 25 der EG-Richtlinie nur fordert, dass im Daten-Empfängerland ein "angemessenes" Datenschutzniveau besteht, also bewusst auf die Forderung nach einen äquivalenten Datenschutzniveau verzichtet wurde, wurden insoweit die Anforderungen (partiell) sogar übererfüllt.
Unklarheiten bestanden jedoch bzgl. einiger Begriffsbestimmungen, sodass problematisch war, ob der Geltungsbereich des "Gesetzes" sich mit den Vorgaben der EG-Richtlinie deckt. Unklarheiten bestanden auch bezüglich Ausnahmeregelungen bzw. Bezugnahmen auf andere vorrangige Rechtsvor-

schriften, da von der Aufsichtsbehörde nicht beurteilt werden konnte, ob diese die Voraussetzungen des Art. 13 der EG-Richtlinie erfüllen oder das anspruchsvolle Datenschutzregelwerk letztlich aushöhlen.
Da das Unternehmen insoweit in der "Bringschuld" gegenüber der Aufsichtbehörde steht, wurde um entsprechende Erläuterungen gebeten.

Die entscheidenden Probleme aber sah die Aufsichtsbehörde bezüglich der verfahrensrechtlichen Mechanismen zur Durchsetzung der inhaltlichen Anforderungen.

So sehr die ausführlichen Regelungen über Aufgaben und Rechte des zu bestellenden betrieblichen Datenschutzbeauftragten zu begrüßen waren, ist durch diese vorgesehene interne Kontrolle aber noch keine gute Befolgungsrate gewährleistet.
Laut Angaben der bermudischen Anwälte solle dem Finanzministerium die Aufsicht obliegen. Eindeutig war die Aussage jedoch nicht, da es wohl keine expliziten Regelungen gibt. Vor allem aber waren die Aussagen über die Ausübung der Aufsicht, über die konkreten Befugnisse und möglichen Maßnahmen sehr vage, sodass ohne eine Stellungnahme des Finanzministeriums selbst nicht davon ausgegangen werden kann, dass dieses eine wirksame externe Kontrolle wahrnimmt.

Die bermudischen Anwälte haben außerdem dargelegt, dass bei einem Verstoß gegen das "Privatgesetz" wohl der Attorney General (eine Art Generalstaatsanwalt) eine Klage wegen unerlaubter Handlung zugunsten der Betroffenen gegen das Unternehmen erheben könnte. Da es keine Regelungen über Zuständigkeiten und Konsequenzen bei Verstößen gegen "Privatgesetze" und keine Präzedenzentscheidungen gibt, haben die Anwälte eine Analogie zu einem Fall gezogen, bei dem der Attorney General geklagt hatte, weil einer Vielzahl von Personen erheblicher (körperlicher und materieller) Schaden drohte.

Es blieb aber zweifelhaft, ob der Attorney General auch klagen würde, wenn "nur" einfache Datenschutzverstöße zulasten einzelner Betroffener begangen würden. Daher holten die bermudischen Anwälte auf entsprechenden Hinweis der Aufsichtsbehörde eine Stellungnahme des Attorney General ein. Dieser erklärte aber nur lapidar, dass er für die Durchsetzung von Verpflichtungen aus öffentlichen und "privaten" Gesetzen verantwortlich sei. Er sei gemäß der Verfassung Berater der Regierung, nicht aber jeglicher anderer Personen.

Angesichts dieser wenig erhellenden Aussage und angesichts dessen, dass auch unklar blieb, ob die Betroffenen selbst eine unmittelbare Klagemöglichkeit hätten, konnte die Aufsichtsbehörde nicht bestätigen, dass eine effektive Durchsetzung der Datenschutzbestimmungen gewährleistet sei.

Die deutschen Korrespondenzanwälte teilten die Kritikpunkte den bermudischen und britischen Anwälten des Unternehmens mit. Von dort wurde eine Überarbeitung des Regelwerkes und ergänzende Stellungnahmen angekündigt.

Bei Redaktionsschluss dieses Berichtes lagen diese Unterlagen noch nicht vor.
Die weitere Entwicklung bleibt abzuwarten.

10.2 Globales Personalinformationssystem

Im Elften Tätigkeitsbericht wurde unter Nr. 8.1 (Landtagsdrucksache 14/4159 vom 16. September 1998, S. 16 f.) das Vorhaben einer international agierenden deutschen Unternehmensgruppe aus dem Bankbereich dargestellt, ein einheitliches Personalinformationssystem einzuführen.

In einer ersten Stufe sollte das System zunächst nur der Umsetzung eines Bonussystems dienen. Hierbei sollten die Übermittlungen von personenbezogenen Mitarbeiterdaten zunächst auf Europa beschränkt bleiben. Es war jedoch bereits geplant, das Personalinformationssystem weltweit für die Verarbeitung von Mitarbeiterdaten einzusetzen, unter anderem für Übermittlungen in das nichteuropäische Ausland.
Das Vorhaben hat mittlerweile konkrete Formen angenommen.

Eine sehr detaillierte (neue) Konzernbetriebsvereinbarung löst die für die erste Stufe getroffene Vereinbarung ab. Außerdem wurde zwischen der deutschen Konzernmutter (und Konzernzentrale) und den globalen Koordinationsstellen für die Auslandsregionen eine (neue) Vereinbarung zum grenzüberschreitenden Datenschutz getroffen. Diese beide Regelwerke nehmen wechselseitig aufeinander Bezug.

Grundsätzlich werden alle Personaldaten in der zentralen globalen Datenbank bei der Konzernmutter in Deutschland gespeichert.
Dieses zentrale Rechenzentrum hat auch bereits bisher Datenverarbeitungsdienstleistungen i.S.d. § 11 BDSG für rechtlich selbstständige Unternehmen innerhalb des Konzerns erbracht und ist nach § 32 BDSG bei der Aufsichtsbehörde gemeldet.

Von dieser Datenbank können Daten weltweit abgerufen werden.
Der Abruf erfolgt zum einen von den Unternehmen, bei denen der Mitarbeiter beschäftigt ist, also von seinem Arbeitgeber. Der Abruf kann dabei unter Umständen auch von einer unselbstständigen ausländischen (und außereuropäischen) Filiale der deutschen Konzernmutter oder der deutschen Konzerntöchter erfolgen, soweit dieser Filiale besondere Aufgaben zugewiesen sind.

Darüber hinaus können personenbezogene Daten von in Deutschland beschäftigten Mitarbeitern unter Umständen auch von rechtlich selbstständigen ausländischen Tochter-Unternehmen angerufen werden.
Dies ist vor dem Hintergrund der globalen und unternehmensbereichsbezogenen Ausrichtung des Konzerns zu sehen: Aus wirtschaftlichen Erwägungen werden Sparten gebildet, die insgesamt oder teilweise aus eigenständigen juristischen Personen bestehen und unter einer holdingähnlichen Leitung stehen ("Matrixstrukturen").
Dies bringt es mit sich, dass Planungs- und Entscheidungsbefugnisse in personellen Angelegenheiten in gewissem Umfang länder- und unternehmensübergreifend angelegt sind.

Die Konzernbetriebsvereinbarung enthält im Wesentlichen folgende Regelungen:

- Sehr konkrete und abschließende Festlegung der Datengruppen.
  Ein Katalog der Datenfelder wird beim Konzernbetriebsrat hinterlegt. Über Änderungen wird er informiert.

- Abschließende Regelung der Zugriffsberechtigten, des Zugriffsumfangs sowie der Vergabe der Zugriffsberechtigung.
  Der Zugriffsumfang richtet sich nach der sachlichen, räumlichen und funktionalen Zuständigkeit. Hierbei wird zwischen lesend, schreibend, ändernd und löschend unterschieden.

- Regelungen über die Datenerhebung und Datenverarbeitung, insbesondere über Datenauswertungen.
  In einer Anlage sind die vorgesehenen Standardauswertungen festgehalten. Eine Erweiterung des Kataloges der Standardauswertungen bedarf der Zustimmung des Konzernbetriebsrates.
  Für Auswertungen, die über die Standardauswertungen hinausgehen (so genannte variable Verknüpfungen) ist in einer weiteren Anlage ein Katalog von Datenfeldern enthalten, mit denen keine Verknüpfungen vorgenommen werden dürfen (so genannter Negativkatalog). Dies wird auch systemtechnisch sichergestellt.
  In der Zugriffsregelung (siehe oben) ist festgelegt, wer variable Verknüpfungen vornehmen darf.
  Die variablen Verknüpfungen werden (elektronisch) dokumentiert.

- Für die Datenübermittlung in das Ausland ist zusätzlich festgelegt, dass beim Personalbereich eine Liste hierüber geführt wird (dies gilt auch für Übermittlungen an andere Unternehmen innerhalb des Konzerns in Deutschland). Ausnahmen bestehen nur für das interne Mitarbeiter- bzw. Telefonverzeichnis und bestimmte Übermittlungen zur Kontrolle von Insidergeschäften.

  Außerdem verpflichtet sich die Konzernmutter, mit den globalen Koordinationsstellen für die Auslandsregionen eine Vereinbarung zum grenzüberschreitenden Datenschutz zu treffen.

- Die Mitarbeiter werden einmal im Jahr unaufgefordert über ihre gespeicherten Daten informiert.
  Künftig sollen sie ihre Daten im Rahmen eines Stammdatenreports über eine Web-Applikation lesen können. Sie werden außerdem über etwaige Datenübermittlungen ins Ausland informiert. Ferner wurde die Geltung der Rechte des Bundesdatenschutzgesetzes vereinbart.

- Die Durchführung der Vereinbarung wird durch den Konzernbetriebsrat, die Revision und den Datenschutzbeauftragten überwacht.

- Bei Datenverarbeitungen außerhalb des Konzerns muss die Einhaltung der Konzernbetriebsvereinbarung sichergestellt werden.

Da die Konzernbetriebsvereinbarung für leitende Angestellte nicht gilt (§ 5 Abs. 3 Betriebsverfassungsgesetz), soll mit Vertretern dieser Personengruppe eine gleich lautende Vereinbarung geschlossen werden.

Der Entwurf für eine Vereinbarung zwischen der Konzernmutter und den Koordinationsstellen für die Auslandsregionen beinhaltet im Wesentlichen folgende Regelungen:

- Beschreibung der Zweckbestimmung der Datenverarbeitung,
- Konzernweite Geltung der Regelungen des Bundesdatenschutzgesetzes,
- Konzernweite Beachtung der Konzernbetriebsvereinbarung,
- Auskunftsanspruch und umfassende Kontrollbefugnisse der Konzernmutter bzgl. der Einhaltung der datenschutzrechtlichen Vorgaben,
- Einsatz von Subunternehmern nur mit ausdrücklicher schriftlicher Zustimmung der Konzernmutter und bei schriftlicher Verpflichtung auf die Einhaltung der Regelungen dieses Vertrages,
- Datensicherheitsmaßnahmen,
- Bestellung von Datenschutz-Ansprechpartnern bei den ausländischen Koordinationsstellen.
- Die Konzernmutter hat das Recht, bei Bedarf Anweisungen über das Verfahren und die Maßnahmen, die zur Beantwortung von Anfragen und zur Wahrung der Rechte der Betroffenen auf Auskunft, Berichtigung, Löschung, Sperrung und Widerspruch erforderlich sind, zu erteilen.
  Regresspflicht der Auslandsstellen gegenüber der Konzernmutter, wenn Rechte von Mitarbeitern durch Vertragsverstöße verletzt werden.
- Die Auslandsstellen sind gegenüber der deutschen Aufsichtsbehörde unmittelbar zur Auskunft verpflichtet und haben ihr oder von ihr beauftragten Personen die Überprüfung vor Ort zu ermöglichen.

Die von der Konzernmutter um Stellungnahme gebetene Aufsichtsbehörde hielt die Erstellung der beiden aufeinander abgestimmten Regelwerke für sehr sinnvoll.

Zwar wäre es eventuell möglich, dass eine Betriebsvereinbarung, die um weitere Regelungen zur Auslandsdatenverarbeitung - wie in der separaten Vereinbarung - ergänzt würde, eventuell auch im Hinblick auf die EG-Richtlinie als Rechtsgrundlage für eine Datenübermittlung in Länder ohne angemessenes Datenschutzniveau anerkannt werden könnte (vgl. Eul/Godefroid, RDV 1998, S. 185 ff., Nr. 5.1 unter Hinweis auf Erwägungsgrund 8 der EG-Richtlinie).
Soweit die ausländischen Stellen unselbstständige Filialen sind, wären sie an die Konzernbetriebsvereinbarung gebunden. Aber auch rechtlich selbstständige ausländische Unternehmen könnten wohl - ebenso wie die deutschen Tochterunternehmen - allein aufgrund der Beherrschungsverträge an die von der deutschen Konzernmutter abgeschlossene Konzernbetriebsvereinbarung gebunden werden.
Gleichwohl ist der Abschluss einer speziellen Vereinbarung zur Auslandsdatenvereinbarung sinnvoll. Er verdeutlicht und konkretisiert die Verpflichtungen der ausländischen Konzernstellen.

Der Abschluss zweier Regelwerke illustriert auch, dass es um zwei sich teilweise überlagernde Problembereiche geht:

Zum einen geht es um die Frage, ob die Übermittlung von Mitarbeiterdaten an andere - rechtlich selbstständige - Unternehmen zulässig ist.
Dies ist auch für Übermittlungen innerhalb Deutschlands relevant.

Zum anderen geht es um die Frage der Auslandsdatenverarbeitung, wobei insoweit unerheblich ist, ob die ausländische Stelle rechtlich selbstständig oder unselbstständig ist.

Soweit es sich nicht um konzerndimensionale Arbeitsverhältnisse handelt - die im konkreten Fall überwiegend nicht vorliegen -, kommt nur § 28 Abs. 1 Nr. 2 BDSG (bzw. § 28 Abs. 2 Nr. 1 a BDSG) als gesetzlicher Erlaubnistatbestand des BDSG für Übermittlungen an andere Unternehmen in Betracht.

Da es keine Konzernklausel gibt, reicht das allgemeine Konzerninteresse an sich nicht aus zur Begründung des "berechtigten Interesses".
Vielmehr muss für das übermittelnde bzw. das empfangende Unternehmen konkret ein berechtigtes Interesse vorliegen. Soweit also jedes beteiligte Unternehmen einen (individuellen) Vorteil aus der Spartenstruktur hat, wäre ein berechtigtes Interesse gegeben. Dies ist freilich nicht ohne weiteres zu begründen, ohne doch auf das allgemeine Konzerninteresse zurückgreifen zu müssen.

Schwieriger noch ist die Bewertung, ob schutzwürdige Belange der betroffenen Mitarbeiter entgegenstehen.
Soweit Personaldaten an beherrschende Unternehmen übermittelt werden, ist dies grundsätzlich problematisch. Konkret war dies zwar weniger relevant, da die Mitarbeiter in Deutschland überwiegend beim beherrschenden Unternehmen beschäftigt sind.
Gleichwohl gibt es auch in Deutschland Tochtergesellschaften, von denen Mitarbeiterdaten zum Teil an das beherrschende Unternehmen übermittelt werden.

Damit bei allen diesen Übermittlungen die Belange der Mitarbeiter gewahrt werden, wurde die Konzernbetriebsvereinbarung geschlossen. Diese stellt eine "andere Rechtsvorschrift" i.S.d. § 4 Abs. 1 BDSG dar.

Betriebsvereinbarungen können vom BDSG solange abweichen, wie sie die dort getroffenen Regelungen durch Schutzvorkehrungen ersetzen, die den je spezifischen Beschäftigungsbedingungen besser angepasst, allerdings mindestens ebenso weit reichend sind (Simitis in Simitis/Dammann/Geiger/Mallmann/Walz, BDSG-Kommentar, § 28, Rdnr. 47).

Hinsichtlich des in der ersten Stufe implementierten unternehmensübergreifenden Bonussystems für eine besonders wichtige Konzernsparte wurde von der Aufsichtsbehörde insoweit kein Problem gesehen, da das System insgesamt zu einer deutlich überdurchschnittlichen Vergütung der betroffenen Spartenmitarbeiter führte. Die entsprechenden Regelungen in der Betriebsvereinbarung (bzw. der vorläufigen Regelabsprache) konnten nicht als Mittel zum Unterlaufen des BDSG bewertet werden.

Die Erweiterungen des Spartensystems waren schwieriger zu beurteilen und wurden intensiv diskutiert.
Aber angesichts der sehr dezidierten Regelungen in der Konzernbetriebsvereinbarung sah die Aufsichtsbehörde im Ergebnis keine Veranlassung, diese als datenschutzrechtlich unzureichend zu bewerten.

Hinsichtlich der Auslandsdatenverarbeitung war die Aufsichtsbehörde der Auffassung, dass die Vereinbarung mit den Koordinationsstellen für die Auslandsregionen den Anforderungen des WP 12 (siehe oben 10.1) entspricht und dadurch die schutzwürdigen Belange der Mitarbeiter gewahrt werden.

Da das beherrschende Unternehmen ein deutsches Unternehmen ist, ist von einer wirkungsvollen Umsetzung der Regelungen auszugehen. Auf eine Vertragsstrafen-Regelung zugunsten der Konzernmutter konnte daher angesichts der sonstigen Durchsetzungsmechanismen verzichtet werden.

Auf Anregung der Aufsichtsbehörde wurde jedoch noch die Regelung aufgenommen, dass Betroffene bei einem Datenschutzverstoß durch ausländische

Stellen einen Schadensersatzanspruch gegen ihren Arbeitgeber geltend machen können, der für die Auslandsdatenverarbeitung verantwortlich bleibt.
Soweit die ausländische Stelle keine unselbstständige Filiale des deutschen Arbeitgebers ist, ist dies nicht selbstverständlich, zumal auch nicht von einer Auftragsdatenverarbeitung ausgegangen werden kann. Die Regelung ist sachgerechter, als den Betroffenen einen Schadensersatzanspruch gegen die ausländischen Daten verarbeitenden Stellen einzuräumen.

Da vertragliche Regelungen etwaige Zugriffe ausländischer Behörden nicht verhindern können, wäre es nicht akzeptabel, wenn die Matrixstrukturen so gestaltet wären, dass Personaldaten zu "Vorgesetzten" in totalitären Staaten übermittelt würden. Dies ist jedoch nicht der Fall.

11. Arbeitnehmerdatenschutz

11.1 Zugriffe des Arbeitgebers auf Mitarbeiter-E-Mails

Ein Mitarbeiter, der als Administrator des unternehmensweiten E-Mail-Systems beschäftigt ist, erhielt von seinem Arbeitgeber den Auftrag, eine Rücksicherung von bestimmten E-Mails aus den Monatssicherungen vergangener Jahre durchzuführen. Bisher hatte dieser Mitarbeiter diese Rücksicherungen nur dann durchgeführt, wenn der Besitzer einer E-Mail-Adresse ihm persönlich den Auftrag erteilt hatte, weil er z.B. eine bestimmte E-Mail frühzeitig gelöscht hatte und doch noch einmal auf diese zugreifen musste.

Da der Administrator datenschutzrechtliche Bedenken hinsichtlich des verlangten Zugriffs hatte, bat er die Aufsichtsbehörde um Auskunft, inwieweit er dem Ansinnen seiner Vorgesetzten nachkommen müsse oder damit gegen bestehende Rechtsnormen verstoße.

Bedauerlich war bei diesem Vorfall, dass der Mitarbeiter zum betrieblichen Datenschutzbeauftragten nicht das vollständige Vertrauen aufbringen konnte, um diese Angelegenheit mit ihm zu klären. Bei einer ordnungsgemäßen Tätigkeit eines betrieblichen Beauftragten für den Datenschutz muss zunächst dieser versuchen, eine Klärung im eigenen Unternehmen herbeizuführen und erst dann, wenn er sich außerstande sieht, eine endgültige Aussage zu treffen, sollte auf die Aufsichtsbehörde zurückgegriffen werden.

Im Unternehmen bestand die eindeutige Weisung, dass das Mail-System ausschließlich betrieblichen Zwecken zu dienen hat. Eine private Nutzung war somit ausgeschlossen. Der Arbeitgeber war daher weder Anbieter von Telekommunikationsdiensten i.S.d. Telekommunikationsgesetzes noch von Telediensten i.S.d. TDDSG.

Dies bedeutet jedoch nicht, dass die Protokollierung und Auswertung der E-Mail-Nutzung unbegrenzt zulässig wäre.

Vielmehr ist zunächst § 31 BDSG zu berücksichtigen.
Soweit die Daten für Zwecke der Datensicherung gespeichert wurden, ist die enge Zweckbindung des § 31 BDSG zu beachten, d.h. eine spätere Nutzung für andere Zwecke ist ausgeschlossen.

Wenn Daten nicht nur für Zwecke der Datensicherung, sondern auch für andere Zwecke, insbesondere für eine Verhaltens- und Leistungskontrolle der Mitarbeiter genutzt werden sollen, muss von vornherein eine entsprechend erweiterte Zweckbindung festgelegt werden.

Dabei muss die Mitbestimmungspflicht des Betriebsrates gemäß Betriebsverfassungsgesetz beachtet werden.

Grundsätzlich sind Kontrollen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes zulässig. Demzufolge muss der Arbeitnehmer eine Kontrolle nur dann hinnehmen, wenn die diesbezüglichen Maßnahmen des Arbeitgebers erforderlich und geeignet sind, um den Zweck des Arbeitsverhältnisses zu erreichen.

Als legitimes Interesse des Arbeitgebers kommt der Schutz der firmeneigenen Dateien vor elektronischen Viren und der Schutz der Betriebssysteme vor Überlastung in Betracht. (Diese Zwecke lassen sich auch unter § 31

BDSG subsumieren, sodass insoweit kein Problem der unzulässigen Zweckänderung besteht.)

Bezüglich der Inhaltskontrolle ist danach zu differenzieren, ob die E-Mails den Schriftverkehr ersetzen oder von der Nutzung her eher mit Telefonverkehr vergleichbar sind.

Wenn der Mitarbeiter beispielsweise mittels E-Mail Verträge über Warenlieferungen oder Ähnliches für das Unternehmen abschließt, kann der Vorgesetzte - wie bei Schriftstücken auch - verlangen, dass der Mitarbeiter ihm den Inhalt der entsprechenden E-Mails zugänglich macht. Im Übrigen darf eine Inhaltskontrolle erfolgen, wenn ein begründeter Verdacht bezüglich des Verrats von Geschäftsgeheimnissen, Mobbing oder einer Straftat besteht (Post-Ortmann, RDV 1999, 102).

Mangels genauerer Angaben durch den Administrator konnte die Aufsichtsbehörde keine konkrete Bewertung des Falles vornehmen. Es bleibt zu hoffen, dass die Angelegenheit letztlich datenschutzgerecht geregelt werden konnte.

11.2 Abhören und Aufzeichnen von Telefonaten

Eine Funk-Taxi-Genossenschaft hatte die Telefongespräche ihrer Mitarbeiter ohne deren Wissen abgehört und kündigte an, die Gespräche künftig vollständig aufzuzeichnen. Eine Betroffene wandte sich an die Aufsichtsbehörde.

Die Genossenschaft verwies darauf, dass das Führen privater Telefongespräche untersagt sei und rechtfertigte die Maßnahmen damit, dass die erforderlichen Arbeits- und Leistungskontrollen nur durch die Aufzeichnung der Gespräche erfolgen könne. Andernfalls sei die Arbeitsleistung der Mitarbeiter in der Taxizentrale überhaupt nicht kontrollierbar.

Wenngleich bei Telefonaufzeichnungen der Dateibegriff und damit die Anwendbarkeit des BDSG zweifelhaft ist, so ist doch zu beachten, dass auch dienstliche Telefongespräche dem verfassungsrechtlichen Schutz des allgemeinen Persönlichkeitsrechtes unterliegen. Der Schutz des Rechtes am eigenen Wort als Ausprägung des allgemeinen Persönlichkeitsrechtes wird durch die Kenntnis der Betroffenen von einer Abhörmöglichkeit nicht beseitigt (Linnenkohl RDV 1992, 205 f., BverfGE 34, S. 238 f. [245], 45, S. 148 f. [154]).

Obwohl bei reinen telefonischen Bestellvorgängen (wie hier die Entgegennahme von Taxibestellungen) der objektive Gehalt des Gesagten so sehr im Vordergrund stehen kann, dass die Persönlichkeit des Sprechenden nahezu völlig dahinter zurücktritt, muss gleichwohl die Verfügungsbefugnis des Einzelnen anerkannt werden, soweit es um Leistungs- und Verhaltenskontrollen geht (Linnenkohl a.a.O.).

Darüber hinaus ist der Schutzbereich des § 201 StGB betroffen, jedenfalls wenn Gespräche mittels "Abhöreinrichtungen" i.S.d. § 201 StGB unbefugt mitgehört werden. Das unbefugte Aufzeichnen ist ebenfalls strafbar.

Als Rechtfertigungsgrund kommt grundsätzlich nur eine Einwilligung des Betroffenen in Betracht, wobei in strafrechtlicher Hinsicht unter Umständen auch eine mutmaßliche oder konkludente Einwilligung genügt.

Angesichts der arbeitnehmertypischen Abhängigkeit ist jedoch kritisch zu hinterfragen, ob eine vom Arbeitgeber eingeholte Einwilligung tatsächlich als wirksam anerkannt werden kann. Insoweit ist maßgeblich, ob es unter Berücksichtigung der Interessen beider Parteien als angemessen erscheint, dass die Übertragung der Telefontätigkeit von der Einwilligung in Abhör- und Aufzeichnungsmaßnahmen abhängig gemacht wird.

Im konkreten Fall hielt die Aufsichtsbehörde es für unangemessen, wenn der Vorstand einer Taxi-Genossenschaft die unbeschränkte Möglichkeit hat, sämtliche Gespräche jederzeit mitzuhören. Selbst wenn hierfür Einwilligungen eingeholt würden bzw. wenn man Qualitätsverpflichtungen etc. im Arbeitsvertrag als Einwilligung im weitesten Sinne bewerten könnte, wären diese wohl unwirksam. Gleiches gilt für die unbeschränkte Aufzeichnung der Telefongespräche.

Eine Qualitätskontrolle durch den Arbeitgeber ist gleichwohl nicht ausgeschlossen.
Selbstverständlich ist hierbei zunächst das Mitbestimmungsrecht des Betriebsrates zu berücksichtigen. Im konkreten Fall war jedoch kein Betriebsrat vorhanden.

Ebenso wie für Schulungen ist für eine spätere Qualitätssicherung und -kontrolle ein Mithören zulässig bzw. eine diesbezüglich eingeholte Einwilligung wirksam, wenn das Mithören offen erfolgt, d.h. indem der Mithörende neben dem Arbeitnehmer sitzt oder die so genannte Anklopf-Funktion aktiviert hat.

Auch ohne Aktivierung der Anklopf-Funktion kann ein Mithören zur Qualitätskontrolle gerechtfertigt sein, wenn es auf einen verhältnismäßig kurzen Zeitraum (etwa eine Woche) begrenzt ist und dem Arbeitnehmer dieser Zeitraum unmissverständlich mitgeteilt wird (möglichst schriftlich und gegebenenfalls durch zusätzliche Einblendung am Bildschirm).
Voraussetzung ist, dass sämtliche Modalitäten klar und unter Berücksichtigung der Arbeitnehmerinteressen geregelt werden (z.B. Besprechung und gemeinsame Bewertung mit dem Arbeitnehmer, auf Wunsch unter Hinzuziehung einer Vertrauensperson).

Die Taxi-Genossenschaft hielt entgegen, dass derartige Maßnahmen unzureichend seien, um Privatgespräche zu verhindern.

Auch im Hinblick auf das Interesse an der Vermeidung von solchen Missbräuchen ist eine unbegrenzte Abhörmöglichkeit jedoch unverhältnismäßig und unzulässig.

Zuletzt trug die Taxi-Genossenschaft vor, dass speziell die Aufzeichnung der Gespräche auch zu Beweiszwecken erforderlich sei, beispielsweise für den Fall, dass ein Kunde behauptet, er habe sein Flugzeug verpasst, weil das Taxi nicht zur vereinbarten Zeit gekommen sei.

Ein legitimes beiderseitiges Beweisinteresse wie beim Telefonbanking kann die Aufzeichnung von Gesprächen durchaus rechtfertigen, sofern entsprechende Einwilligungen vorliegen und die Aufzeichnungen nur bei Beweisnot abgehört werden. Inwieweit bei Taxizentralen ein vergleichbares Beweisinteresse besteht, ist zweifelhaft und wird noch weiter zu diskutieren sein.

Bei alledem geht es nicht nur um die Arbeitnehmerbelange, sondern auch um die Belange der Kunden.
Während bei Telefonbanking-Verträgen die schriftliche Kunden-Einwilligung im Vertrag eingeholt wird, erfolgt im Fall der Taxi-Genossenschaft noch nicht einmal eine telefonische Information.

Da es sich wohl um ein bundesweites Problem handelt und bei Redaktionsschluss dieses Berichtes noch keine Einigung erzielt werden konnte, wird die Aufsichtsbehörde auf Anregung der Taxi-Genossenschaft ein Gespräch mit dem in Frankfurt ansässigen Bundesverband der Taxiunternehmen führen.

11.3 Nutzung von Daten einer Arbeitnehmerin für Werbezwecke

Eine Arbeitnehmerin wurde davon überrascht, dass sie ihre persönlichen Daten und ihr Foto auf einer Chipkarte wiederfand, die von Ihrem Arbeitgeber zu Demonstrations- und Werbezwecken genutzt wurde. Sie war vorher nicht um ihr Einverständnis gebeten worden; sie arbeitete auch nicht in der Werbeabteilung des Unternehmens und hatte keine Repräsentationsaufgaben im Unternehmen.

Eine derartige Vorgehensweise ist nicht von einem normalen Arbeitsvertrag gedeckt; § 28 BDSG enthält auch keine entsprechenden Erlaubnistatbestände. Es wurden eindeutig die schutzwürdigen Belange der Arbeitnehmerin beeinträchtigt. Hinzu kommt, dass die Arbeitnehmerin ein Urheberrecht an der Veröffentlichung ihres eigenen Bildes hat.
Die Aufsichtsbehörde konnte keinen Kontakt zu dem betroffenen Arbeitgeber aufnehmen, da die Arbeitnehmerin ihn nicht nannte.

Entsprechend den Empfehlungen der Aufsichtsbehörde wird die Arbeitnehmerin voraussichtlich versuchen, über den betrieblichen Datenschutzbeauftragten die Situation in ihrem Sinne zu beeinflussen.

Es sollte die allgemein übliche Bezeichnung "Musterfrau" (oder Mustermann) mit fiktiven Daten auf der Demonstrations-Chipkarte verwendet werden. Auch ein Bild kann nur mit dem Einverständnis der persönlich Betroffenen genutzt werden.

12. Medizinischer Bereich

12.1 Umgang mit Patientendaten nach dem Tod eines Arztes

Gravierende Missstände bezüglich der Aufbewahrung von Patientenunterlagen offenbarte folgender Fall:

Ein Arzt war verstorben, und seine Frau und Kinder hatten die Erbschaft ausgeschlagen. Ein Praxisnachfolger war (zunächst) nicht vorhanden. Die Ermittlung weiterer Erben durch das Amtsgericht nahm mehrere Monate in Anspruch, bis das Amtsgericht die Erbenermittlung schließlich beendete, da sämtliche Angehörige die Erbschaft ausgeschlagen hatten. Die Bestellung eines Nachlasspflegers lehnte das Amtsgericht ab, da der Nachlass hoch verschuldet war und es nicht Aufgabe eine Nachlasspflegers sei, für die Verwahrung von Patientenunterlagen zu sorgen.

Der Vermieter der Praxisräume machte sein Vermieterpfandrecht geltend und verschloss daher die Räume nach dem Tod des Arztes. Er verwies darauf, dass die Patientenunterlagen für ihn keinerlei materiellen Wert hätten und die Landesärztekammer oder sonstige Stellen sie abholen mögen. Gleichwohl war er bereit, die Unterlagen zunächst zu verwahren und ehemaligen Patienten ihre Unterlagen auszuhändigen, sofern sie sich zuvor auswiesen und anschließend die Übergabe quittierten.

Nach einem halben Jahr fand der Vermieter schließlich einen Praxisnachfolger, der auch die kassenärztliche Zulassung erhielt.
Im Hinblick auf diese Nachfolge ließ der Vermieter umfangreiche Renovierungsarbeiten durchführen, an denen sich der Praxisnachfolger aktiv beteiligte. Der Mietvertrag mit dem Praxisnachfolger sollte aber erst mit Abschluss der Renovierungsarbeiten wirksam werden.

Bei einer Überprüfung musste die Aufsichtsbehörde feststellen, dass mehrere tausend Patientenkarteikarten völlig ungesichert in den Schränken lagerten. Eine Vielzahl von Handwerkern konnte ungehindert Zugriff nehmen, ebenso hätten wohl sonstige Besucher oder Bewohner des Mehrfamilienhauses Zugang gehabt, da die Räumlichkeiten während der Bauphase nicht abgeschlossen waren.
Vermieter und Praxisnachfolger betonten nachdrücklich, dass sie keinerlei rechtliche Verpflichtung ihrerseits sähen, für eine Datensicherung zu sorgen.
Die Aufsichtsbehörde konnte in dieser Situation keine Anordnung treffen.
Nach dem Bundesdatenschutzgesetz kann sie nur gegenüber "speichernden Stellen" Maßnahme zum technisch-organisatorischen Datenschutzanordnen.
Das Problem war, dass sich weder der Vermieter noch der Nachfolger als "speichernde Stelle" sahen und drohten, die Unterlagen gegebenenfalls auf die Straße zu stellen, wenn man mit Anordnungen gegen sie vorgehe.
Die Unterlagen waren somit mehr oder weniger herrenlos.
In einem gleich gelagerten Fall wurden in Nordrhein-Westfalen Sicherungsmaßnahmen nach Polizei- und Ordnungsrecht getroffen. Trotz eindringlicher Hinweise des Regierungspräsidiums Darmstadt als obere Aufsichtsbehörde nach dem Hessischen Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) hat der zuständige Magistrat der Stadt jedoch keine Veranlassung gesehen, Maßnahmen nach HSOG zu treffen.

Letztlich hat der Vermieter doch noch vorläufige Sicherungsmaßnahmen getroffen. Nach Praxisübernahme hat der Nachfolger schließlich für die Sicherung gesorgt.

Der Fall hat offensichtlich werden lassen, dass grundsätzliche Probleme bestehen:

Wenn Erben vorhanden sind, geht die Schweigepflicht nach § 203 Strafgesetzbuch (StGB) auf diese über. Als Gesamtrechtsnachfolger des Verstorbenen (§ 1922 Bürgerliches Gesetzbuch [BGB]) haben sie die Aufbewahrung ärztlicher Aufzeichnungen entsprechend der ärztlichen Berufsordnung sicherzustellen.
Hier stellt sich dann "nur" die Frage, ob die Erben sich ihrer Pflichten bewusst sind und diese ordnungsgemäß wahrnehmen. Die Landesärztekammer hat hierzu mitgeteilt, dass sie die Erben entsprechend informieren würde.

Wenn alle Erben die Erbschaft ausschlagen, käme der Fiskus als Erbe in Betracht (§§ 1936, 1964, 1942 Abs. 2, 2011 BGB), repräsentiert durch das Regierungspräsidium.
Im konkreten Fall hat das Amtsgericht, trotz ausdrücklichen Hinweises hierauf, aber davon abgesehen, die - konstitutive - Erbenfeststellung des Fiskus vorzunehmen (weil der Nachlass überschuldet war). In der Tat bestehen große Zweifel, ob es sachgerecht wäre, den Fiskus in die Pflicht zu nehmen. Es erscheint interessengerechter, wenn die Kassenärztliche Vereinigung und die Landesärztekammer in die Pflicht genommen würden.

Die Kassenärztliche Vereinigung hat nach § 75 Sozialgesetzbuch V die vertragsärztliche Versorgung sicherzustellen. Dies dürfte beinhalten, dass Maßnahmen oder Regelungen getroffen werden, damit die Kassenpatienten-Unterlagen verstorbener Ärzte ordnungsgemäß aufbewahrt und im Bedarfsfall an betroffene Patienten oder - mit deren Einwilligung - an weiterbehandelnde Ärzte herausgegeben werden bzw. eine Beauskunftung erfolgt. Mit dem Sicherstellungsauftrag wäre es unvereinbar, wenn die Behandlungsdokumentationen in Notfallsituationen nicht verfügbar wären oder allgemein, wenn Untersuchungen doppelt gemacht werden müssten, weil die Unterlagen nicht ordnungsgemäß verwahrt werden.
Explizit geregelt ist dies freilich nicht.
Bezüglich der Verantwortung der Ärztekammer besagt die arztrechtliche Literatur (Narr, Ärztliches Berufsrecht, S. 585), dass eine Aufbewahrung der Arztunterlagen durch diese dann in Erwägung zu ziehen ist, wenn alle dem Arzt oder den Angehörigen zumutbaren Maßnahmen zur ordnungsgemäßen Aufbewahrung gescheitert sind.
Dies müsste erst recht dann gelten, wenn keine Erben vorhanden sind.
Rechtlich eindeutig ist die Verantwortung der Landesärztekammer aber leider nicht geregelt. Nach § 5 Abs. 1 Hessisches Heilberufegesetz hat die Kammer zwar die Berufspflichten der Kammerangehörigen zu überwachen, völlig zweifelsfrei ergibt sich daraus aber nicht, dass die Kammer nach dem Tode eines Arztes für die ordnungsgemäße Aufbewahrung zu sorgen hat. Daher hat die Landesärztekammer darauf hingewiesen, dass sie zwar eine moralische Verantwortung sehe und deshalb für künftige Fälle eine grundsätzliche Lösung zusammen mit der Kassenärztlichen Vereinigung anstrebe, dass aber keine rechtliche Verpflichtung bestünde. Die Aufsichtsbehörde hat deshalb dem Hessischen Sozialministerium über die grundsätzliche Problematik berichtet, welches nun eine Änderung des Heilberufegesetzes oder sonstiger Vorschriften prüft.

12.2 Aids-Hilfe Verein

Ein Aids-Hilfe Verein bat die Aufsichtsbehörde um Auskunft, welche datenschutzrechtlichen Anforderungen er zu beachten habe und inwieweit sich Schweigeverpflichtungen aus dem Strafgesetzbuch (StGB) ergäben.

Zunächst konnte positiv festgestellt werden, dass der Verein seine Klienten grundsätzlich anonym berät. Name und Anschrift werden nur erfragt, wenn der Klient weiterhin Kontakt wünscht, Akten werden nur in Kenntnis des Klienten angelegt und grundsätzlich nur dann, wenn er Hilfestellung bei der Beantragung öffentlicher oder privater Leistungen erbittet.

Das BDSG ist daher zurzeit mangels dateimäßiger Datenverarbeitung nicht anwendbar. Im Hinblick auf einen etwaigen späteren Einsatz der elektronischen Datenverarbeitung gab die Aufsichtsbehörde aber entsprechende Hinweise.

Hinsichtlich der Frage nach Schweigepflichten gemäß StGB war wie folgt zu differenzieren:

- Als hauptamtlicher Mitarbeiter war ein staatlich anerkannter Diplom-Sozialarbeiter eingestellt. Dieser unterfällt der Schweigepflicht nach § 203 Abs. 1 Nr. 5 StGB.
  Unter den besonderen Schutz des § 203 StGB fallen danach solche Geheimnisse, die den Personen dieser Berufsgruppe "als" Sozialarbeiter anvertraut werden.
  Da von den Angehörigen dieser Berufsgruppe ganz unterschiedliche Aufgaben wahrgenommen werden können, die nur zum Teil vertrauensgebunden sind, ist § 203 Abs. 1 Nr. 5 StGB so auszulegen, dass eine Tätigkeit "als" Sozialarbeiter i.S.d. § 203 StGB nur vorliegt, wenn solche Aufgaben wahrgenommen werden, die dessen spezifische Ausbildung erkennen lassen und deren Erfüllung ein besonderes Vertrauen in die Verschwiegenheit des Betreffenden voraussetzt (Schönke/Schröder, Kommentar zum StGB, 25. Aufl., § 203, Rdnr. 13).

  Diese Voraussetzungen waren hier erfüllt:
  Die Tätigkeit in einer privaten Aids-Hilfe Beratungsstelle gehört zu den typischen Betätigungsgebieten eines Sozialarbeiters und erfordert entsprechende ausbildungsspezifische Kenntnisse. Die Erfüllung der Aufgabe setzt auch ein besonderes Vertrauen in die Verschwiegenheit voraus.

- Die bei dem Aids-Hilfe Verein tätigen ehrenamtlichen Berater waren selbst keine staatlich anerkannten Sozialarbeiter (und auch keine Sozialpädagogen), sodass § 203 Abs. 1 Nr. 5 StGB nicht (unmittelbar) galt.
  Auch eine Schweigepflicht nach § 203 Abs. 1 Nr. 4 StGB schied aus.
  Nach § 203 Abs. 1 Nr. 4 StGB unterfallen "Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung öffentlichen Rechts anerkannt ist", der Schweigepflicht.
  Die Tätigkeit bei dem Aids-Hilfe Verein umfasst zwar in gewissem Umfang Beratung in Drogenfragen, da der Verein jedoch keine von öffentlicher Stelle anerkannte Sucht-(Drogen-)Beratungsstelle ist, kann sich auch keine Schweigepflicht aus § 203 Abs. 1 Nr. 4 StGB ergeben.

  Eine Schweigepflicht der ehrenamtlichen Berater kann sich jedoch aus § 203 Abs. 3 StGB ergeben, wonach den in § 203 Abs. 1 StGB Genannten ihre berufsmäßig tätigen Gehilfen gleichstehen.
  Wenn also die ehrenamtlichen Berater dem Sozialarbeiter zur beruflichen Unterstützung zugeordnet sind, erstreckt sich seine Schweigepflicht (nach § 203 Abs. 1 Nr. 5 StGB) somit (nach § 203 Abs. 3 StGB) auf die ehrenamtlichen Berater. Hiervon war im konkreten Fall auszugehen. (Ansonsten würden die ehrenamtlichen Berater allenfalls unter die Bestimmungen des Bundesdatenschutzgesetzes fallen.)

  Gleiches gilt für die Bürokraft, auch diese ist "Gehilfin".

  Da in erster Linie der Sozialarbeiter unter die Schweigepflicht fällt, muss er seine Gehilfen über die Schweigepflicht belehren und dies schriftlich festhalten.

Ein Verstoß gegen die Schweigepflicht liegt vor, wenn die der Schweigepflicht unterfallenden Informationen unbefugt offenbart werden.

Als Rechtfertigungsgrund kommt grundsätzlich nur die Einwilligung (bzw. Schweigepflichtentbindungserklärung) des Betroffenen in Betracht.
Auch der Informationsaustausch mit anderen Trägern der Aids-Hilfe ist daher grundsätzlich nur mit der Einwilligung des Betroffenen zulässig.
Im konkreten Fall legte der Verein dar, dass ein solcher Informationsaustausch in aller Regel nur im Zusammenhang mit der Beantragung von Hilfen für den Klienten erfolge. Da dies nur geschehe, wenn der Klient ausdrücklich um entsprechenden Beistand bei der Beantragung anderer Hilfen bittet, wird in der Regel eine zumindest konkludente Einwilligung vorliegen.

In strafrechtlicher Hinsicht reicht unter Umständen eine konkludente oder sogar nur mutmaßgebliche Einwilligung.

Soweit das BDSG einschlägig ist, ist in datenschutzrechtlicher Hinsicht grundsätzlich eine schriftliche Einwilligung erforderlich.

Im Verhältnis der Berater untereinander wäre bei Informationsweitergaben (die Rückschlüsse auf den betroffenen Klienten zulassen) keine Einwilligung

erforderlich, wenn sie als Einheit auftreten, das heißt, wenn die ehrenamtlichen Berater als Gehilfen des Sozialarbeiters fungieren (nur dann sind diese - wie oben ausgeführt - selbst schweigepflichtig). Dies sollte den Klienten aber transparent gemacht werden.
(Andernfalls bestünde auch im Verhältnis des Sozialarbeiters zu den ehrenamtlichen Beratern eine Schweigepflicht.)
Eine weitere Frage war, ob auch gegenüber dem Gesamtvorstand des Vereins die Schweigepflicht besteht. Der Gesamtvorstand besteht aus den haupt- und ehrenamtlichen Beratern sowie weiteren Personen, die den Klienten nicht ohne weiteres bekannt sind.

Im Verhältnis zum Gesamtvorstand, d.h. zu den Vorstandsmitgliedern, die nicht selbst Berater sind, müsste im Grundsatz ebenfalls Vertraulichkeit gewahrt werden, es sein denn, es liegen besondere Gründe vor, die eine Befassung des Gesamtvorstandes mit den Daten erforderlich machen, beispielsweise die Gewährung finanzieller Hilfen. Auch insoweit ist gegenüber dem Klienten für Transparenz zu sorgen, sodass zumindest eine konkludente oder mutmaßliche Einwilligung vorliegt.

Den Verein interessierte außerdem, wie bei einer etwaigen Auflösung der Beratungsstelle zu verfahren sei:
Hier muss sichergestellt werden, dass die Datenträger (Akten etc.) entweder an die Betroffenen herausgegeben oder datenschutzgerecht vernichtet werden.
Wenn die Funktion der Beratungsstelle von einer anderen Beratungsstelle übernommen werden soll, käme eventuell auch in Betracht, dass die andere Stelle die Unterlagen mit übernimmt. Aber auch dies wäre nur mit Einwilligung der Betroffenen zulässig. Entsprechend der Rechtssprechung des Bundesgerichtshofes zum Verkauf von Arztpraxen kann hierbei eine mutmaßliche Einwilligung der Betroffenen nicht pauschal unterstellt werden. Vielmehr müssen entweder die Betroffenen vor der Auflösung gefragt werden, ob sie mit einer Weitergabe einverstanden sind, oder es muss sichergestellt werden, dass die neue Stelle erst mit Einverständnis der Betroffenen Zugriff auf die Unterlagen nimmt. In Betracht käme, dass etwa ein Mitarbeiter der alten Beratungsstelle die Unterlagen sicher verwahrt und nur dann - einzeln - herausgibt, wenn sich der Betroffene bei der neuen Stelle in Beratung begibt, oder die neue Stelle erhält die Unterlagen in verschlossenen Umschlägen, auf die nur im Beisein des Betroffenen oder, falls ein Mitarbeiter der alten Stelle übernommen wurde, in dessen Beisein Zugriff genommen wird.
Ob in Einzelfällen aufgrund der Hilfsbedürftigkeit des Betroffenen eine Weitergabe der Unterlagen auch ohne dessen Einverständnis möglich ist (nach den Grundsätzen des rechtfertigenden Notstandes) müsste jeweils sorgfältig geprüft werden.

12.3 Datenbank über potenzielle Spender von Knochenmark

Um ausreichend viele Spender für Knochenmarktransplantationen zur Verfügung zu haben, hat es sich als notwendig herausgestellt, weltweit nach Spendern Ausschau zu halten. Wirtschaftlich möglich ist diese Form der weltweiten Zusammenführung von Spender und Patient nur mit Hilfe moderner Informationstechnologie. Ein gemeinnütziger Verein, der diese Aufgabe in Hessen übernommen hat, erfüllt die medizinischen Voraussetzungen und speichert die erforderlichen personenbezogenen Daten der potenziellen Spender in einer zentralen Datei. Aus dieser Datei werden mit Hilfe einer Code-Nummer, des Geburtsdatums und der Angabe des Geschlechts des bzw. der potenziellen Spender die erforderlichen medizinischen Daten in ein von einer gemeinnützigen Gesellschaft geführtes Zentralregister übermittelt. Dort stehen sie für den weltweiten Abgleich zur Verfügung.

Erst nachdem die entsprechenden medizinischen Untersuchungen bei dem Patienten, welcher eine Knochenmarkspende nachsucht, stattgefunden haben und mit Hilfe einer eingefrorenen Blutprobe des potenziellen Spenders geklärt wurde, dass die erforderlichen Voraussetzungen erfüllt sind, wird mit Hilfe der Code-Nummer auf den potenziellen Spender zurückgegriffen. Ausschließlich die hier ansässige speichernde Stelle hat dann die Möglichkeit, den betreffenden Spender zu identifizieren. Sie gibt die Personalien des potenziellen Spenders jedoch auch dann nicht weiter, sondern spricht ihn selbst an, damit er - nach einem weiteren ärztlichen Beratungsgespräch - nun endgültig über die Knochenmarkspende entscheidet.

Nach erfolgter Entnahme des Knochenmarks wird dieses unter der Code-Nummer an die behandelnden Ärzte des Empfängers weitergeleitet. Als Erlaubnistatbestand zur Datenverarbeitung wird die schriftliche Einwilligung nach § 4 BDSG vom Betroffenen eingeholt. Die von dem Verein um datenschutzrechtliche Beratung gebetene Aufsichtsbehörde konnte bestätigen, dass die vorgelegte Einwilligung alle Anforderungen des § 4 BDSG erfüllt.
Durch eine genaue Beschreibung der Vorgehensweise wurde dafür gesorgt, dass informierte Einwilligungen vorliegen.

Außerdem bestehen genaue Zugriffsregelungen und weitere Maßnahmen zur Datensicherheit liegen vor.

13. Direktmarketing und Werbung

13.1 Zweifelhafte Herkunft von Empfehlungsadressen

Alle Einzel-, Groß- und Versandhändler sowie viele Dienstleister anderer Branchen leben von ihren ständigen Bemühungen, neue kaufkräftige Kunden zu gewinnen. Eine beliebte und oft auch erfolgreiche Methode, kostenlos neue Namen und Anschriften zu erfahren, ist es, Kunden im Katalog oder auf dem Bestellschein zu bitten, die Daten von interessierten Freunden oder Verwandten anzugeben. Leider wissen die betroffenen Bekannten oftmals nichts von dieser gut gemeinten Weitergabe ihrer Adressdaten und werden unvorbereitet mit Werbezusendungen oder Vertreterbesuchen von unbekannten Firmen überrascht. Die Frage der Betroffenen nach der Herkunft ihrer Daten wird dann nur mit einem lapidaren Verweis auf die Empfehlung durch irgendwelche Freunde beantwortet, was bei vielen Betroffenen den Verdacht nährt, dass die Unternehmen eine vermeintlich unzulässige Datenquelle verschleiern möchten. Wo genau die Daten herstammten, war auch für die eingeschaltete Datenschutzaufsichtsbehörde in den seltensten Fällen nachvollziehbar.

Die Unternehmen wurden aufgefordert, künftig die Herkunft der werblich genutzten Adressdaten nachvollziehbar zu dokumentieren. Dazu gehört bei der Nutzung von neuen Empfehlungsadressen auch der Name und die Anschrift des Kunden, der die Daten seiner Bekannten, Verwandten oder Freunde weitergibt. Nur so ist es möglich, dass das unabdingbare Recht von betroffenen Bürgerinnen und Bürgern auf Auskunft über Art und insbesondere Herkunft der gespeicherten Daten nach § 34 BDSG realisiert werden kann und dass überprüft werden kann, ob die Datenerhebung gegen Treu und Glauben verstieß.

13.2 Ein Dauerbrenner: Die Nichtbeachtung von Werbewidersprüchen und Auskunftsersuchen

In jedem Berichtsjahr ist es im Bereich der Massenwerbung leider immer wieder notwendig, dass den Forderungen von Bürgerinnen und Bürgern nach Beachtung ihrer datenschutzrechtlichen Rechte durch die Datenschutzaufsichtsbehörde Nachdruck verliehen werden muss. Regelmäßig werden Anfragen von Betroffenen nach der Herkunft ihrer zur Werbung genutzten Daten (§ 34 Abs. 1 BDSG) und Widersprüche gegen die werbliche Nutzung der Adressdaten (§ 28 Abs. 3 BDSG) von Unternehmen nicht beachtet. Wie schon so oft wurde gegenüber der Behörde behauptet, die Schreiben der Petenten wären in den Firmen nie angekommen oder auch nur versehentlich nicht beantwortet worden. Einige Unternehmen wurden aufgefordert, die Werbedaten nicht zu löschen, sondern i.S.d. § 35 Abs. 3 BDSG in Sperrlisten zu speichern. Mit den Sperrvermerken sollen in der Zukunft die zumeist angemieteten Adresslisten der Unternehmen abgeglichen werden, sodass die Betroffnen schon vor der Versendung von Werbebriefen ausgefiltert und deren Daten zuverlässig von der werblichen Nutzung ausgeschlossen werden können.

Die berechtigten Beschwerden der Petenten betrafen überwiegend Einzelhandelsunternehmen verschiedener Branchen (Möbel, Kraftfahrzeuge, Computer) und auch eine Bank. Alle Unternehmen haben letztlich auf die Beanstandungen der Aufsichtsbehörde reagiert, die Daten für die werbliche Nutzung gesperrt und die Anfragen der Beschwerdeführer nach der Adressherkunft hinreichend beantwortet.

Den betroffenen Bürgerinnen und Bürgern ist zu empfehlen, sich mit ihren Werbewidersprüchen und Auskunftsbegehren unter Bezug auf das Bundesdatenschutzgesetz immer direkt an den betrieblichen Datenschutzbeauftragten und nicht an die datenschutzrechtlich erfahrungsgemäß eher unsensible Werbe- oder Marketingabteilung des jeweiligen Unternehmens zu wenden.

14. Datenverarbeitung und Beauskunftung im Versandhandel

14.1 Versandhändler offenbart die Telefonnummern seiner Kunden

Der Kunde eines Versandhändlers beschwerte sich darüber, dass bei der Lieferung durch den Versandhändler auf dem zugestellten Paket deutlich sichtbar seine Telefonnummer verzeichnet war. Der Betroffene begründete sein Missfallen damit, dass er bei der Beantragung seines Telefons gebeten hatte, in den öffentlichen Verzeichnissen mit seiner Telefonnummer nicht zu erscheinen. Da er zum Zeitpunkt der Anlieferung nicht anwesend gewesen sei, habe der Zustelldienst das Paket an einen Nachbarn übergeben. Aufgrund der auf dem Paket aufgeführten Telefonnummer, die somit der Nachbarschaft zugänglich gemacht worden ist, sah der Betroffene seine schutzwürdigen Belange erheblich beeinträchtigt, weil er seine private Telefonnummer nur von ihm ausgewählten Personen zur Verfügung stellen möchte.

Das Unternehmen führte als Begründung an, dass sowohl Zustelldienste als auch Nachbarn, die freundlicherweise derartige Zusendungen entgegennehmen, die auf dem Paket angegebene Zustell-Telefonnummer anrufen können, um dem Empfänger Bescheid zu geben, dass sein Paket entweder zugestellt wird oder aber beim Nachbarn abholbereit steht.

Das Unternehmen wurde aufgefordert, das Verfahren zu ändern. Es besteht die Möglichkeit, vor Aufdruck der Telefonnummer in öffentlichen Verzeichnissen nachzuschauen, ob diese Telefonnummer dort vorhanden ist. In diesem Fall bestehen keine Bedenken gegen eine weitere Veröffentlichung. Wenn sie dort aber nicht zu finden ist, hat der Aufdruck zu unterbleiben. Eine andere Möglichkeit wäre, bei der Bestellannahme oder in irgendeiner anderen Form vor dem Versand den Betroffenen um seine Einwilligung zu bitten.

14.2 Angabe des Geburtsdatums bei Bestellungen

Einige Betroffene haben ihren Unmut darüber geäußert, dass sie bei Bestellungen von den Versandhändlern aufgefordert werden, neben Name, Anschrift und Kundennummer auch ihr Geburtsdatum anzugeben. Die Betroffenen waren der Auffassung, dass die Frage nach dem Geburtsdatum nicht zur Erfüllung des Kaufvertrages erforderlich sei.

Die Versandhändler begründen ihre Frage nach den Geburtsdaten damit, dass sie sich absichern möchten, dass der Besteller auch derjenige ist, der die Ware tatsächlich kaufen möchte. Die Aufsichtsbehörde konnte sich davon überzeugen, dass es bedauerlicherweise sehr häufig vorkommt, dass Ware auf Namen und unter der Anschrift von Empfängern bestellt wird, ohne dass diese davon Kenntnis haben. Dies verursacht einen enormen Kostenaufwand für die Versandhändler, da der Betroffene, der die unverlangte Ware erhält, diese zurücksendet und dafür natürlich nicht belangt werden kann. Der Verursacher der Kosten ist unbekannt.

Durch die Frage nach dem Geburtsdatum können solche Fehllieferungen zum Teil vermieden werden. Dies ist etwa dann der Fall, wenn der Adressat der Lieferung mit seinem Geburtsdatum bereits in der Kundendatei gespeichert ist und der telefonische Besteller dieses Geburtsdatum nicht kennt.

Darüber hinaus wird die Angabe des Geburtsdatums nach Auffassung der Versandhändler auch für die Durchführung von Bonitätsprüfungen, also für Schufa-Anfragen, benötigt, soweit Lieferung auf Rechnung gewünscht wird. Dies ist gerechtfertigt, denn durch die Angabe des Geburtsdatums als weiteres Identifikationsmerkmal können Verwechslungen vermieden werden (insbesondere bei häufig vorkommenden Namen).

Die Versandhändler verwiesen außerdem darauf, dass zu ihrem Kundenkreis auch solche Mitmenschen gehören, die von vornherein betrügerische Absichten hegen. Durch falsche oder unvollständige Angabe der Personalien wür-

den diese Personen sich erhoffen, dass ein Negativ-Eintrag bei der Schufa nicht bekannt wird und säumige Zahlungen bei späteren Bestellungen nicht zuordenbar wären.

Ob man diesem Problem durch die Frage nach dem Geburtsdatum wirksam begegnen kann, erscheint zweifelhaft, denn wer betrügen will bzw. Negativ-Einträge bei der Schufa verschleiern will, gibt auch das Geburtsdatum falsch an und erschwert damit die Zuordnung erst recht.

Allenfalls in den Fällen, in denen die betrügerische Energie nicht allzu hoch ist und etwa nur der Vorname leicht inkorrekt angegeben wird (beispielsweise durch etwas andere Schreibweise oder indem nur der zweite Vorname genannt wird), aber das Geburtsdatum richtig angegeben wird, ermöglicht dieses zusätzliche Merkmal die Identifikation des Kunden.

Im Ergebnis beanstandete die Aufsichtsbehörde die Erhebung und Verarbeitung des Geburtsdatums nicht.

Nicht akzeptabel ist es jedoch, wenn die Versandhändler das Merkmal teilweise wiederum selbst zur Unterscheidung nicht ernst nehmen:
So kann es vorkommen, dass ein Betroffener, der bereits Kunde bei einem Versandhändler ist und bei dem zufälligerweise Namensgleichheit mit einem unseriösen Neukunden besteht, dessen Anschrift und Bestellung zugeordnet erhält.
Das kann z.B. im Rahmen einer telefonischen Bestellannahme geschehen, wenn der Kunde nach seiner Kundennummer gefragt wird und behauptet, er habe sie gerade nicht zur Verfügung. Wenn er dann auch noch die Frage bejaht, ob er eine neue Anschrift angeben möchte, kann diese Fehlzuordnung zustande kommen. In einem derartigen Fall ist dann das Datum "Geburtsdatum" nur noch nebensächlich und wird als untergeordnetes Merkmal betrachtet, dem keine Bedeutung zukommt.
Gerade in Fällen wie diesen müssten die Versandhändler durch Frage nach dem Geburtsdatum die Identität des Anrufers aufklären.

15. Datenübermittlung an Dachverband

Ein Rechtsanwalt, der eine Reihe von Sportvereinen vertritt, wandte sich gegen die Änderung der Spielordnung eines Hessischen Sport-Dachverbandes.

Während nach der alten Fassung die Mitgliedsvereine und die Spieler lediglich verpflichtet waren, den Abschluss und die Änderung von Amateurverträgen dem Dachverband mitzuteilen, schreibt die Neufassung vor, dass Vertragsabschlüsse, Änderungen und Verlängerungen durch Zusendung einer Ausfertigung der Vertragsurkunde anzuzeigen sind.

Da die Vertragsurkunde auch Informationen über

- Vergütungsregelungen,
- Prämienvereinbarungen und
- Sondervereinbarungen

enthält, vertrat der Beschwerdeführer die Auffassung, dass diese Neuregelung datenschutzrechtlich unzulässig sei.

Die Regelung, dass die Vertragsurkunde beim Verband zu hinterlegen ist, wurde auf Initiative und Vorgabe des Bundesverbandes eingeführt, um im Einzelfall Beweisschwierigkeiten über den Inhalt des Vertrages zu vermeiden. Anlass war der Fall eines Spielers, der zwei Verträge mit unterschiedlichen Vereinen geschlossen hatte. Streitig war eine Ausstiegsklausel in einem der beiden Verträge. Es ließ sich nicht feststellen, welcher Vertrag die Originalfassung wiedergab. Der Streit hatte Bedeutung für die Zulässigkeit des beabsichtigten Wechsels, der Spielberechtigung, die Zahlung der Transfersumme und einer Ausbildungs- und Förderungsentschädigung.

Für die spieltechnischen Fragen soll es künftig allein auf den beim Verbund hinterlegten Vertrag ankommen.

Die Spieler haben laut Spielordnung das Recht, der Weitergabe ihres Vertrages an den Verband zu widersprechen. Sie trifft dann lediglich ein Beweis-

nachteil, da nicht (rechtzeitig) hinterlegte Verträge bei Streitigkeiten wie im dargestellten Fall nicht berücksichtigt werden können.

Die Verpflichtung zur Vorlage der Amateurverträge ist daher grundsätzlich gerechtfertigt, da es zu den satzungsgemäßen Aufgaben der Landesverbände gehört, unter anderem die Zulässigkeit von Spielerwechseln und die Spielberechtigung zu prüfen. Hierfür benötigen die Verbände die in den Verträgen enthaltenen Daten über die Vertragspartner, die Vertragslaufzeit und etwaige Ausstiegsklauseln.

Mit dem vom Landesverband eingeschalteten Bundesverband konnte die Aufsichtsbehörde Einigkeit erzielen, dass die Angaben über Vergütungsregelungen und Prämienvereinbarungen im Vertrag geschwärzt werden können, da diese Angaben für die Verbandsaufgaben nicht erforderlich sind.
Hinsichtlich sonstiger Sondervereinbarungen kommt es auf den jeweiligen Gegenstand an: Soweit ihr Inhalt weder Laufzeit noch Kündigungsregelungen noch sonstige die Wirksamkeit des Vertrages unmittelbar betreffende Bestimmungen enthält, können sie ebenfalls geschwärzt werden.

Die Offenlegung des Vertrages gegenüber Dritten erfolgt nur, soweit dies im Rahmen der Spielerverwaltung erforderlich ist (z.B. Sportgericht, anderer Landesverband).

Insgesamt konnte so einvernehmlich eine Auslegung und Handhabung gefunden werden, die allen Interessen gerecht wird.

Der Bundesverband wird alle Landesverbände unterrichten.

16. Datenverarbeitung durch Parteien

Die von der CDU durchgeführte Protestbrief-Aktion gegen die Rentenpolitik der Bundesregierung veranlasste Bürger zu Eingaben bei der Aufsichtsbehörde.

Da die Briefe sich an die Rentner richten sollten, vermuteten die Bürger, dass die Partei über "Rentnerdateien" verfüge, und baten um datenschutzrechtliche Bewertung.

Die Hessische CDU hat jedoch lediglich die auf einer aktuellen Telefon-CD-ROM gespeicherten Daten in der Weise genutzt, dass durch ein Dienstleistungsunternehmen anhand einer Vornamenanalyse diejenigen Personen (nebst Adresse) herausgefiltert wurden, die sich wahrscheinlich im Rentenalter befinden.

Die Vornamenanalyse basiert lediglich auf der Erkenntnis, dass die Verwendung von Vornamen den Änderungen des Zeitgeschmacks unterliegt und somit eine Wahrscheinlichkeitszuordnung von Name und Geburtsjahr der betreffenden Person möglich ist. Sie wird in der gewerblichen Wirtschaft häufig für Werbemaßnahmen eingesetzt.

Diese Vorgehensweise ist nach § 28 Abs. 1 Nr. 3 BDSG erlaubt, da die Telefon-CD-ROM eine allgemein zugängliche Quelle ist und die Abwägung zwischen dem Interesse der Partei, durch die Briefe an der politischen Willensbildung mitzuwirken, und etwaigen entgegenstehenden schutzwürdigen Interessen von Betroffenen ergibt, dass letztere jedenfalls nicht offensichtlich überwiegen können.

Die anfragenden Bürger wurden von der Aufsichtsbehörde außerdem darauf hingewiesen, dass sie nach dem neuen Telekommunikationsrecht selbst entscheiden können, ob und in welchem Umfang ihre Daten in ein öffentliches elektronisches Kundenverzeichnis aufgenommen werden sollen.

Außer der oben dargestellten Adressauswahl nebst Versendung der Protestbriefe wurden die Briefe auch auf folgende Weise verteilt:

Die Kreisverbände erhielten Informationsbriefe, welche nicht persönlich adressiert waren und verteilten diese durch Parteimitglieder an diejenigen Haushalte, in welchen nach den persönlichen Kenntnissen der Parteimitglieder Rentner wohnen.

Eine Rentner-Datei oder Ähnliches bestand auch bei den Kreisverbänden nicht.
Dieser Verteilungsweg ist daher datenschutzrechtlich von vornherein irrelevant, weil keinerlei Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien erfolgt und daher das BDSG nicht anwendbar ist.

17. Verteilung von Kopien aus dem Liegenschaftsbuch

Die Vervielfältigung von Auszügen aus dem Liegenschaftskataster zu gewerblichen Zwecken und die Weitergabe dieser Kopien an Dritte unterliegt nach § 17 Abs. 2 Hessisches Vermessungsgesetzes (HVG) einem Genehmigungsvorbehalt durch die Kataster- und Landesvermessungsbehörden. Dieser Vermerk wird auf jedem Auszug aus dem Liegenschaftskataster angebracht und zudem mit einem Hinweis auf die entsprechende Bußgeldvorschrift des § 22 HVG versehen. Auch wenn diese Genehmigung vorliegt, sind die auf den Auszügen enthaltenen personenbezogenen Daten (z.B. Geburtsdatum oder Eigentumsanteil des Eigentümers oder der Eigentümer) zu schwärzen, soweit diese nicht für den Zweck der Weitergabe erforderlich sind.

Ein betroffener Grundstücksnachbar eines Baugrundstückes wies die Datenschutzaufsichtsbehörde darauf hin, dass ein Architekt - ohne Berücksichtigung etwaiger schutzwürdiger Belange der betroffenen Anwohner - genaue Kopien aus dem Katasterbuch ungeschwärzt an alle Anliegerhaushalte verteilte, um deren Standpunkt zu einigen Details des Neubaues zu erfahren. Dass es für die Erlangung solcher Stellungnahmen nicht erforderlich ist, die Geburtsdaten oder die Eigentumsanteile aller Anwohner zu übermitteln, versteht sich von selbst. Bei der Ermittlung des Sachverhaltes stellte sich zusätzlich heraus, dass dem Architekten noch nicht einmal die Genehmigung der Katasterbehörde zur Vervielfältigung des Auszugs vorlag. Das Architekturbüro wurde auf die klare Rechtslage hingewiesen und die ungeschwärzte Verteilung der Kopien beanstandet. Der Aufsichtsbehörde wurde zugesagt, dass bei künftigen Projekten die unnötigen Detailangaben geschwärzt werden und vor der Vervielfältigung der Katasterauszüge eine Genehmigung nach § 17 Abs. 2 HVG eingeholt wird.

18. Instrumentalisierung des Datenschutzrechts

18.1 Datenweitergabe an Subauftragnehmer und angebliche Missbräuche des Dienstleisters

Ein Unternehmer, der als Dienstleister unter anderem für Banken tätig gewesen war, sah seine wirtschaftliche Existenz vernichtet und führte dies auf einen pflichtwidrigen Umgang mit seinen Daten zurück.

Der von einer Bank beauftragte Subunternehmer - ein Konkurrenzunternehmen - habe seine (Konto-)Daten bei der Datenverarbeitung ausgespäht und zu seinem Nachteil genutzt.

Für diese Behauptungen (Befürchtungen?) ließen sich keine schlüssigen Beweise finden. Der behauptete Verstoß ließ sich vor allem deshalb nicht nachweisen, weil die Vorgänge schon Jahre zurücklagen und der Betroffene seine Beschwerden über den Zeitraum von mehreren Jahren nach seinen eigenen Ausführungen nur mündlich gegenüber der Bank vorgetragen hatte. Sämtliche betroffenen Bankmitarbeiter bestritten aber, dass derartige Beschwerden überhaupt erhoben worden seien. Darüber hinaus lagen im fraglichen Zeitraum die detaillierten Bankdaten dem Subunternehmer nicht zur Datenverarbeitung vor.
Nach über zehn Jahren ließ sich auch nicht mehr aufklären, ob und gegebenenfalls auf welche Art und Weise ein Kontoauszug verschwunden war.

Es besteht die Möglichkeit, dass im vorliegenden Fall die Datenschutzproblematik nur vorgetragen wurde - so die Auffassung der betroffenen Bank -, um eine möglichst vorteilhafte Schuldenregelung gegenüber der Bank zu erlangen.

Als Konsequenz hieraus kann nur empfohlen werden, Datenschutzbeschwerden schriftlich dem Datenschutzbeauftragten des Unternehmens und gegebenenfalls auch der Aufsichtsbehörde zeitnah vorzutragen. Wenn über Jahre

von einem Betroffenen - der sich aufgrund seiner Tätigkeit in Datenschutzfragen auskennt - weder der Datenschutzbeauftragte des beschuldigten Unternehmens noch die Aufsichtsbehörde eingeschaltet wird, kann daraus nur der Schluss gezogen werden, dass ihm entweder Datenschutzfragen gleichgültig waren oder dass das behauptete Problem überhaupt nicht existierte.

18.2 Verweigerung der Herausgabe von Akten an das Amtsgericht

Das Amtsgericht hat die Zuverlässigkeit von Inkassounternehmen zu überprüfen und muss gegebenenfalls die Zulassung nach § 15 der Ausführungsverordnung zum Rechtsberatungsgesetz widerrufen.

Bei entsprechenden Amtshandlungen eines Amtsgerichtes verweigerte ein Inkassounternehmen die Herausgabe von Inkassodaten mit dem Hinweis auf den Datenschutz. Wie soll das Amtsgericht aber seiner Aufsichtspflicht gemäß der genannten Verordnung nachkommen, wenn keine Akteneinsichtsmöglichkeit besteht?
Ganz offensichtlich wollte sich das betroffene Unternehmen mit den vorgeschobenen Datenschutzargumenten einer staatlichen Aufsicht entziehen.
Eine Besonderheit am Rande war zudem, dass bei einer kurzfristig anberaumten Kontrolle durch die Datenschutzaufsichtsbehörde die gewünschten Inkassoakten angeblich alle "zufällig" beim Steuerberater waren.

Offensichtlich wird von dem Unternehmen - entsprechend den jeweiligen Bedürfnissen - der Datenschutz instrumentalisiert.

Das Amtsgericht berief sich zu Recht darauf, dass die Einsichtnahme in die konkreten Daten unbedingt erforderlich war, um seine Aufsicht wahrzunehmen und dass eine entsprechende Datenerhebung folglich durch die genannte Ausführungsverordnung zwingend vorausgesetzt wurde.

Damit war auch die Übermittlung der Daten durch das Inkassounternehmen an das Amtsgericht gerechtfertigt, es lag zumindest der Erlaubnistatbestand des § 28 Abs. 2 Nr. 1 a BDSG vor (Übermittlung im öffentlichen Interesse erforderlich).

Nach dieser Diskussion erhielt das Amtsgericht auch die geforderten Akten.

19. Externer Datenschutzbeauftragter und interne Koordination im Konzern

Ob bei einem großen Unternehmen die Bestellung eines externen Datenschutzbeauftragten sachgerecht ist, muss jeweils kritisch hinterfragt werden, da bei einem großen Konzern so viele unternehmensspezifische Einzelheiten bekannt sein müssen, dass für einen einzelnen Externen die Übersicht verloren gehen kann. Ein externer Datenschutzbeauftragter ist daher nach Auffassung der Aufsichtsbehörde für mittlere und kleinere Unternehmen besser geeignet.

Im Konzern werden dem Datenschutzbeauftragten in der Regel in den einzelnen Betriebsteilen Koordinatoren zugeordnet. Diese Koordinatoren sind in den einzelnen Gliederungen des Betriebes Ansprechpartner der Betriebsangehörigen und sammeln gleichzeitig Informationen für den Datenschutzbeauftragten. Bei einem externen Datenschutzbeauftragten kann auf Koordinatoren prinzipiell nicht verzichtet werden, weil die Mitarbeiter auch einen ortsnahen Ansprechpartner haben müssen. Mit den Koordinatoren kann der Datenschutzbeauftragte bei Schulungen einen guten Multiplikatoreffekt erreichen, was für den Betrieb in der Regel kostengünstiger ist als zentrale Schulungen.
Der Koordinator sollte über eine geeignete Qualifikation verfügen und nicht ausgerechnet für die Leitung der Datenverarbeitung zuständig sein. Der Leiter der Datenverarbeitung eines Betriebsteils ist sicher fachlich sehr geeignet, aber eine unabhängige Kontrolle seiner eigenen Tätigkeit kann er nicht ausüben. Es wird von einem Datenverarbeitungsleiter ohnehin erwartet, dass er unter Einhaltung der Datenschutzvorschriften seine Tätigkeit verantwortungsvoll organisiert.
Ein 4-Augen-Prinzip, d.h., eine von der Leitungsebene unabhängige Kontrolle lässt sich nur durch einen anderen Datenschutzkoordinator erreichen.

Würde dies nicht angestrebt, wären über die Hintertür der Koordination die leitenden Mitarbeiter des Datenverarbeitungsbereiches auch ihre eigenen Kontrolleure.

Bei Konzernunternehmen, die sehr unterschiedliche Geschäftsfelder aufweisen und nicht einheitlich strukturiert sind, sollte möglichst dezentral für jedes Tochterunternehmen ein Datenschutzbeauftragter ernannt werden. Synergieeffekte sind hier mit einem zentralen Datenschutzbeauftragten nicht in jedem Fall (oder nur in geringem Umfang) zu erwarten.

20. Datensicherheit - Warum Kundendaten löschen - der Speicherplatz reicht doch noch

Bei einem bundesweit organisierten System zum (Vor-)Verkauf von Konzert- und sonstigen Eintrittskarten wurde ein Programm angewandt, bei welchem ein programmmäßiges (softwaremäßiges) Löschen von personenbezogenen Daten nicht vorgesehen war. Es bestand die Anweisung an die verkaufenden Stellen, dass der Datensatz im Bereich des Namensfeldes mit Buchstabenkombinationen zu überschreiben sei, wenn ein Kunde eine Löschung verlange.

Die Aufsichtsbehörde hält das Löschen von Bestellerdaten im Kartenvorverkaufgeschäft für unabdingbar, da, nachdem die Karten gekauft worden sind, ein Zweck hinsichtlich der Verarbeitung personenbezogener Daten für die Vorabbestellung nicht mehr vorhanden ist. Sie forderte daher das Unternehmen auf, das Verfahren in absehbarer Zeit so zu verändern, dass für die Mitarbeiter in den einzelnen Verkaufsstellen die Möglichkeit besteht, ein automatisches programmmäßiges Löschen vorzunehmen. Das Unternehmen hat der Aufsichtsbehörde schriftlich zugesichert, das Verfahren entsprechend zu verändern.

21. Ordnungswidrigkeitenverfahren

Von den bereits im letzten Tätigkeitsbericht aufgeführten Bußgeldverfahren konnten im Berichtsjahr 1999 zwei weitere Verfahren nach § 44 Abs. 1 Nr. 6 BDSG gegen zwei Dienstleistungsunternehmen mit einer Bußgeldsumme von 1.450 DM abgeschlossen werden. Die Geschäftsführer der beiden Unternehmen hatten trotz mehrmaliger Aufforderung entgegen § 38 Abs. 3 Satz 1 BDSG der Datenschutzaufsichtsbehörde keine bzw. unvollständige Auskünfte zur Verarbeitung personenbezogener Daten in ihren Betrieben erteilt. Beide Bußgeldbescheide sind inzwischen rechtskräftig geworden.

Im Berichtsjahr 1999 wurden von den Aufsichtsbehörden sechs Verfahren nach dem Gesetz über Ordnungswidrigkeiten nach § 44 Abs. 1 BDSG gegen die Geschäftsführer Daten verarbeitender Gewerbebetriebe eingeleitet. Ein Verfahren betraf ein Unternehmen, das als Dienstleistungsdatenverarbeiter sogar der Meldepflicht zum bei der Aufsichtsbehörde geführten Register nach § 32 Abs. 1 BDSG und damit der Regelaufsicht der Behörde unterliegt. Obwohl das Unternehmen sowohl schriftlich als auch persönlich vor Ort auf seine Auskunftspflichten hingewiesen wurde, konnte dem Anspruch der Datenschutzaufsicht auf rechtzeitige, vollständige und korrekte Angaben erst mit dem Erlass eines Bußgeldbescheides über 3.500 DM der erforderliche Nachdruck verliehen werden.

Zwei Verfahren wurden gegen den persönlich haftenden Gesellschafter und den Datenschutzbeauftragten einer als Kommanditgesellschaft geführten Auskunftei wegen nicht erfolgter Benachrichtigung nach § 33 BDSG durchgeführt. Beide wurden mit unterschiedlicher Gewichtung als verantwortlich für den Verstoß angesehen. Der gegen den Datenschutzbeauftragten erlassene Bußgeldbescheid über 1.000 DM ist unmittelbar rechtskräftig geworden. In dem Verfahren gegen den persönlich haftenden Gesellschafter ist durch Urteil des Amtsgerichts Kassel die Geldbuße auf 6.000 DM reduziert worden.

Gegen die beiden Geschäftsführer eines Direktmarketingunternehmens wurden ebenfalls Ordnungswidrigkeitenverfahren eingeleitet. Dabei wurde auf die Ahndung eines Verstoßes gegen die Pflicht zur rechtzeitigen Änderungsmeldung zum Register verzichtet. Die wegen nicht rechtzeitig erfolgter

Bestellung eines Datenschutzbeauftragten erlassenen Bußgeldbescheide über jeweils 1.000 DM haben nach Rücknahme der Einsprüche im gerichtlichen Verfahren zwischenzeitlich Rechtskraft erhalten.

Ein weiteres Verfahren betraf einen Internet-Provider im Rhein-Main-Gebiet, auf den die Aufsichtsbehörde auf Grund einer Beschwerde gegen die unverlangte Zusendung von Werbe-E-Mails aufmerksam wurde, als deren Absender das Unternehmen ermittelt werden konnte. Der Geschäftsführer dieses Internet-Anbieters hatte trotz mehrfacher Aufforderung die Fragen nach der Herkunft der vielen für die unverlangten Werbe-E-Mails benutzten E-Mail-Adressen zunächst ausweichend und auf genauere Nachfragen schließlich gar nicht mehr beantwortet. Obwohl er zur Erteilung der für die Arbeit der Behörde erforderlichen Auskünfte nach § 8 Abs. 1 TDDSG in Verbindung mit § 38 Abs. 3 Satz 1 BDSG ausdrücklich gesetzlich verpflichtet ist und auf das drohende Bußgeld hingewiesen wurde, hat er auf das gegen Ende des Berichtsjahres eingeleitete Bußgeldverfahren lediglich uneinsichtig und mit Drohungen gegen die Dienststelle reagiert.

Abschließend kann festgehalten werden, dass zwar vielen der modernen Datenverarbeitungsunternehmen selbst minimale datenschutzrechtliche Pflichten nicht bekannt sind. Der Großteil der angesprochenen Unternehmen ist allerdings nach entsprechenden Hinweisen der Datenschutzaufsichtsbehörden oder in einigen Fällen spätestens nach Androhung eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten durchaus bereit, den Aspekt des Schutzes personenbezogener Daten ihrer Kunden bei ihrer Geschäftstätigkeit künftig angemessen zu berücksichtigen. Die im letzten angeführten Fall erwähnte Totalverweigerung der Auskunftserteilung gegenüber der Datenschutzaufsichtsbehörde bleibt bisher die Ausnahme.

Wiesbaden, 25. August 2000

Der Hessische Ministerpräsident
Koch

Der Hessische Minister des Innern
und für Sport
Bouffier