15. Wahlperiode

Drucksache **15/357**

HESSISCHER LANDTAG

27. 08. 99

Vorlage
der Landesregierung

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

Vorgelegt mit der Stellungnahme zum Siebenundzwanzigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten - Drucks. 15/23 - nach § 30 Abs. 2 des Hessischen Datenschutzgesetzes vom 11. November 1986.

Eingegangen am 27. August 1999 · Ausgegeben am 14. September 1999

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 145 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.

Eingaben und Beschwerden direkt betroffener Bürger waren in 184 Fällen der Anlass für die Überprüfung der Verfahren zur Verarbeitung personenbezogener Daten bei diesen Stellen. Auf Vorfälle in 9 Unternehmen wurde die Aufsichtsbehörde durch Pressemeldungen und Fernsehbeiträge aufmerksam.

Betroffen waren:

- Kreditinstitute und Banken in 30 Fällen,
- der Handel und Einzelhandel in 15 Fällen,
- Interessenverbände und eingetragene Vereine in 15 Fällen,
- der Datenschutz in Arbeitsverhältnissen in 14 Fällen,
- Handels- und Wirtschaftsauskunfteien in 14 Fällen,
- Versicherungsgesellschaften in 12 Fällen,
- die Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa) in 11 Fällen,
- Online-Dienste und Internet-Provider in 10 Fällen,
- Unternehmen der Direktmarketing- und Werbebranche in 9 Fällen,
- Versandhandelsunternehmen in 7 Fällen,
- Vermieter, Hausverwaltungen und Mietervereine in 6 Fällen,
- das Gesundheitswesen (Kliniken, Apotheken, Ärzte) in 6 Fällen,
- Kreditkartenunternehmen in 6 Fällen,
- Adresshandelsunternehmen in 5 Fällen,
- Verlage und Unternehmen der Presse- und Medienwirtschaft in 4 Fällen,
- Markt- und Meinungsforschungsunternehmen in 3 Fällen,
- Inkassounternehmen in 3 Fällen,
- sonstige Stellen (z.B. Reisebüro, Taxizentrale, Anwälte) in 14 Fällen.

Die Häufung der Beschwerden aus dem Bereich der Geld- und Kreditwirtschaft (Banken, Auskunfteien, Schufa, Kreditkarten, Inkasso) ist zunächst auf die Konzentration dieser Branche in der Rhein-Main-Region des Regierungsbezirks Darmstadt zurückzuführen. Sie veranschaulicht allerdings auch die hohe Sensibilität der Bürger und Bürgerinnen für datenschutzrechtliche Fragestellungen im Zusammenhang mit dem Umgang und der Verarbeitung ihrer Einkommens-, Vermögens- und Bonitätsdaten.

In 46 Fällen waren die Beschwerden begründet. Sämtliche bei diesen Nachforschungen der Aufsichtsbehörde festgestellten unzulässigen Verarbeitungen personenbezogener Daten führten zu Beanstandungen der jeweiligen Verarbeitungsverfahren in den Unternehmen.

Die durch Verstöße gegen Datenschutzbestimmungen begründeten Eingaben richteten sich im Detail in neun Fällen gegen Kreditinstitute und Banken, in jeweils sieben Fällen gegen Einzelhändler und Firmen aus der Werbe- und Direktmarketingbranche, in jeweils drei Fällen gegen die Schufa, einen Online-Dienst und Vereine sowie Stellen, die Personal- und Bewerberdaten verarbeiten, in jeweils drei Fällen gegen Inkassounternehmen, Auskunfteien

und Ärzte sowie in jeweils einem Fall gegen ein Kreditkartenunternehmen, eine Versicherung, einen Vermieter und einen Marktforscher.

Bei zwölf 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 Aufsichtsbehörde führten, konnte durch die Diskussion der jeweiligen Sachverhalte eine zunehmende Sensibilisierung für datenschutzrechtliche Problemstellungen bei den speichernden Stellen erreicht werden.

In 25 Fällen waren die Ermittlungen der Aufsichtsbehörden zum Ende des Berichtsjahres noch nicht abgeschlossen.

Von den aus den Vorjahren anhängigen Beschwerden wurden 36 Fälle abgeschlossen. Die Beurteilung dieser in der Regel nur mit hohem Ermittlungsaufwand aufklärbaren Fälle durch die Aufsichtsbehörde ergab, dass davon 15 Eingaben begründet waren. Dabei hatten in drei Fällen Wirtschaftsauskunfteien, in jeweils zwei Fällen Versicherungen, Banken und Ärzte, sowie in jeweils einem Fall ein Hausverwalter, ein Unternehmen der Werbewirtschaft, eine politische Partei, eine Religionsgemeinschaft, die Schufa und ein Arbeitgeber personenbezogene Daten unzulässig verarbeitet oder genutzt.

Bei vier bereits in den Vorjahren eingereichten Beschwerden betroffener Bürger konnte eine abschließende Beurteilung, ob die Datenverarbeitung in zulässiger oder in unzulässiger Weise erfolgt war, mangels eindeutigen Sachverhaltes nicht getroffen werden.

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 Aufsichtsbehörde führt 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 der Datenschutzaufsichtsbehörde.

Am 1. Februar 1999 waren 685 meldepflichtige Unternehmen im Register der Aufsichtsbehörde eingetragen. Es konnte eine Steigerung gegenüber dem Vorjahr von ca. 11 v.H. verzeichnet werden.

Den größten Anteil hieran haben mit 542 Meldungen die nach § 32 Abs. 1 Nr. 3 BDSG gemeldeten Unternehmen, die im Auftrage Dritter als Dienstleistungsunternehmen weisungsgebunden im Sinne des § 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 Direktmarketing.

Mit 58 Meldungen haben die nach § 32 Abs. 1 Nr. 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 42 Registereinträgen die nach § 32 Abs. 1 Nr. 1 BDSG gemeldeten Unternehmen, die personenbezogene Daten zum Zwecke der Übermittlung speichern.

2.2 Prüfungsübersicht

Im Berichtsjahr wurden 35 Prüfungen nach § 38 Abs. 2 BDSG durchgeführt. Davon betrafen Datenverarbeiter nach § 32 Abs. 1 Nr. 3 BDSG insgesamt 20, nämlich

- Datenerfasser und Schreibbüros 7

- Telemarketingunternehmen 1
- Datenträgervernichter 6
- Servicerechenzentren 3
- Sonstige 6

Außerdem wurden insgesamt acht Datenverarbeiter nach § 32 Abs. 1 Nr. 1 BDSG geprüft, nämlich

- Auskunfteien 8
- Adresshändler 1

Des Weiteren wurden drei Unternehmen aus dem Bereich der Markt- und Meinungsforschung geprüft (§ 32 Abs. 1 Nr. 2 BDSG).

Die Prüfungen brachten folgendes Ergebnis:

- Beanstandungen 26
- Empfehlungen 6
- Ohne wesentliche Beanstandungen 3

Folgende wesentliche Mängel wurden am häufigsten festgestellt:

1. Keine bzw. verspätete oder unvollständige Registermeldung nach § 32 BDSG
2. Kein Datenschutzbeauftragter, Mängel in der Aus- und Fortbildung, Mängel in der Tätigkeit
3. Fehlende bzw. unvollständige Dokumentation
4. Mängel in der Benachrichtigung der Betroffenen (bei Auskunfteien)
5. Unzureichende Stichproben (bei Auskunfteien)
6. Keine bzw. unvollständige Weisungen des Auftraggebers nach § 11 BDSG
7. Mangelhafte Zugangskontrolle
8. Fehlende Zugriffskontrolle, unzureichende Passwortverwendung
9. Fehlende Verpflichtung auf das Datengeheimnis nach § 5 BDSG

2.3 Schwerpunkt bei den Datenschutzüberprüfungen nach § 38 Abs. 2 BDSG

Die Überprüfung von Auskunfteien bildete einen Schwerpunkt bei den im Berichtszeitraum nach § 38 Abs. 2 BDSG durchgeführten Datenschutzüberprüfungen. Die Überprüfungen bezogen sich unter anderem auf die Einhaltung bzw. Umsetzung der Absprachen zwischen den Verbänden der Handelsauskunfteien und den obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich.

1. Überprüfung der Angabe des berechtigten Interesses durch die Auskunfteien

Nach den oben genannten Absprachen sind zwei Promille der Anfragen bzw. mindestens 12 Stichproben jährlich im Hinblick auf die Angabe des berechtigten Interesses der anfragenden Stellen von den Auskunfteien durchzuführen.
Diese Mindestzahlen aus der Vereinbarung werden zu 100 v.H. eingehalten, in der Regel sogar überschritten.
Dennoch ist die Vorgehensweise bei 90 v.H. der geprüften Auskunfteien beanstandenswert:

Telefonische Anfragen wurden teilweise überhaupt nicht kontrolliert. Darüber hinaus werden Anfrager zwar mit einem Formblatt angeschrieben, dessen Beantwortung aber wird nicht weiter verfolgt. 50 v.H. der Auskunfteien erinnern zwar mit einem zweiten Schreiben, schließen dann aber auch den Fall ab, unabhängig davon, ob die Stelle nun antwortet oder nicht. 20 v.H. der geprüften Auskunfteien schrieben sogar die anfragenden Kundenmitarbeiter direkt an, statt der Geschäftsführung des anfragenden Unternehmens.

Da wesentlich mehr anfragende Stellen angeschrieben werden als erforderlich sind, reichen die Rückläufe immer noch über das Mindestmaß der zahlenmäßig geforderten Kontrollen hinaus. Nach Auffassung der Aufsichtsbehörde ist aber eine ausbleibende Beantwortung der Frage zur Angabe des berechtigten Interesses ein Indiz dafür, dass unter Umständen ein berechtigtes Interesse nicht vorgelegen hat.

Ebenso wenig ausreichend ist die bloße Wiederholung des bei der Anfrage angegebenen berechtigten Interesses ohne weitere Erläuterung. Hier sind die Auskunfteien gefordert, ein Niveau zu erreichen, das den Anforderungen der Absprache auch inhaltlich entspricht.

2. Benachrichtigung

Alle geprüften Betriebe nutzen zur Benachrichtigung ein Standardschreiben, welches jedoch häufig veraltet ist und nicht dem neuesten Stand der Absprachen mit den obersten Aufsichtsbehörden für den Datenschutz entspricht. Wenngleich die Abweichungen geringfügig sind, sollte doch die neueste Fassung verwendet werden.

Anlass zur Besorgnis gibt außerdem der Ablauf der Benachrichtigung. So wird automatisch vom System ein Zeichen gesetzt, wenn die Voraussetzungen zur Benachrichtigung erfüllt sind. Erst danach werden die Benachrichtigungen vom System bereitgestellt. Bei 50 v.H. der speichernden Stellen werden die Benachrichtigungen innerhalb des zentralen Systems ausgedruckt und mit normaler Post an die Einzelnen speichernden Stellen versandt. Es findet keinerlei Kontrolle hinsichtlich Vollständigkeit und Richtigkeit der Benachrichtigungen statt. So können beim Druck, beim Versand und auch bei der Weiterverarbeitung durch die Einzelnen speichernden Stellen durchaus Benachrichtigungen verloren gehen. Hier sollte ein anderes Konzept mit einer besseren Überprüfbarkeit langfristig verwirklicht werden.

3. Erfüllung der Benachrichtigungspflicht nach § 33 Abs. 1 Satz 2 BDSG durch Aufnahme eines Hinweises in ein Inkassoschreiben

Die Vertreter der obersten Datenschutzaufsichtsbehörden sind der Auffassung, dass eine Benachrichtigung des Betroffenen über die Weitergabe seiner personenbezogenen Daten an einen Auskunftsempfänger nicht im Rahmen eines Inkassomahnschreibens erfolgen kann. Insoweit fordert es der Grundsatz der Transparenz, dass im Falle der erstmaligen Übermittlung personenbezogener Daten an Auskunftsempfänger die gesetzlich vorgeschriebene Benachrichtigung durch die übermittelnde Stelle erfolgt. Dabei ist vor allem auch zu berücksichtigen, dass zum Zeitpunkt der Versendung eines Inkassoschreibens die Voraussetzungen für eine Benachrichtigung regelmäßig nicht gegeben sind.
Eine Einigung konnte bisher bei den Gesprächsteilnehmern nicht erreicht werden. Die Handelsauskunfteien hatten allerdings zugesagt, ihren Standpunkt nochmals zu überprüfen.

Bei 100 v.H. der Überprüfungen stellte sich heraus, dass ausschließlich im Rahmen des ersten Mahnschreibens unten auf dem Anschreiben unter P.S. folgender Hinweis erfolgt: "Über Sie sind auch Daten gespeichert bei: Auskunftei XY."

Auf Befragen erläuterten alle Geschäftsführer, dass sie diese Form der Benachrichtigung für ausreichend erachten.

4. Beauskunftung von Ehegatten

Es ist in der Vergangenheit immer wieder vorgekommen, dass im Rahmen einer Auskunft auch personenbezogene Daten des Ehepartners eines Vorstandsmitgliedes oder eines Geschäftsführers bzw. einer Geschäftsführerin übermittelt worden sind, da die Daten von Ehepartnern zusammen gespeichert worden waren. Gerechtfertigt ist eine Beauskunftung über Ehepartner jedoch erst dann, wenn die Auskunftei Grund zu der Annahme hat, dass es sich um so genannte Strohmannverhältnisse handeln könnte. Aufgrund der Absprachen mit den Verbänden sind Datenverarbeitungssysteme dahingehend geändert worden, dass eine eindeutige Trennung der Daten nach Personen durchgeführt wird. Das heißt, dass z.B. Daten zum Ehemann einer Geschäftsführerin nicht mehr automatisch an den Datensatz der Geschäfts-

führerin angekoppelt sind, sondern auch diese Daten in einem eigenständigen Datensatz verarbeitet werden. Mit dieser Maßnahme findet keine automatische Zusammenführung der Daten mehr statt.

Die Bereinigung des Altdatenbestandes wird allerdings noch einige Zeit in Anspruch nehmen, wobei die Auskunfteien sich bemüht zeigten, den Anforderungen Rechnung zu tragen.

In Anbetracht dessen, dass in der Regel im Jahresrhythmus alle Daten überarbeitet werden, fällt dies auch nicht schwer. Lediglich wenn feststeht, dass es sich um eindeutige Strohmannverhältnisse handelt, wird der Anfrager entsprechend informiert.

5. Datensicherheit

Hinsichtlich der Maßnahmen zur Datensicherheit kann zusammenfassend ausgeführt werden, dass bei allen überprüften Auskunfteien kein Grund zur Aussprache einer wesentlichen Beanstandung vorgelegen hat. Die Datenbestände werden ordnungsgemäß gesichert, es sind in der Regel ordnungsgemäße Zugriffsregelungen getroffen worden und die Verwendung von Passwörtern entspricht dem derzeitigen technischen Niveau.

3. Bearbeitung von Anfragen zu Problemen des Datenschutzes

Die Vielfalt der Anwendungsmöglichkeiten moderner Kommunikations- und Informationstechnologie in Kombination mit der fortschreitenden Globalisierung der Verarbeitung personenbezogener Daten im nicht-öffentlichen (privatwirtschaftlichen) Sektor führt in vielen Fällen zu erheblichem datenschutzrechtlichen Beratungsbedarf in den Unternehmen, Verbänden und bei den betroffenen Bürgern. Dies lässt sich an der hohen Fallzahl bei der Bearbeitung von telefonisch und schriftlich vorgetragenen Bitten um Stellungnahme und datenschutzrechtliche Beurteilung von Verarbeitungsverfahren oder geplanten Projekten durch die Datenschutzaufsichtsbehörde ersehen.

Die immer schnellere Verbreitung modernster Datenverarbeitungstechnologien mit nahezu unbegrenzten Speicherkapazitäten in sämtliche Lebensbereiche der Bürger macht Datenschutz zu einem überaus breit gefächerten Querschnittsthema, was sich auch in der Variationsbreite der bearbeiteten Anfragen widerspiegelt. Das Themenspektrum der Fragen erstreckte sich unter anderem auf Datenschutzprobleme bei Internetdiensten, Versicherungen, Ärzten, Apotheken, Krankenhäusern, Banken, der Werbewirtschaft, Videoüberwachung, europäischem Datenschutzrecht und Auslandsdatenverarbeitung, Arbeitnehmerdatenschutz, Schufa, Handelsauskunfteien und Vereinen bzw. Verbänden.

Zahlenmäßige Schwerpunkte waren auch im Berichtsjahr wieder bei den Anfragen zur Position und Funktion des betrieblichen Datenschutzbeauftragten nach §§ 36, 37 BDSG und der Verarbeitung personenbezogener Daten in Vereinen mit kulturellem, sportlichem oder sozialem Hintergrund zu verzeichnen, für die die Aufsichtsbehörde bereits seit Jahren geeignetes Informationsmaterial und ein umfassendes Beratungsangebot bereithält.

Zusätzlich hatten sich die Aufsichtsbehörden im Berichtsjahr verstärkt mit umfangreichen neuen rechtlichen Fragestellungen zu beschäftigen, die sich aus der Nutzung globaler Firmennetze und weltweiter Internet-Dienste (www, e-Mail) durch Unternehmen, Arbeitnehmer und Privatpersonen ergeben.

Immer deutlicher zeigt sich angesichts der Internationalisierung der Datenverarbeitung auch der Trend, die Datenschutzaufsichtsbehörde unter Vorlage entsprechend umfassender Konzeptionen um die datenschutzrechtliche Beurteilung technischer und juristischer Sachverhalte für geplante Verfahren und Projekte - oft im europäischen oder globalen Zusammenhang - zu bitten. Die Unternehmen versuchen durch die kooperative Zusammenarbeit mit der Aufsichtsbehörde, datenschutzrechtlichen Beanstandungen durch deutsche Dienststellen vorzubeugen und kostspielige Fehlinvestitionen zu vermeiden. Insgesamt ist dadurch eine deutliche qualitative Veränderung der Anfragen festzustellen.

Auch wenn zurzeit nur die betrieblichen Datenschutzbeauftragten einen formalen Rechtsanspruch auf Beratung im Sinne des § 37 Abs. 1 BDSG haben, ist es sicherlich sinnvoll, auch mit Unternehmensleitungen und/oder Mitarbeitervertretungen auftretende Zweifelsfragen bereits im Vorfeld geplanter Vorhaben abzuklären, statt abzuwarten, bis sich problematische oder unzulässige Verfahren etabliert haben, die dann beanstandet und abgeändert werden müssten.

Für Unsicherheiten auf Seiten der Unternehmen und ihrer Beschäftigten sorgte hier auch immer wieder die noch ausstehende Umsetzung der EG-Datenschutzrichtlinie in geltendes deutsches Recht. Es bleibt zu hoffen, dass diese Verunsicherungen durch die überfällige Novellierung des BDSG behoben werden und für alle Beteiligten durch klare allgemein verständliche Regelungen Rechtssicherheit für die Verarbeitung personenbezogener Kunden- oder Personaldaten in internationalen Zusammenhängen geschaffen werden kann.

4. Anlassunabhängige Überprüfungen bei Internet-Providern

Vor allem das Regierungspräsidium in Darmstadt hat sich im Berichtszeitraum eingehend mit der Thematik der neuen Medien und den speziellen datenschutzrechtlichen Anforderungen im Teledienstedatenschutzgesetz und im Mediendienstestaatsvertrag beschäftigt.

§ 8 Teledienstedatenschutzgesetz und § 18 Abs. 1 Mediendienstestaatsvertrag geben den Aufsichtsbehörden die Möglichkeit, anlassunabhängige Kontrollen bei Tele- und Mediendiensteanbietern durchzuführen.

Zunächst hat sich die Aufsichtsbehörde daher anhand von Recherchen im Internet, in Fachzeitschriften und der Tagespresse einen ersten allgemeinen Überblick über die im Aufsichtsbezirk ansässigen Tele- und Mediendiensteanbieter, insbesondere die Provider, verschafft.
Dabei wurde festgestellt, dass mindestens 100 Provider ihren Sitz im Aufsichtsbezirk haben.

An zehn dieser Provider hat die Aufsichtsbehörde einen Fragebogen zur Umsetzung der neuen Regelungen versandt, um sich insoweit einen ersten Eindruck zu verschaffen. Außerdem hat sie um Übersendung der Allgemeinen Geschäftsbedingungen gebeten.

Die Auswertung der Rückläufe ergab ein unterschiedliches Bild:

Zum Teil zeigte sich, dass die Unternehmen sich jedenfalls mit den gesetzlichen Anforderungen befasst und diese im Wesentlichen verstanden hatten. Zum Teil wurde aber auch aus den Antworten offenbar, dass noch sehr viel Aufklärungsarbeit notwendig ist.

Vor allem diese Fälle wird die Aufsichtsbehörde aufgreifen, um beratend tätig zu werden und gegebenenfalls Prüfungen durchzuführen.
Aus den Antworten wurde unter anderem ersichtlich, dass hinsichtlich der Unterscheidung von Tele- und Mediendiensten große Unsicherheiten bestehen.

Bei zwei Providern wurde bereits mit der Versendung des Fragebogens ein Prüftermin festgelegt. Der Fragebogen diente insofern gezielt der Prüfungsvorbereitung.
Diese Vorgehensweise hat sich in dem neuen Rechtsgebiet als sinnvoll erwiesen, weil sie zu einer kooperativen und zugleich effizienten Auseinandersetzung beiträgt.

In einzelnen Punkten gab offensichtlich der Fragebogen den Anstoß, dass sich die Unternehmen erstmals mit den gesetzlichen Anforderungen befassten.

Insgesamt waren die Erfahrungen der Aufsichtsbehörde insoweit recht positiv, als sich beide Unternehmen kooperativ zeigten. Eine abschließende Bewertung kann bei einem der geprüften Unternehmen erst erfolgen, wenn eine Reihe noch geforderter Unterlagen vorgelegt worden sind. Bezüglich des

anderen Unternehmens wird auf die Darstellung unter Punkt 9.1 und 9.3 verwiesen.

5. Datenverarbeitung bei Banken

5.1 Vergessene Unterlagen beim Umzug der Bank

Durch den Hinweis eines Korrespondenten der Deutschen Presse Agentur erhielt die Aufsichtsbehörde Kenntnis davon, dass ein Kunsthändler eine Kundenliste einer Bankfiliale in seinem Besitz hatte.

Der Kunsthändler war Nachmieter von Räumen, die zuvor als Geschäftsräume der Bank gedient hatten. Nach Angaben des Kunsthändlers sei er nun – ein Jahr nach dem Umzug – auf die Bankunterlagen gestoßen. Er habe Platz gebraucht und deshalb das Schloss eines bislang verschlossenen Einbauschrankes aufbohren lassen. Dort habe er die 1990 erstellten Kundenlisten gefunden. Diese enthielten unter anderem die Namen und Geburtsdaten, Kontonummern, Jahresumsätze und Salden der damaligen Kunden.

Wie es geschehen konnte, dass diese Unterlagen beim Umzug in den Räumlichkeiten verblieben waren, konnte nicht eindeutig geklärt werden. Für die Außerbetriebnahme von Betriebsstätten besteht eine interne Regelung der Bank. Darin wird jedoch nicht explizit angewiesen, nach dem Auszug zu kontrollieren, ob nichts vergessen wurde. Diese Selbstverständlichkeit muss allerdings auch nicht zwingend schriftlich fixiert werden. Mehrere Mitarbeiter der Filiale meinten sich jedenfalls zu erinnern, die Räume nach Abschluss des Umzuges begangen zu haben, um sicherzustellen, dass nichts zurückgeblieben war. Es existierte auch ein Übergabeprotokoll, in dem die Einbauschränke - im Zusammenhang mit der Zahlung eines Ablösebetrages für deren Entfernung durch den Vermieter - ausdrücklich erwähnt wurden. Dass gleichwohl offenbar etwas übersehen wurde, war nach Auffassung der Bank auf menschliches Versagen in Verbindung mit der Verkettung unglücklicher Umstände zurückzuführen.

Die Absicht der Bank, in die Formulierung für Übergabeprotokolle künftig einen Passus des Inhaltes aufzunehmen, dass die Räume vollständig leer übergeben wurden und/oder dass sich keine Bankunterlagen mehr in den Räumen befinden, wurde von der Aufsichtsbehörde ausdrücklich begrüßt. Ob sich entsprechende Vorkommnisse dadurch völlig ausschließen lassen, bleibt freilich zweifelhaft.

Die Rolle des Kunsthändlers konnte nicht eindeutig geklärt werden. Er übergab zunächst nur einen Teil der Unterlagen. Auf die Frage des Filialleiters, ob er noch weitere Unterlagen gefunden habe, antwortete er, nach Rücksprache mit seinem Rechtsanwalt werde er dazu keine Angaben machen. Die Bank schloss jedoch aus seinen Angaben gegenüber der Presse, dass sich weitere Unterlagen als die übergebenen in seinem Besitz befinden müssten.

In der Folge entstand ein Streit über die Herausgabe der restlichen Unterlagen.
Der Kunsthändler forderte die Abholung durch ein Mitglied des Vorstandes der Bank und behauptete, die Bank habe Übergabefristen verstreichen lassen. Die Bank wiederum behauptete, der Kunsthändler sei nie anwesend gewesen, wenn ein Mitarbeiter die fehlenden Unterlagen abholen wollte. Letztlich bestand bei der Bank verständlicherweise keine Bereitschaft, die Unterlagen durch ein Vorstandsmitglied persönlich abholen zu lassen – vor laufenden Fernsehkameras.

Die Aufsichtsbehörde wies den Kunsthändler darauf hin, dass er nicht berechtigt sei, die Daten länger zu behalten und Unbefugten zu zeigen.

Schließlich übergab der Kunsthändler die Unterlagen der Polizei, welche sie an die Bank zurückgab. Ein aufgrund des Strafantrages des Kunsthändlers eingeleitetes Ermittlungsverfahren gegen die Bank stellte die Staatsanwaltschaft ein.

5.2 Fund von Unterlagen mit personenbezogenen Daten auf einem öffentlichen Parkplatz

Ein Unternehmen der Presse wandte sich an die Aufsichtsbehörde und zeigte an, dass ihm ein Müllsack voller Unterlagen einer örtlichen Bankfiliale übergeben worden sei. Der Müllsack sei von einem Passanten auf einem öffentlichen Parkplatz gefunden worden.
Die Aufsichtsbehörde führte umgehend eine Überprüfung vor Ort durch. Sie stellte fest, dass es sich um Überweisungsträger, allgemeine Schreiben und diverse Bankformulare handelte, kurzum alle Unterlagen, die im Laufe von mehreren Monaten im Rahmen der Bankgeschäfte anfallen können und die aus verschiedenen Gründen zu vernichten gewesen wären. Eine Reihe dieser Unterlagen enthielten personenbezogene Daten, die aus Dateien stammten oder zur Eingabe in automatisierte Verfahren bestimmt gewesen waren.

Es konnte festgestellt werden, dass es sich ausschließlich um Materialien handelte, die zur Entsorgung vorgesehen waren.

Die betreffende Bank hat die Entsorgung von zu löschenden Datenträgern mit personenbezogenen Daten in Abstimmung mit ihrem betrieblichen Datenschutzbeauftragten geregelt. Das Material wird vom Reinigungspersonal aus den Papierkörben in Müllsäcke geschüttet und in einem nur für das Personal zugänglichen Raum aufbewahrt. Der Besitz eines Schlüssels zum Betreten der Filialräume ist dokumentiert. Ein Mitarbeiter ist für den Transport von den Filialen in die Hauptstelle zuständig. Der Transport findet unregelmäßig, je nach Anfall der zu vernichtenden Unterlagen, statt. In der Hauptstelle wird das Material der endgültigen Entsorgung zugeführt.

Die Bank beschäftigt bis hin zur Reinigungskraft nur eigenes Personal, welches auch - soweit erforderlich - nach § 5 BDSG auf das Datengeheimnis verpflichtet ist.

In die Räume der Filiale war nicht eingebrochen worden. Da die Unterlagen nicht auf einen Tag bzw. auf eine Entsorgungsperiode beschränkt waren, sondern aus einem längeren Zeitraum stammten, ließen sich die möglichen Ursachen für das Abhandenkommen der Unterlagen auch nicht auf einen Verlust auf dem Transportweg eingrenzen. Daher geriet zunächst jeder Mitarbeiter in Verdacht. Es konnte nur ein Mitarbeiter oder eine Mitarbeiterin über eine längere Periode diese Unterlagen von den übrigen zu entsorgenden Unterlagen getrennt, in den gefundenen Müllsack gesteckt und auf dem öffentlichen Parkplatz abgelegt haben.

Ein Beweis für diese Annahme konnte jedoch nicht gefunden werden. Die Ermittlungen ergaben lediglich, dass während der Periode, in der die Unterlagen gesammelt worden waren, eine Reinigungskraft als Aushilfe beschäftigt worden war. Nachweise über Unregelmäßigkeiten dieser Aushilfskraft ergaben sich aber nicht.

Die Bank reagierte umgehend auf die Vorkommnisse, indem sie versuchte, eventuelle Risiken zu vermindern: In jeder Filiale wurden Papiervernichter (Schredder) installiert, durch welche Unterlagen mit personenbezogenen Daten vor Ablage in den Müllsäcken zu schreddern sind. Dem betrieblichen Datenschutzbeauftragten wurde auferlegt, bei dem Einsatz von Aushilfskräften nicht nur eine formale Verpflichtung nach § 5 BDSG auf das Datengeheimnis vorzunehmen, sondern eine besondere Schulung über Maßnahmen zum Datenschutz und zur Datensicherheit, bezogen auf die Besonderheiten im Rahmen der Tätigkeit, durchzuführen.

5.3 Unsicherheiten von Kontoauszugsdruckern

In der Vergangenheit wurden bei Großbanken Probleme mit den Kontoauszugsdruckern bekannt. Es reichte aus, einen Kartenrohling im entsprechenden Kartenaufbau auf dem Magnetstreifen mit der Kontonummer und der Bankleitzahl zu versehen, und es konnten so der jeweilige Kontostand und gegebenenfalls auch neue Umsätze problemlos ausgedruckt werden.

Die Forderung, dass für eine Gültigkeitsprüfung einer Karte nicht nur die auf der Karte aufgedruckten Daten bzw. die auf jedem Geschäftsbrief ablesbaren Kontonummern und Bankleitzahlen verwendet werden, wurde von den Großbanken nach einer Übergangsphase zufriedenstellend umgesetzt. Auch bei den Volks- und Raiffeisenbanken sind insoweit Verbesserungen vorgenommen worden.

Entgegen ursprünglichen Angaben von Bankvertretern entsprechen diese Sicherungen den Maßnahmen der Großbanken. Die Verbindung zur zentralen Kontoführung ermöglicht es, dass eindeutige (nicht-öffentliche) Merkmale abgefragt werden können.
Die konzeptionellen Schwächen der Nutzung des Magnetstreifens sind erst mit der Umstellung auf Chipkarten zu beseitigen. Die Übergangsphase bringt nur begrenzte Risiken, da im Missbrauchsfall der Kontoauszugsdruck gesperrt werden kann. Missbräuche wurden im vergangenen Jahr nicht gemeldet.
Abschließend sei angemerkt, dass bei der Darstellung dieses Sachverhaltes aus Sicherheitsgründen darauf verzichtet werden musste, darzulegen, wer welche Sicherheitsmerkmale abfragt; eine Anleitung zum Missbrauch von Kontoauszugsdruckern sollte nicht gegeben werden.

5.4 Anschriftenübermittlung an einen gewalttätigen Ehegatten

Im Zusammenhang mit dem Schutz des informationellen Selbstbestimmungsrechts wird die Aufsichtsbehörde mit allen Lebensbereichen konfrontiert.

In einem Fall war eine Frau ihrem gewalttätigen Ehemann nur durch den Wohnungswechsel an eine für ihn unbekannte Adresse entkommen.

Noch aus der Ehezeit des mittlerweile geschiedenen Paares bestand ein Darlehensvertrag mit beiden Ehegatten als Darlehensnehmer. Auf Betreiben der Ehefrau übernahm diese mit einem Pfandtausch auf ein neues Objekt den gesamten Darlehensvertrag, und der Ehemann wurde aus seinen Verpflichtungen entlassen.

Nachdem die Bonitätsprüfung der Ehefrau als zukünftige alleinige Vertragspartnerin abgeschlossen war, teilte die Bank dem Ehemann mit, dass er nun aus der persönlichen Schuldhaft für das Darlehen entlassen würde, allerdings unter der Bedingung, dass die Ehefrau als alleinige Eigentümerin im Grundbuch eingetragen werde.
Im Betreff nannte die Bank die Anschrift des neuen Beleihungsobjektes, welches dem Ehemann bis dahin unbekannt war.

Das neue Sicherungsobjekt war aber zugleich auch der Wohnort der Betroffenen, und sie sah sich nun unkalkulierbaren Risiken ausgesetzt.

Die Frage, ob die Bank unzulässigerweise Informationen an ihren früheren Schuldner gegeben hatte, musste verneint werden, weil bei einem Pfandtausch - dem zunächst beide Vertragspartner zustimmen müssen - nicht davon ausgegangen werden kann, dass ein Vertragspartner von dem neuen Pfandobjekt nichts erfahren soll. Im konkreten Fall hatten die Ehepartner auch anfangs in gemeinsamer Korrespondenz die Bank darüber informiert, dass sie einen Austausch des Pfandobjektes erwägen, sodass die Bank keinerlei Anhaltspunkte für ein Geheimhaltungsbedürfnis hatte. Es gab deshalb keine Gesichtspunkte, die für ein datenschutzrechtlich zu beanstandendes Verhalten der Bank sprachen.

Den Betroffenen kann nur empfohlen werden, die Bank auf die besonderen persönlichen Umstände hinzuweisen und gemeinsam eine Lösung zu erarbeiten, die zu einer Vermeidung von unerwünschten Datenübermittlungen führt.

Die Banken nehmen in der Mehrzahl ihre Verantwortung hinsichtlich der Vertraulichkeit ihrer Daten ernst, besondere Probleme bei bestehenden Einzelverträgen und den Vertragsparteien untereinander sind für sie jedoch - ohne besondere Hinweise - nicht berücksichtigungsfähig.

5.5 Falsche Erfassung von neuen Depotdaten

Eine Bankkundin erhielt beim erstmaligen Kauf von Fondsanteilen eine Depotänderungsmitteilung, die auch Adressdaten eines ihr unbekannten Mannes enthielt.
Eine Depotänderung konnte nicht vorliegen, da die Kundin erstmals überhaupt ein Depot eröffnete und mit dem Mann in keinerlei Verbindung stand.

Es stellte sich heraus, dass ein Kunde ausgeschieden war. Statt dessen Depot zu löschen, wurde es mit einer Änderung der betroffenen Bankkundin zugeordnet. Da diese Änderung nur teilweise vollzogen wurde, enthielt das Bankdepot nunmehr Daten des früheren Kunden und der neuen Kundin.

Datenschutzrechtlich war zu beanstanden, dass durch die falsche (wahrscheinlich bequemere) Arbeitsweise Daten über Geschäftsbeziehungen eines früheren Kunden an die neue Kundin mit der Depotänderungsmitteilung übermittelt wurden.

Die betreffende Bank räumte ein, dass bei einer Einhaltung der vorgeschriebenen Arbeitsweise (Löschung von Depots als vollständige Löschung und Neuanlage von Depots als völlige Neueingabe) der geschilderte Fehler nicht aufgetreten wäre.

Änderungen von Depots dürfen nur eingegeben werden, wenn es sich tatsächlich um die Änderung einer bestehenden Geschäftsbeziehung handelt.

Der dargestellte Bearbeitungsfehler war auf menschliches Versagen im Einzelfall zurückzuführen. Eine Änderung der Arbeitsweise war nicht möglich, da die entsprechenden Transaktionen (Löschung, Änderung, Neuanlage) grundsätzlich benötigt werden. Die Bank hat in einer schriftlichen Anweisung die Mitarbeiter und Mitarbeiterinnen darauf hingewiesen, dass je nach Geschäftsfall die Transaktionen eindeutig zuzuordnen sind. Da bei derartigen Ereignissen auch der Imageverlust einer Bank erheblich ist, ist davon auszugehen, dass zumindest zukünftig sorgfältiger gearbeitet wird.

5.6 Fehlerträchtige Bedienung von Textverarbeitungsprogrammen

Die Nutzung moderner Textverarbeitungsprogramme bietet viele Vorteile und vereinfacht die Abläufe im Büroalltag. Das automatisierte Einfügen von Adressfeldern und der Eindruck personenbezogener Daten in den Text und die Kopfzeilen von Folgeseiten sind gerngenutzte Funktionen dieser Standard-Bürosoftware.

In einer südhessischen Bankfiliale machte man es sich allerdings zu leicht: Bei jedem neuen Individual-Anschreiben an Kunden wurde als in dem Programm voreingestellter Standard einfach der zuvor für einen anderen Kunden in einem anderen Zusammenhang erstellte Brief aufgerufen und je nach Sachverhalt entsprechend abgeändert bzw. ergänzt und ausgedruckt. Ein Petent, der in einem Schreiben des Institutes den Namen und die Anschrift eines ihm unbekannten weiteren Bankkunden eingedruckt fand, wies die Aufsichtsbehörde auf diese fehlerträchtige Bedienungsvariante hin. Die Datenschutzaufsichtsbehörde beanstandete den aufgetretenen Fehler, bei dem unzulässig personenbezogene Daten von Bankkunden übermittelt wurden und hat die Bank aufgefordert, das Textverarbeitungssystem so zu konfigurieren, dass bei der Neuerstellung eines Schreibens von vornherein keine fremden Kundendaten aus anderen Schreiben und Zusammenhängen in die Textverarbeitung geladen werden, sondern - wie allgemein üblich - ein Briefkopf mit leeren Eingabefeldern benutzt wird.

6. Schufa

6.1 Vortäuschen eines berechtigten Interesses

Ein privater Vermieter war zugleich Gesellschafter eines Inkasso- und Leasing-Unternehmens, welches bei der Schufa einen Vertrag als Leasing-Unternehmen hatte. Über einen vermeintlichen (unter Umständen auch tatsächlichen) Mietschuldner holte sich das Unternehmen bei der Schufa eine Auskunft, obwohl unstrittig kein Leasingvertrag existierte.

Der verantwortliche Geschäftsführer vertrat die Auffassung, dass die ausstehende Mietforderung ihn berechtigte, über seinen Schuldner Auskünfte einzuholen.

Die Schufa gibt jedoch Vermietern keinerlei Auskünfte über deren Mieter. Der bestehende Schufa-Vertrag des Anfragenden als Leasing-Unternehmen wurde missbräuchlich genutzt, um die gewünschten Auskünfte zu erlangen.

Während Vermieter nach derzeitiger Rechtslage bei Mietrückständen keine Schufa-Auskünfte erhalten, können sie bei Kreditauskunfteien Auskünfte erhalten. Mit solchen Auskünften wollte sich der Verantwortliche des Unternehmens nicht begnügen, da die Schufa-Auskünfte für seine Zwecke geeigneter seien.

Dass das Erschleichen von Auskünften ein Straftatbestand ist, der mit Freiheitsstrafe geahndet werden kann, war dem Verantwortlichen angeblich nicht bewusst. Der betroffene Mieter hat Strafantrag gestellt, und es bleibt abzuwarten, wie der Fall gerichtlich entschieden wird.

Die Datenschutzaufsicht konnte in diesem Zusammenhang nur fordern, dass derartige Abfragen zukünftig unterbleiben müssen. Da die Schufa mittlerweile den Vertrag mit dem Verantwortlichen gekündigt hat, sind weitere Missbräuche ausgeschlossen.

6.2 Personenverwechslung bei häufigen Namen

Die Schufa verwertet auch die Adressdaten der Deutschen Post Adress GmbH (Adressen aus den Nachsendeaufträgen der Deutschen Post AG). Angaben zu Geburtsort und Geburtsdatum werden von der Deutschen Post Adress GmbH in der Regel nicht erfasst und sind somit in den übermittelten Daten nicht enthalten.

Aus diesem Datenbestand erhielt innerhalb eines Postleitzahlenbereichs ein Herr Schmidt eine neue Adresse, obwohl nicht er, sondern ein Namensvetter mit dem gleichen Vornamen umgezogen war. Dieser Namensvetter war noch gar nicht in den Schufa-Bestand aufgenommen worden, und er erhielt wegen der vermeintlichen Identität plötzlich eine Kreditkündigung und die Aufforderung, seine Einkaufskarte zurückzusenden. Der Namensvetter bekam zumindest eine Vorstellung von den finanziellen Problemen des Unbekannten gleichen Namens.

Beim Abgleich der Geburtsdaten stellte sich sehr schnell heraus, dass es sich um zwei unterschiedliche Personen handelte.

Bei der Schufa muss ein Mitarbeiter in solchen Einzelfällen durch persönliches Eingreifen die Adressen zuordnen; dies ist hier offensichtlich fehlerhaft geschehen. Es wäre allenfalls vertretbar gewesen, an die Schufaanschlusspartner eine Meldung zu senden, in der gefragt wird, ob Personenidentität vorliegt.

Es ist zwar jeder Einzelfall zu prüfen, aber die Fehlerwahrscheinlichkeit steigt bei häufigen Namen zwangsläufig. In der Vergangenheit gab es sogar schon den Fall, dass jemand mit gleichem Vornamen, Namen, Geburtsort und Geburtstag negative Daten bei der Schufa erhielt, die einer anderen Person mit sehr schlechtem Finanzgebaren zuzuordnen waren. Nach der Klarstellung hat sich die Bank des solventen Kunden hierzu Vermerke mit weiteren Unterscheidungsmerkmalen angefertigt.

Betroffenen mit ähnlichen Namensproblemen kann allgemein nur empfohlen werden, vor der Beantragung eines Kredits eine Eigenauskunft bei der Schufa einzuholen.

6.3 Erledigter Negativsaldo wurde gemeldet

Eine Volksbank hat nach über zwei Jahren einen Negativsaldo einer Betroffenen an die Schufa gemeldet, obwohl dieser bereits ausgeglichen war. Diese Meldung führte zu einer Datenspeicherung bei der Schufa, und so entstand eine Beeinträchtigung des Kreditrufes der Betroffenen.

Eine Überprüfung ergab, dass die Meldung keinesfalls hätte erfolgen dürfen. Die Löschung der Negativdaten wurde bei der Schufa kurzfristig vollzogen.

Dies Beispiel illustriert, dass die Schufa zwar über die allgemein besten Datenbestände verfügt, in Einzelfällen jedoch immer wieder Fehler auftreten (können).

Die Qualität der Schufa-Daten steht und fällt mit der Sorgfalt der einmeldenden Unternehmen. Mit dem zunehmenden Automatisierungsgrad ist die Fehlerhäufigkeit insgesamt rückläufig.

6.4 Eintragung einer Bürgschaft ohne Einwilligung

Ein Betroffener hatte in größerem Umfang gebürgt, gegenüber der Bank des Hauptschuldners jedoch keine Schufa-Klausel unterschrieben. Er war auch kein Kunde bei dieser Bank. Nach einiger Zeit wurde er aus der Bürgschaft in Anspruch genommen, und die Bank meldete den Sachverhalt der Schufa.

Aufgrund der Datenspeicherung entstand der fälschliche Eindruck, der Betroffene habe sich leichtfertig überschuldet und könne nun seinen Verbindlichkeiten nicht nachkommen.

Obwohl die Forderung der Bank unstrittig war, bestand jedoch keine Rechtsgrundlage für die Weitergabe der Forderungsdaten (aus der Bürgschaft) an die Schufa.

Die Daten wurden daraufhin bei der Schufa gelöscht. Mit dem wiederhergestellten Kreditruf hatte der Betroffene Aussichten, seinen selbstständigen Tätigkeiten unter besseren Voraussetzungen nachzugehen.

7. Auskunfteien

7.1 Bonitätsauskunft an eine falsche Fax-Nummer

Der Faxversand von Auskünften hat zwar den Vorzug der Schnelligkeit, es treten dafür jedoch andere Risiken auf als beim Postversand.
Dem unverschlüsselten Fax ist nicht anzusehen, ob es auf seinem Weg zum Empfänger unbefugt gelesen bzw. kopiert wurde. Zwangsläufig erreichte die Aufsichtsbehörde insoweit noch keine einzige Beschwerde.
Bekannt werden dafür Faxe, die versehentlich an den falschen Empfänger gesendet werden. Beim Versand eines Faxes sollte vor dem Bedienen der Starttaste immer noch einmal die eingegebene Faxnummer verglichen werden.

Eine Auskunftei versuchte, diesen möglichen manuellen Fehlern im Einzelfall dadurch vorzubeugen, dass sie im Computer die Faxnummern der Kunden speichert. Wünscht der Kunde eine Auskunft, wird der Auftrag mit der Kundennummer abgewickelt, und bei der Erledigung per Fax werden Name, Anschrift und Faxnummer des Kunden automatisch hinzugefügt. Der Sachbearbeiter sieht auf dem Bildschirm diese Daten und kann im Bedarfsfall korrigierend eingreifen. Versehentlich wurde der in einem Fall bei der Anlage des Kundenstammsatzes eine falsche Faxnummer des Kunden eingegeben. Diese falsche Faxnummer war rein zufällig die Faxnummer der Redaktion einer überregionalen Boulevardzeitung. Bedingt durch diesen Eingabefehler erhielt die Zeitungsredaktion eine vertrauliche Auskunft per Fax, die eigentlich für einen Kunden der Auskunftei bestimmt war. Die Zeitungsredaktion nutzte die Gelegenheit für einen Artikel zum Thema Datenschutz. Nachträglich wurde der Auskunftei zugesichert, dass das falsch adressierte Fax mit seinen vertraulichen Daten vernichtet wurde. Die Zeitungsredaktion hat sich insoweit korrekt verhalten.

Bei der Auskunftei stellte sich heraus, dass bei der Eingabe des Kundenstammsatzes eine Kontrollerfassung offensichtlich nicht stattgefunden hatte. Die falsch eingegebene Faxnummer führte zu der geschilderten ungewollten Datenübermittlung und hätte ohne Reaktion der Zeitung auch noch weitere Fehlleitungen verursachen können.

Als Ergebnis konnte hierzu nur festgestellt werden, dass eine Kontrollerfassung unverzichtbar ist und derartige Fehler (relativ) sicher verhindern kann. Leider wird aus Kostengründen in der Wirtschaft verstärkt auf die Kontrollerfassung verzichtet.

7.2 Alle Auskunftsangaben bis auf die Adresse sind falsch

Die Qualität der Auskünfte hängt von der Qualität der recherchierten und auf Datenspeicher eingegebenen Daten ab.
Bei der Dateneingabe findet in der Regel eine Kontrollerfassung nicht mehr statt. Diese Vorgehensweise ist vor allem bei der Eingabe von Zahlen riskant, weil hier am ehesten Fehler entstehen können.

Beschwerden gibt es jedoch fast ausschließlich wegen schlecht (oder überhaupt nicht) durchgeführter Recherchen.
In einem krassen Einzelfall waren die Daten über einen Einzelhandelsunternehmer - bis auf die Adresse - vollständig falsch. Schutzwürdige Belange des Betroffenen wurden durch die Datenübermittlung an die Kunden der Auskunftei massiv beeinträchtigt.

Gegenüber dem Rechercheur wurden personelle Maßnahmen veranlasst.
Derartigen Missständen lässt sich nur vorbeugen, indem mit einer arbeitsteiligen Vorgehensweise Kontrollen eingebaut werden. Im geschilderten Fall hatten die Kontrollmechanismen offensichtlich versagt. Wenn der Rechercheur völlig selbstständig - quasi als freier Mitarbeiter allein tätig ist - sind Kontrollen nur unter erschwerten Bedingungen durchführbar.

7.3 Speicherung der eidesstattlichen Versicherung eines Geschäftsführers

In mehreren Fällen beschwerten sich Geschäftsführerinnen/Geschäftsführer darüber, dass in der Auskunft über das von ihnen geleitete Unternehmen die von ihnen geleistete private eidesstattliche Versicherung erwähnt wurde.

Bei der Prüfung der Einzelfälle wurde immer festgestellt, dass die Geschäftsführer alleinvertretungsberechtigt waren und somit über einen sehr großen Einfluss verfügten. In einem Fall war zusätzlich die Ehefrau die alleinige Gesellschafterin, sodass von einer sehr starken Durchdringung privater und geschäftlicher finanzieller Probleme ausgegangen werden musste.

In den geprüften Fällen war es für den Kreditruf der Unternehmen von Bedeutung, ob die Geschäftsführer eidesstattliche Versicherungen abgegeben hatten.
Die alleinvertretungsberechtigten Geschäftsführer haben mit der eidesstattlichen Versicherung dokumentiert, dass sie im privaten Bereich in finanziellen Dingen nicht mit der erforderlichen Sorgfalt vorgegangen sind und auch nicht in der Lage waren, die Situation aus eigenen Kräften zu bereinigen. Wenn die privaten Schulden vollständig bezahlt werden, kann eine Löschung der Eintragung beim Amtsgericht beantragt werden und die Auskunfteien müssen diese Löschung dann nachvollziehen.

Solange ein Geschäftsführer jedoch privat überschuldet ist, stellt er vor allem mit seiner Alleinvertretungsvollmacht ein so großes Risiko für das von ihm geleitete Unternehmen dar, dass seine schutzwürdigen Belange zurückstehen müssen.

Eine Geschäftsführerin fragte, wie sie geschäftlich überhaupt wieder erfolgreich sein und ihre Schulden zurückbezahlen könne, wenn sie wegen des schlechten Kreditrufes Geschäfte verliere. So bedauerlich die Auswirkungen in diesem Einzelfall waren, wurde keine Möglichkeit gesehen, von der ursprünglichen Bewertung abzugehen.

7.4 Mangelnde Sorgfalt bei Auskunfteien - Immer wieder Kuvertierungsfehler

Bei mehreren Auskunfteien und Inkasso-Services kam es im Berichtsjahr durch menschliches Versagen zur unzulässigen Offenbarung personenbezogener Angaben aus dem Bereich der Kredit- und Bonitätsdaten.

Der Aufsichtsbehörde wurde unter anderem von einem Beschwerdeführer ein Schreiben vorgelegt, mit dem ihm eine Wirtschaftsauskunftei einen gerichtlichen Vollstreckungsbescheid inklusive Kopie der entsprechenden Postzustellungsurkunde einer ihm unbekannten dritten Person mit anderem Namen und Anschrift zugesandt hatte.

Ein Inkasso-Büro fügte einem Mahnschreiben an einen Schuldner auch gleich die Mahnungen und Forderungsaufstellungen für zwei weitere fremde Schuldner bei.

In beiden Fällen wurden durch das Regierungspräsidium fehlende oder unzureichende Kontrollen bei der manuellen Kuvertierung festgestellt und beanstandet. Die Unternehmen haben daraufhin ihre Arbeitsabläufe in geeigneter Weise umgestaltet und zusätzliche Kontrollmaßnahmen beim Postversand eingeführt.

8. Versicherungen

8.1 Neuordnung eines Versicherungskonzerns

Eine große Versicherungs-Unternehmensgruppe stellte ihre Planungen für ihre neue Konzernstruktur sowie die beabsichtigten Neufassungen der datenschutzrechtlichen Einwilligungsklausel und der Schweigepflichtentbindungsklausel nebst zugehöriger Merkblätter für Kunden und Nichtkunden vor und bat die Aufsichtsbehörde um Stellungnahme.
Ziel der neuen Konzernstruktur ist eine Organisation der Versicherungsgesellschaften nach Geschäftsstrukturen über die Grenzen der jeweiligen Einzelgesellschaft als Rechtsträger hinaus.

Zwischen den Gesellschaften der Unternehmensgruppe wurden ein Rahmenvertrag sowie Einzelverträge über Funktionsausgliederungen und die Erbringung von Dienstleistungen geschlossen.

Nach Auffassung der Aufsichtsbehörde handelt es sich dabei - bis auf eine mögliche Ausnahme - nicht um Auftragsdatenverarbeitung, sondern um Funktionsübertragungen, da der Funktionsübernehmer eigenverantwortlich Entscheidungen zu treffen hat, die für das übertragende Unternehmen verbindlich sind. Im Rahmenvertrag war ausdrücklich geregelt, dass das übertragende Unternehmen (= Leistungsempfänger im Sinne des Dienstleistungsvertrages) kein Weisungsrecht gegenüber dem Unternehmen hat, welches die Funktion übernimmt (= Leistungserbringer im Rahmen des Dienstleistungsvertrages).

In dem Entwurf des Versicherungskonzerns für ein neues Datenverarbeitungsmerkblatt waren die geplanten neuen Strukturen im Wesentlichen dargestellt.
Die vorgelegte Einwilligungsklausel enthielt gegenüber der vom Gesamtverband der Deutschen Versicherungswirtschaft mit den obersten Aufsichtsbehörden abgestimmten "Musterklausel" die Ergänzung, dass Daten auch "zur Erfüllung administrativer konzerninterner Aufgaben" übermittelt werden sowie einen entsprechenden Verweis auf das Merkblatt.

Die Bewertung durch die Aufsichtsbehörde führte zu folgendem Ergebnis:

Die geplante Struktur bringt es mit sich, dass auch besondere Antrags-, Vertrags- und Leistungsdaten konzernintern ausgetauscht werden.
Darin liegt ein wesentlicher Unterschied zur bereits erwähnten "Mustereinwilligungsklausel":
Diese sieht grundsätzlich nur die Übermittlung allgemeiner Antrags-, Vertrags- und Leistungsdaten vor. Besondere Antrags-, Vertrags- und Leistungsdaten dürfen nur an Rückversicherer oder andere Versicherer zwecks Abklärung des Risikos übermittelt werden, nicht aber konzernintern.

Gleichwohl ist die Abweichung damit nicht unzulässig.

Zu beachten ist, dass Einwilligungen nicht unbedingt erforderlich sind, wenn bereits aus der Vertragsgestaltung deutlich wird, welches Unternehmen welche Aufgaben übernimmt.
Die Einbeziehung in die Datenschutz-Einwilligungsklausel ist aber durchaus sinnvoll. Allerdings ist die oben genannte Formulierung zu pauschal. Hier sollte eine etwas konkretere Formulierung gewählt werden, beispielsweise, dass die Daten, die sich aus den Antragsunterlagen oder der Vertragsdurchführung ergeben, zum Zwecke der zentralisierten Vertragsverwaltung und Leistungsbearbeitung (oder: Bestandsverwaltung/Vertragserfüllung), wie im

Merkblatt dargestellt, an Unternehmen der Versicherungsgruppe übermittelt werden.

Im Falle von Lebens-, Kranken- und Unfallversicherungen müssen Schweigepflichtentbindungserklärungen eingeholt werden.
Lehnt ein Versicherungsnehmer die Unterzeichnung der Einwilligungsklausel ab und ist das Unternehmen der Auffassung, auch ohne Einwilligung die Übermittlung vornehmen zu können, muss der Versicherungsnehmer hierauf hingewiesen werden, damit er die Wahl hat, ein anderes Unternehmen einzuschalten.

Die Übermittlungen dürfen also keinesfalls "hinter dem Rücken" des Betroffenen erfolgen, d.h. dieser muss dann die Entscheidung haben, ob er unter diesen Umständen überhaupt am Vertrag festhalten will.

Bei Änderung der im Merkblatt aufgeführten Strukturen ist (zumindest) eine Benachrichtigung des Versicherungsnehmers erforderlich.

Die Aufsichtsbehörde legte außerdem Wert darauf, dass die Schutzrechte des Betroffenen angesichts der neu in Aussicht genommenen Strukturen nicht beeinträchtigt werden.

Daher muss außerdem sichergestellt werden, dass der Betroffene seine ihm nach dem BDSG zustehenden Rechte (insbesondere § 34 BDSG und § 35 BDSG) auch bei dem Unternehmen gelten machen kann, mit dem er den Versicherungsvertrag abgeschlossen hat.

8.2 Unzulässiges Verfahren zur Identitätsprüfung bei Adressänderung

Großes Erstaunen sowohl bei dem Beschwerdeführer als auch bei der Aufsichtsbehörde verursachte die Methode eines Versicherungsunternehmens, die vermutete Anschriftenänderung eines Versicherungsnehmers zu verifizieren.

Dem Petenten aus Süddeutschland wurde eine Beitragsrechnung für eine Rechtsschutzversicherung zugesandt, obwohl er nicht bei der Gesellschaft versichert war. Das Unternehmen, bei dem ein gleichnamiger Kunde aus Norddeutschland versichert war, ging aus nicht mehr nachvollziehbarem Anlass offensichtlich davon aus, dass der Kunde zwischenzeitlich umgezogen sei. Nachdem der Rechnungsempfänger gegen die Zahlungsaufforderung protestierte und darauf hinwies, dass er nie einen Versicherungsvertrag unterschrieben habe, wurde ihm der Einfachheit halber kurzerhand eine Kopie des kompletten Versicherungsvertrages seines Namensvetters aus Norddeutschland mit allen persönlichen Angaben dieser Person als angeblicher Nachweis für sein bestehendes Versicherungsverhältnis zugesandt.

Dieses Verfahren zur Identitätsprüfung, bei dem personenbezogene Daten eines Versicherungsnehmers unzulässig an eine dritte Person übermittelt wurden, hat die Aufsichtsbehörde beanstandet und das Unternehmen darauf hingewiesen, dass bei ungesicherter Identität eine komplette Offenlegung der Vertragsdaten eines Kunden wohl kaum das geeignete Mittel zur Prüfung einer Anschriftenänderung sein kann.

9. Neue Medien (TDG, TDDSG, MDStV)

9.1 Identitäts- und Altersprüfung, pseudonyme Nutzung, Verwendung von Daten zu Werbezwecken

a) Ein Internet-Provider gewährt seinen Kunden nur dann den vollen Zugang zum Internet und das Recht, e-Mails und Newsartikel zu schreiben, sowie eine eigene Homepage anzulegen, wenn sie eine Fotokopie des Personalausweises übersenden.
Wer dies nicht tut bzw. wer unter 18 Jahren alt ist, kann nur im deutschen Teil des Internets surfen (nicht im globalen Internet) und News etc. lesen, aber nicht schreiben.

Gegen die Forderung nach Vorlage des Personalausweises richteten sich mehrere Eingaben von (potenziellen) Kunden, die nach der Zulässigkeit dieses Vorgehens fragten.

Dies betrifft zunächst die grundsätzliche Frage der anonymen oder pseudonymen Nutzungsmöglichkeit.

Wie bereits im letzten Tätigkeitsbericht (unter Kapitel 10.1) ausgeführt, sieht die Aufsichtsbehörde jedenfalls derzeit keinen Grund zur Beanstandung, wenn der Internet-Provider keine völlige Anonymität (d.h. auch im Verhältnis zum Provider) des Teilnehmers gewährleistet.
Eine pseudonyme Nutzungsmöglichkeit der angebotenen Dienste reicht aus.
Hier war vor allem zu bedenken, dass der Kunde mit der Zuweisung der Schreibberechtigung jederzeit selbst zum Anbieter werden kann, sodass ihn gegebenenfalls sogar eine Impressumspflicht treffen kann (s. nachfolgend 9.2).

Der Provider rechtfertigte seine Forderung nach Vorlage einer Personalausweiskopie damit, dass er sich selbst vor der Gefahr strafrechtlicher Verfolgung wegen etwaiger rechtswidriger Inhalte schützen wolle. Er verwies dabei auf die Compuserve-Entscheidung.
In diesem Zusammenhang habe er ein Interesse an einer Identitätsüberprüfung der Kunden als potenzielle Anbieter, aber auch an einer Altersfeststellung der Kunden als Nutzer (von Jugendlichen unter 18 Jahren werde das Einverständnis der Erziehungsberechtigten verlangt).

Vor diesem Hintergrund hat die Aufsichtsbehörde die Forderung nach Vorlage einer Ausweiskopie nicht beanstandet.

Es stellte sich jedoch des Weiteren die Frage, ob die weitere Verwendung der Kopien zulässig ist. Die Prüfung ergab, dass die Kopien gescannt werden und nach einer kurzen Plausibilitätsprüfung der Angaben im Antrag auf Schreibberechtigung als pixelorientiertes Bild mit einer Indexnummer auf ein WORM-Medium gebrannt werden.
Die Personalausweisnummer wird nicht verarbeitet, ein Datenfeld ist nicht vorgesehen. Das DV-Verfahren bietet nicht die Möglichkeit einer Selektion mittels Personalausweisnummer.
Die Ausweiskopien werden in einem abgeschlossenen Stahlbehälter gesammelt und dann datenschutzgerecht vernichtet.

Im Hinblick auf das Personalausweisgesetz, wonach die Seriennummer nicht so verwendet werden darf, dass mit ihrer Hilfe ein Abruf personenbezogener Daten aus Dateien oder eine Verknüpfung von Dateien möglich ist, wurde das Vorgehen als akzeptabel bewertet, da diese Gefahr hier nicht besteht.

Jedoch wurde bezüglich des Erforderlichkeitsgrundsatzes um Prüfung gebeten, ob eine Beschränkung der Erfassung auf das unbedingt erforderliche Minimum erfolgen kann.

Ein etwaiger Einsatz anderer Verarbeitungssysteme wurde als unzulässig bewertet. Die Personalausweisnummer darf nicht in die Bestandsdatenbank übernommen werden.

b) Das Unternehmen hatte dargelegt, dass durch die automatisierte Zuweisung einer Teilnehmerkennung, unter welcher die Nutzung von Diensten erfolgen kann, die Möglichkeit einer pseudonymen Nutzung gewährleistet sei.

Allerdings bietet das Unternehmen jedem Teilnehmer (mit Schreibberechtigung) folgenden Service an:

"... Wenn Sie einen Teilnehmer [desselben Unternehmens] ansprechen wollen, können Sie seine Benutzernummer herausfinden und wenn Sie eine Mail eines Teilnehmers [desselben Unternehmens] empfangen, seinen Namen nachschlagen ....".

Wenngleich davon auszugehen ist, dass die meisten Teilnehmer großes Interesse an einem solchen Service haben dürften, muss doch beachtet

werden, dass nach dem Sinn und Zweck des § 4 Abs. 2 Teledienstedatenschutzgesetz (TDDSG) der Diensteanbieter seinen Kunden selbstverständlich auch im Verhältnis untereinander eine pseudonyme Inanspruchnahme seines Dienstes zu ermöglichen hat.
Um den gesetzlichen Anforderungen gerecht zu werden, muss daher jedem Teilnehmer die Möglichkeit gegeben werden, dass seine Daten nicht in dieser Nachschlagedatei aufgenommen werden. Eine entsprechende Information (beispielsweise in den Allgemeinen Geschäftsbedingungen) ist erforderlich.

Bei Abfassung dieses Berichtes hatte sich das Unternehmen hierzu noch nicht geäußert, sodass die Aufsichtsbehörde erneut mit dem Unternehmen in Verbindung treten wird.

c) Ein weiterer Gegenstand der Beschwerden gegen das Unternehmen war die Nutzung der Teilnehmerdaten zu Werbezwecken.

Angesichts bestimmter Formulierungen in den Allgemeinen Geschäftsbedingungen und im Teilnehmerantrag entstand bei den Betroffen der Eindruck, ihre Bestands- und Nutzungsdaten würden personenbezogen an Dritte übermittelt.
Die entsprechenden Formulierungen stehen im Widerspruch zu anderen Bestimmungen, wonach nur eine anonyme Nutzung zu Werbezwecken bzw. zum Zwecke der Angebotsoptimierung erfolgen solle.

Tatsächlich werden, wie die Überprüfung durch die Aufsichtsbehörde ergab, Nutzerdaten ausschließlich anonymisiert zur Erstellung statistischer Media-Daten genutzt, welche an die Partnerfirmen, deren Angebote der Provider auf seinem System bereithält, übermittelt werden:
Die Alters-, Geschlechts-, Postleitzahlen- und Berufsgruppenanteile der Nutzer werden ermittelt und dem Anbieter mitgeteilt.

Hiergegen bestehen keine Bedenken.

Da die Geschäftsbedingungen widersprüchlich oder zumindest äußerst missverständlich sind, wurde das Unternehmen aufgefordert, eine klarstellende Neuregelung zu treffen.

Für den Fall, dass künftig doch eine personenbezogene Nutzung und Übermittlung der Daten zu Werbezwecken beabsichtigt sei – diese Erwägung wollte das Unternehmen nicht völlig ausschließen – wies die Aufsichtsbehörde darauf hin, dass die in der derzeitigen Fassung des Schreibantrages enthaltene "Einverständniserklärung" völlig unzureichend sei. Gemäß den §§ 3 Abs. 1, 4 Abs. 4, 5 Abs. 2 und 7 Abs. 3 TDDSG wäre eine eindeutig formulierte Einwilligungserklärung erforderlich, welche die Anforderungen des § 3 Abs. 5 und 6, sowie gegebenenfalls des Abs. 7 TDDSG erfüllen müsste. Entsprechendes ist bei einer Einwilligung nach dem Mediendienstestaatsvertrag nach § 12 Abs. 3 MDStV zu fordern.

9.2 Impressumspflicht

Ein großer Service-Provider bietet seinen Kunden die Möglichkeit, eigene Homepages zu erstellen und veröffentlicht dann stets Name, Anschrift, Kundennummer und e-Mail-Adresse der betreffenden Homepage-Inhaber.

Hiergegen beschwerte sich einer der Kunden bei der Aufsichtsbehörde. Er verlangte, dass seine Homepage anonym erscheinen müsse.

Diese Forderung ist jedoch nicht gerechtfertigt. Eine Homepage stellt entweder einen Tele- oder einen Mediendienst dar.

Sie kann als Mediendienst im Sinne des Mediendienstestaatsvertrages (MDStV) bewertet werden, wenn die Absicht der Übermittlung eines Inhaltes an eine Vielzahl von Nutzern im Vordergrund steht (von Heyl, ZUM 1998, 115).
Für die Einstufung als Mediendienst ist es dabei unerheblich, ob es sich um ein kommerzielles oder ein privates Angebot handelt.

Mit der Erstellung einer Homepage ist der Kunde damit selbst zum Anbieter geworden.

Während dem Nutzer die Inanspruchnahme von Mediendiensten anonym oder unter Pseudonym zu ermöglichen ist, soweit dies technisch möglich und zumutbar ist (§ 13 Abs. 1 MDStV), kann der Anbieter der Dienste für sich selbst gerade keine Anonymität (oder Pseudonymität) beanspruchen.

Für Mediendienste gilt eine uneingeschränkte Impressumspflicht (Pflicht zur Anbietererkennung), d.h. der Anbieter muss Name und Anschrift angeben (§ 6 Abs. 1 MDStV).

Aber selbst wenn im konkreten Fall bei der Erstellung der Homepage nicht die Absicht der Inhaltsübermittlung an eine Vielzahl von Nutzern im Vordergrund stünde, sondern das Anknüpfen von Interaktion und Dialog mit einigen dazu bereiten Nutzern, und die Homepage danach nicht als Mediendienst zu bewerten wäre, ergäbe sich kein anderes Ergebnis:
Die Homepage wäre dann als Teledienst im Sinne des Teledienstegesetzes (TDG) und des Teledienstedatenschutzgesetzes (TDDSG) zu bewerten. Auch hierbei kommt es nicht darauf an, ob es sich um ein kommerzielles oder ein privates Angebot handelt.

Der Homepage-Inhaber wäre danach Teleddiensteanbieter. Für Teledienste besteht eine Impressumspflicht, soweit es sich um ein "geschäftsmäßiges" Angebot handelt (§ 6 TDG).
Eine Gewinnerzielungsabsicht oder eine Gewerbsmäßigkeit wird hierbei aber nicht vorausgesetzt. Ein geschäftsmäßiges Angebot liegt bereits vor, wenn eine gewisse Nachhaltigkeit, also Dauerhaftigkeit gegeben ist (Bundestagsdrucks. 13/7385, S. 21, Begründung zu § 6 TDG).
Bei Homepages dürfte diese Voraussetzung in aller Regel erfüllt sein. Daher wäre der Homepage-Inhaber auch nach dem Teledienstegesetz verpflichtet, seinen Namen und seine Anschrift anzugeben.

Folglich ist die vom Service-Provider vorgenommene automatische Veröffentlichung von Name und Anschrift ("Zwangsimpressum") keinesfalls zu beanstanden.

Bei der Kundennummer, welche der Service-Provider zusätzlich automatisch veröffentlicht, kann es sich nur bei Altkunden um die Telefonnummer handeln. Mittlerweile werden nur noch Kundennummern vergeben, die von der Telefonnummer unabhängig sind. Auch Altkunden haben jedoch die Möglichkeit, eine Kundennummer zu erhalten, die keinen Rückschluss auf die Telefonnummer zulässt.

Die Aufnahme der Kundennummer in das Zwangsimpressum war daher nicht zu beanstanden.

Bezüglich der zusätzlichen Veröffentlichung der e-Mail-Adresse findet eine weitere Abklärung mit dem Provider statt. Danach wird insoweit die abschließende Bewertung erfolgen.

9.3 Auskunftspflicht

Gegenstand kontroverser Diskussionen mit einem Provider war die Verpflichtung zur Auskunftserteilung an die Kunden bzw. die Frage der Entgeltlichkeit.

Der Provider hatte in einer "Ethikrichtlinie", auf die er in seinen Allgemeinen Geschäftsbedingungen Bezug nahm, geregelt, dass Auskünfte über die gespeicherten Daten (nur) gegen Erstattung der Kosten erteilt würden.

Als die Aufsichtsbehörde dies beanstandete, erklärte der Provider, dass eine Gebühr nur verlangt würde, wenn der Kunde darauf bestehe, eine schriftliche Auskunft (auf postalischem Wege) zu erhalten.

Zur Begründung verwies er darauf, dass gemäß der seiner Auffassung nach abschließenden Regelung des § 7 TDDSG der Diensteanbieter nicht verpflichtet sei, dem Nutzer die Auskunft in jeder vom Nutzer gewählten Form unentgeltlich zu gewähren. Nach § 7 TDDSG könne der Nutzer die Daten

entweder "beim Diensteanbieter", also in dessen Geschäftsräumen, "einsehen" (und dort gegebenenfalls einen Ausdruck verlangen) oder eine Auskunft in elektronischer Form erhalten.
Verlange der Nutzer die Auskunft in einer anderen Form, könne der Diensteanbieter entstehende Kosten ersetzt verlangen.

Die Aufsichtsbehörde vermochte sich dieser Argumentation nicht anzuschließen:

Aus § 1 Abs. 2 TDDSG ergibt sich, dass das BDSG subsidiär gilt, soweit das TDDSG keine abschließende Sonderregelung trifft (und dass es dabei nicht auf den Dateibegriff ankommt).
§ 7 TDDSG enthält insoweit aber gerade keine abschließende Spezialregelung.
Nach der Gesetzesbegründung stellt § 7 TDDSG "sicher, dass der Nutzer über das nach dem BDSG geltende Auskunftsrecht hinaus die über ihn oder sein Pseudonym gespeicherten Daten elektronisch einsehen kann" (Bundestagsdrucks. 13/7385, S. 25). Dies bedeutet, dass eine dem Medium entsprechende Erweiterung des Auskunftsrechts hinsichtlich der Modalität der Auskunft statuiert wurde. Damit wurde im Interesse der Betroffenen eine Erleichterung geschaffen.

Es würde aber diesem Zweck zuwiderlaufen, wenn man die Rechte des Betroffenen auf diese Auskunftsform und die Einsichtnahme am Ort des Unternehmens beschränken würde: Im Hinblick auf die nicht ohne weiteres gewährleistete Vertraulichkeit bei der elektronischen Datenübermittlung ist die elektronische Auskunftserteilung nicht immer ein adäquater Ersatz für eine schriftliche Beauskunftung. Würde man ausschließlich ein Recht auf elektronische Auskunftserteilung anerkennen, würde man damit die Rechte des Betroffenen beschränken, statt sie zu erweitern.

Soweit und solange bei der elektronischen Auskunftserteilung keine automatische Verschlüsselung erfolgt, hat der Betroffene ein Recht auf schriftliche Auskunftserteilung nach § 34 Abs. 3 BDSG, da die elektronische Auskunftserteilung nicht als angemessene andere Form i.S.d. § 34 Abs. 3, 2. Halbsatz BDSG gewertet werden kann.

Die Unentgeltlichkeit ergibt sich aus § 34 Abs. 5 Satz 1 BDSG. Unentgeltlich bedeutet hier, dass auch keine Auslagen in Rechnung gestellt werden dürfen (Umkehrschluss aus § 34 Abs. 5 Satz 3 BDSG).

Die Aufsichtsbehörde verlangte daher, die "Ethikrichtlinie" entsprechend zu ändern bzw. die fragliche Regelung zu streichen.
Der Provider hat sich hierzu noch nicht abschließend geäußert. Er versicherte jedoch, entsprechenden Bitten um schriftliche Auskunftserteilung bis auf weiteres nachzukommen, ohne Kostenerstattung zu verlangen.
Auch wenn damit faktisch kein großes Problem bestehen dürfte, sollte die Ethikrichtlinie geändert werden, um eine insoweit möglicherweise "abschreckende" Wirkung auf Betroffene zu vermeiden.

Bei einer etwaigen Novellierung des TDDSG sollte eine klarstellende Formulierung in § 7 TDDSG erfolgen.

9.4 Unsicherer Versand von Zugangsdaten

Ein Online-Dienst verschickte an seine Kunden die geheimen Anmelde- bzw. Zugangsdaten (Teilnehmerkennung und Passwort) in unzureichend gesicherten perforierten Faltbriefen (ohne Briefumschlag). Mit Hilfe einer starken Lampe konnte man die Zugangsdaten lesen, ohne den Brief zu beschädigen.

Die Gefahr, dass die Daten auf diese Weise tatsächlich von Unbefugten gelesen würden, war aber für Neu- und Altkunden unterschiedlich:

Neukunden erhalten regelmäßig eine unternehmenseigene Zeitschrift. In der transparenten Zeitschriftenhülle ist der Brief, der die Kennung enthält, so eingeschweißt, dass durch den Postzustelldienst lediglich ein kleines Fenster geöffnet werden kann, um den Barcode entnehmen zu können, der beweist, dass das Schriftstück per eigenhändigem Einschreiben zugestellt wurde. Ein

Entnehmen des Umschlages, der die Kennung enthält, wäre somit nur möglich gewesen, wenn ein Postbediensteter den verschweißten Plastikumschlag beschädigt hätte. Dies hätte der Empfänger dann erkennen können.

An Altkunden, die nur eine neue Kennung beantragen, wurden die Briefe allerdings ohne die Zeitschrift versandt. Bei diesem Teil der Kunden wäre es möglich gewesen, dass ein Postbediensteter die Daten hätte lesen können, ohne dass die Betroffenen dies erfahren hätten. Eine Kenntnisnahme durch andere Personen war relativ unwahrscheinlich, da die Briefe immer als eigenhändiges Einschreiben mit Rückschein versendet werden.

Das Unternehmen hat den Missstand mittlerweile abgestellt, indem es die Schreiben für eine kurze Übergangszeit zunächst mit einem dunkelgrauen Raster hinterlegt und sodann mit einem völlig schwarzen Hintergrund versehen hat, sodass ein Durchleuchten keine Informationen mehr offenbart. Die Aufsichtsbehörde hat sich hiervon überzeugt.

Zu begrüßen ist, dass das Unternehmen in den Schreiben an die Kunden nun auch empfiehlt, sofort bei der erstmaligen Benutzung des Online-Dienstes das Passwort aus Sicherheitsgründen zu ändern. Kommt der Kunde dieser Aufforderung nach, dann wäre es für jemanden, dem es gelänge, trotz der neuen Sicherheitsvorkehrungen bei der Herstellung der Briefe die Kennung und das Passwort herauszufinden, nicht mehr möglich, zu Lasten des Kunden auf dessen Account zuzugreifen.

9.5 Unsichere Seiten im World Wide Web

Der Datenverarbeitungsdienstleister einer Bank hatte im World Wide Web im Auftrag der Bank ein Preisausschreiben angeboten. Neben dem Preisausschreiben konnte auch Informationsmaterial angefordert werden. Bedingt durch einen technischen Fehler war die gesamte Verzeichnisstruktur des Dienstleisters und damit auch die Datei mit den Mitteilungen der Preisausschreibenteilnehmer (unter anderem Name, Adresse, Geburtsdatum, Telefonnummer, Kreditkartennummer, Kontonummer) einsehbar. Der Fehler war nach einer Stunde festgestellt worden, wer sich jedoch die Verzeichnisstruktur notiert hatte, konnte in aller Ruhe die gespeicherten Daten über 24 Stunden lesen. Der Dienstleister wurde darauf hingewiesen, dass der Zeitraum des möglichen freien Zugriffs zu lang gewesen ist. Fehler im Einzelfall werden sich nie ganz vermeiden lassen, die Folgen müssen dann aber minimiert werden.
Es wurde entgegengehalten, dass die Teilnehmer auf die Risiken der Datenübermittlung im Internet ausführlich hingewiesen wurden. Im Fehlerfall war jedoch nicht die Datenübermittlung, sondern die Datenspeicherung beim Dienstleister das Risiko. Speziell mit der unbefugten Nutzung der Liste der Kreditkartennummern und Namen hätte beträchtlicher Schaden entstehen können.

Inzwischen kann davon ausgegangen werden, dass zumindest bei diesem Dienstleister das gleiche Problem so schnell nicht wieder entstehen wird.

9.6 Vortäuschung einer fehlgeleiteten e-Mail

Ein Beschwerdeführer hatte eine e-Mail erhalten, in der ein Mann einem Freund (illegale) Ratschläge zur hochverzinslichen Geldanlage auf Nummernkonten gab. Der Beschwerdeführer kannte weder den Verfasser und Absender der e-Mail, noch dessen Freund, also den eigentlichen Adressaten der e-Mail. Die anfänglichen Fragen darüber, wie die e-Mail zu einem völlig falschen Adressaten gelangte, klärten sich sehr schnell auf. Der vermeintliche Irrläufer war offensichtlich als Werbemaßnahme gezielt versandt worden.
Ein datenschutzrechtliches Problem bestand somit nicht.

Allerdings wären bei der Nutzung des Geldanlage-Angebots wahrscheinlich (Steuer-)Straftatbestände erfüllt gewesen. Einen Gewinn dürften diejenigen, welche auf das Angebot hereinfielen, trotzdem nicht erlangen, da ein Betrug des Anbieters wahrscheinlich ist.
Nach der Recherche bei den als Korrespondenzbanken betroffenen deutschen Banken hat die Aufsichtsbehörde ihre Tätigkeit eingestellt, da es nicht ihre

Aufgabe ist, Steuer- und Betrugstatbestände aufzuklären. Es ist jedoch davon auszugehen, dass die auf ihren guten Ruf bedachten deutschen Banken entsprechende Hinweise an die Strafverfolgungsbehörden gegeben haben.

10. Aspekte internationaler Datenverarbeitungen

10.1 Auslandsdatenverarbeitung bei einem Kreditkartenunternehmen

Soweit international agierende Unternehmen oder Unternehmensgruppen in mehreren Unterzeichnerstaaten der EG-Datenschutz-Richtlinie tätig sind, sind sie mit der gegenwärtigen Situation konfrontiert, dass die Richtlinie in einigen Staaten umgesetzt ist und in anderen nicht.
Aber auch in den Staaten, in denen sie noch nicht formell umgesetzt ist, muss sie bei der Auslegung bestehender Datenschutzgesetze berücksichtigt werden.

Diese Situation hat ein Kreditkartenunternehmen bewogen, in Abstimmung mit der Aufsichtsbehörde konkrete Maßnahmen zur Umsetzung der Richtlinie zu ergreifen.

Kernpunkt der Überlegungen war dabei die zentrale Datenverarbeitung bei der amerikanischen Muttergesellschaft in den USA.

Nach der EG-Richtlinie kommt es bei der Beurteilung der Zulässigkeit der Datenübermittlung auf die Angemessenheit des dortigen Datenschutzniveaus an. Dies ist auch bei den "schutzwürdigen Belangen der Betroffenen" nach § 28 Abs. 1 Nr. 2 BDSG von Relevanz.

Hierbei muss das Unternehmen selbst (gewissermaßen im Wege einer Bringschuld) die Aufsichtsbehörde über die im Zielland relevanten Datenverarbeitungsgrundlagen informieren.

Da dies für das Unternehmen aber sehr schwierig erschien bzw. es wohl davon ausging, dass die Annahme eines angemessenen Datenschutzniveaus zweifelhaft bleiben würde, hat es davon abgesehen, die geforderten Informationen zu erbringen und hat sich von vornherein dafür entschieden, durch vertragliche Regelungen im Sinne des Art. 26 Abs. 2 EU-Richtlinie etwaige Datenschutzdefizite in den USA zu kompensieren (soweit dies durch privatrechtliche Regelungen überhaupt möglich ist).

Inhaltlich sind an derartige Verträge im Wesentlichen die gleichen Maßstäbe anzulegen, wie sie auch für die Beurteilung der Angemessenheit des Datenschutzniveaus des betreffenden Staates gelten.

Daher müssen folgende inhaltliche Grundsätze beachtet bzw. umgesetzt werden:

- Grundsatz der Beschränkung auf die Zweckbestimmung
- Grundsatz der Datenqualität und -verhältnismäßigkeit
- Grundsatz der Transparenz
- Grundsatz der Sicherheit
- Recht auf Zugriff, Berichtigung, Löschung und Widerspruch
- Beschränkungen der Weiterübermittlung in andere Drittländer

Für spezifische Arten der Verarbeitung - wie bei sensiblen Daten, beim Direktmarketing und bei automatisierter Einzelentscheidung - gelten besondere Anforderungen.

Darüber hinaus müssen "verfahrensrechtliche" bzw. der Durchsetzung der inhaltlichen Grundsätze dienende Regelungen getroffen werden.

Das Unternehmen legte einen entsprechenden Vertragsentwurf vor, der jedoch noch überarbeitet werden wird.

Da die deutsche Niederlassung nur eine unselbstständige Zweigstelle der amerikanischen Muttergesellschaft ist und die Kreditkartenverträge namens der englischen Tochtergesellschaft geschlossen werden (nach deutschem

Recht), sind Vertragspartner des vorgelegten Vertragsentwurfs die englische Gesellschaft und die amerikanische Muttergesellschaft.
Es ist beabsichtigt, den Vertrag als Rahmenvertrag zu gestalten, dem sich alle Partner- und Tochterunternehmen unterwerfen oder beitreten, sodass die darin festgelegten Datenschutzstandards letztlich weltweit für alle Datenverarbeitungen in der Unternehmensgruppe gelten.

10.2 Internationale Verarbeitung von Kunden- und Mitarbeiterdaten

Eine weltweit tätige Unternehmensgruppe, zu deren Geschäftsgegenstand unter anderem Auftragsdatenverarbeitungen gehören, beabsichtigte, die Verarbeitung personenbezogener Daten von Mitarbeitern und von Kunden bzw. von Personen, deren Daten im Auftrag der Kunden verarbeitet werden, durch einen Vertrag zwischen allen Unternehmen der Gruppe zu regeln. Außerdem sollte eine entsprechende, aber etwas konkreter gefasste Verfahrensvorschrift für alle Mitarbeiter ("code of conduct") erlassen werden.

Die Unternehmensgruppe beabsichtigte ferner, die bestehende, aber sehr allgemein gefasste Konzernbetriebsvereinbarung zum Austausch von Mitarbeiterdaten im Hinblick auf den geplanten Vertragsabschluss, zu kündigen.

Dem Datenschutzbeauftragten eines hier ansässigen Unternehmens der Gruppe, welcher die Aufsichtsbehörde um eine Bewertung des beabsichtigten Vorgehens bat, konnte mitgeteilt werden, dass der Vertragsabschluss grundsätzlich zu begrüßen sei, da er die relevanten Bestimmungen der EG-Richtlinie beinhaltete und dieser somit innerhalb des Konzerns Geltung verschaffte. Auch die Verfahrensvorschrift mit den Erläuterungen und praktischen Beispielen war zu begrüßen.

In einem Punkt musste aber auf ein mögliches Missverständnis der EG-Richtlinie hingewiesen werden:

Der Vertragsentwurf konnte so interpretiert werden, dass die Übermittlung von Mitarbeiterdaten an Externe oder andere der Gruppe angehörige Unternehmen zu Werbezwecken ohne weiteres zulässig sei, dass der betroffene Mitarbeiter aber - entsprechend Art. 14 der EG-Richtlinie - ein Widerspruchsrecht habe.
Hier vertrat die Aufsichtsbehörde die Auffassung, dass Art. 14 der EG-Richtlinie ebenso wie § 28 Abs. 3 BDSG nicht isoliert gesehen werden darf, sondern dass zuvor eine Prüfung zu erfolgen hat, ob die Übermittlung gemäß Art. 7 EG-Richtlinie (vgl. § 28 Abs. 1 und 2 BDSG) zulässig ist. Nach der Prüfpraxis der Aufsichtsbehörde aber kommt § 28 Abs. 1 (u. 2) BDSG nicht als Erlaubnistatbestand in Betracht, soweit es um die Übermittlung von Mitarbeiterdaten für Werbezwecke geht, vielmehr kann dies nur auf der Grundlage einer Einwilligung erfolgen.
Auf ein Widerspruchsrecht kommt es daher nicht an.

Die Aufsichtsbehörde wies außerdem darauf hin, dass der Vertrag eine (Konzern-)Betriebsvereinbarung nicht ersetzen kann, da das Betriebsverfassungsgesetz und etwaige sich daraus ergebende Mitbestimmungsrechte gesondert zu beachten sind.

10.3 Einwilligung nach italienischem Datenschutzrecht

Das zur Umsetzung der EG-Datenschutzrichtlinie erlassene italienische Datenschutzgesetz zeigt Auswirkungen auch auf bestehende Vertragsbeziehungen mit deutschen Unternehmen.

So legte die italienische Handelsvertretung eines deutschen Unternehmens dem deutschen Unternehmen nun Informationen über die Datenverarbeitung vor, insbesondere über den Zweck der Datenverarbeitung, die Kategorien von Empfängern der Daten, die für die Datenverarbeitung zuständige und die verantwortliche Person sowie über die Rechte der Betroffenen.
Dabei ging es zum einen um die Personaldaten des deutschen Unternehmens, zum anderen um "die persönlichen Daten der Firma".

Unter Bezugnahme auf diese Informationen und das italienische Datenschutzgesetz bat das italienische Unternehmen das deutsche Unternehmen

darum, eine "Zustimmungserklärung" zu einer entsprechenden Datenverarbeitung zu unterzeichnen.
Dem italienischen Unternehmen lagen schon seit langem Daten über Mitarbeiter des deutschen Unternehmens vor, soweit diese für die Abwicklung der Vertragsbeziehung erforderlich waren (Namen, Aufgabenbereich und betriebliche Telefonnummern der Ansprechpartner im deutschen Unternehmen). Es ging offensichtlich darum, die bisherige Praxis formal in Einklang mit der neuen Rechtslage zu bringen.
Der Datenschutzbeauftragte des betroffenen deutschen Unternehmens bat die Aufsichtsbehörde um Stellungnahme, ob Bedenken gegen die Unterzeichnung der Zustimmungserklärung bestünden.

Soweit sich die Zustimmungserklärung auf die "persönlichen Daten der Firma" bezog, waren keine datenschutzrechtlichen Belange i.S.d. BDSG tangiert, sondern nur der Schutz von Betriebsgeheimnissen, denn bei dem Unternehmen handelte es sich um eine juristische Person.

Dass diese Daten gleichwohl in die Klausel einbezogen waren, erklärt sich daraus, dass sich der Regelungsgegenstand des italienischen Datenschutzgesetzes grundsätzlich auch auf Daten juristischer Personen erstreckt.

Eine weitere Besonderheit ist, dass im Allgemeinen Einwilligungen eingeholt werden müssen, was im konkreten Fall auch geschehen sollte. Bezüglich der Mitarbeiterdaten durften die Vertreter des Unternehmens die Zustimmung nur abgeben, soweit sich die Datenverarbeitung im Rahmen des § 28 BDSG hält. Für Datenverarbeitungen, die nach deutschem Recht der Einwilligung der betroffenen Mitarbeiter bedürfen, hätte folglich auch deren Einwilligung eingeholt werden müssen.

Es bestand zwar im konkreten Fall kein Anhaltspunkt dafür, dass eine solche Notwendigkeit bestanden hätte, zur Vermeidung etwaiger Missverständnisse wurde dem Datenschutzbeauftragten aber gleichwohl geraten, in die Zustimmungserklärung eine eindeutige Begrenzung auf die nach § 28 BDSG abgedeckten Verarbeitungszwecke einzufügen.

10.4 Kontaktadressen aller Passagiere für Notfälle

In den USA wurde 1998 ein neues Gesetz erlassen, welches die Fluggesellschaften verpflichtet, für den Fall von Flugzeugunglücken Kontaktadressen der US-Bürger zu erheben, die sich auf Flügen in die oder von den USA befinden. Die Fluggesellschaften werden von dieser Verpflichtung nur befreit, wenn nationale Gesetze diese Datenerhebung und -verarbeitung verbieten und die Fluggesellschaften ein Dokument vorlegen können, das dies bestätigt.
Ein etwaiger Konflikt mit nationalen Gesetzen musste vor dem 1. Oktober 1998 angezeigt werden. Spätere Einwände bleiben nach dem Gesetz unbeachtet.

Der Bevollmächtigte einer Fluggesellschaft bat daher die Aufsichtsbehörde kurz vor Fristablauf um eine datenschutzrechtliche Stellungnahme zu dem Gesetz.

Diese kam zu folgender Bewertung:
Die Datenerhebung und -verarbeitung kann nur zulässig sein, wenn die Datenerhebung ausschließlich beim betroffenen Passagier erfolgt und die Freiwilligkeit der Angaben gewährleistet ist.
Der nahe liegende Verwendungszweck, die Information der Kontaktperson nach einem Flugzeugunglück aus humanitären Gründen, rechtfertigt es nicht, die Daten hinter dem Rücken der Passagiere zu erheben (beispielsweise indem aus älteren Passagierlisten die Daten der Begleitpersonen entnommen würden) oder gegen deren freien Willen.
Andernfalls würde die Datenerhebung gegen Treu und Glauben (§ 28 Abs. 1 Satz 2 BDSG) verstoßen bzw. es würde an einer Rechtsgrundlage für die Datenspeicherung und Übermittlung fehlen, da weder eine Einwilligung noch ein berechtigtes Interesse i.S.d. § 28 Abs. 1 Nr. 2 bzw. Abs. 2 Nr. 1a DSG vorhanden wäre.

Soweit es den Schutz der Kontaktperson selbst betrifft, besteht bei dem genannten Verwendungszweck kein Erfordernis, auch diese Person um ihr

Einverständnis zu fragen. Bei einer Krankenhausaufnahme etwa sieht das Aufnahmeformular vor, dass der Patient freiwillig Angaben zu einer Kontaktperson machen kann, die im Notfall zu informieren wäre. Dass die angegebene Person selbst nicht um ihre Zustimmung gebeten wird, ist im Hinblick auf den Verwendungszweck nicht zu beanstanden.
Die Situation ist im Grundsatz vergleichbar, sodass die gleiche Beurteilung erfolgen muss.
Da bestimmten Passagen des vorgelegten Gesetzes zu entnehmen ist, dass die Datenerhebung wohl unmittelbar beim Passagier erfolgen sollte und die Angaben freiwillig seien, bestanden also insoweit zunächst keine Bedenken gegen das Gesetz.

Besonders problematisch aber erschien der im Gesetz enthaltene Vorbehalt für andere Behörden oder Regierungen, die Daten anzufordern und zu nutzen. Primär waren die Daten für das Transportministerium bestimmt. Dieser Vorbehalt für andere Stellen ist vor allem bedenklich, weil nach dem Gesetzestext unklar bleibt, ob diese Stellen schon vor einem Unglücksfall Zugriff auf die Daten haben sollen. Nicht geregelt ist auch, ob und wann die Daten gelöscht werden.
Da hier keine genaueren Informationen vorliegen, war insoweit eine abschließende Bewertung nicht möglich.

Andererseits ist in dem Gesetz ausdrücklich "die Information der US-Regierung im Falle eines Unglücks" als Gesetzeszweck festgelegt. Daher wäre eine Datenübermittlung zu einem vorherigen Zeitpunkt nicht gerechtfertigt und mit den Interessen der Betroffenen auch nicht zu vereinbaren.

Wenn aber eine Datenübermittlung tatsächlich erst im Unglücksfall erfolgt, ist die Gefahr, dass die erhobenen Daten von anderen Behörden zu ganz anderen Zwecken, die den Interessen der Betroffenen zuwiderlaufen, genutzt werden könnten, vermindert.

Die IATA hatte folgende Vorgehensweise zur Umsetzung des Gesetzes empfohlen:

Die US-Passagiere erhalten einen Handzettel (Vordruck) und werden gebeten, diesen auszufüllen (mit den Angaben zur Kontaktperson) oder unausgefüllt in einen Behälter zu werfen. Dieser bleibt - verschlossen - bei der Fluggesellschaft. Nur im Falle eines Unglücks werden die Angaben übermittelt.
Damit wäre sichergestellt, dass die oben genannten datenschutzrechtlichen Anforderungen (Freiwilligkeit, keine Übermittlung vor einem Unglücksfall) erfüllt werden.
Unter der Voraussetzung, dass tatsächlich entsprechend verfahren wird, konnte die US-Regelung letztlich nicht beanstandet werden.

10.5 Auslandsdatenverarbeitung und Meldepflicht nach § 32 BDSG

Zum Betrieb eines weltweiten Servicenetzes verarbeitet ein internationaler Expressdienst- und Transportkonzern auf seinen zentralen DV-Systemen in den USA Millionen Transaktionen je Tag. Zur Erfüllung der Frachtverträge, aber auch zur effektiven Bearbeitung von Anfragen zur globalen Sendungsverfolgung werden auch von der in Südhessen ansässigen deutschen Konzerntochter täglich personenbezogene Daten zur Weiterverarbeitung an die amerikanische Konzernmutter übermittelt.

Im Rahmen der Prüfung dieser Verarbeitungen und Übermittlungen personenbezogener Daten in das außereuropäische Ausland auf die datenschutzrechtliche Konformität dieser Verfahren nach dem BDSG wurde die Aufsichtsbehörde von der deutschen Konzerntochter unter Vorlage entsprechender Unterlagen um datenschutzrechtliche Stellungnahme gebeten. Insbesondere wurde eine Beurteilung gewünscht, ob sich das amerikanische Mutter-Unternehmen nach § 32 Abs. 1 BDSG zum Register der meldepflichtigen Stellen anmelden muss. Ein ausformulierter Vorschlag mit Vereinbarungen zur Auftragsdatenverarbeitung im Sinne schriftlicher Weisungen nach § 11 BDSG wurde ebenfalls mit der Bitte um Prüfung eingereicht.

Die Aufsichtsbehörde hat das Unternehmen darauf hingewiesen, dass die fragliche Datenverarbeitung nicht im Geltungsbereich des BDSG stattfindet und schon von daher keine Meldepflicht des amerikanischen Mutter-

Unternehmens gegeben sein kann. Außerdem kann die amerikanische Konzernmutter nach § 3 Abs. 9 BDSG kein Auftragnehmer im datenschutzrechtlichen Sinne sein. Es liegt somit auch keine Auftragsdatenverarbeitung nach § 11 BDSG vor, sondern es handelt sich um eine Übermittlung personenbezogener Daten an Dritte nach § 3 Abs. 5 BDSG.

Die in dem eingereichten Vereinbarungsvorschlag enthaltenen ausführlichen Regelungen zur Sicherung der Rechte der betroffenen deutschen Kunden wurden dennoch ausdrücklich begrüßt. Sie sind wesentlich für die Kompensation etwaiger Datenschutzdefizite in den USA und damit auch für die Bewertung der Zulässigkeit der Übermittlung nach § 28 Abs. 1 Nr. 2 BDSG bzw., soweit die Übermittlung bereits auf § 28 Abs. 1 Nr. 1 BDSG gestützt werden konnte, für die Sicherstellung, dass die Daten nur im Rahmen des Vertragszweckes verarbeitet werden (s. bereits unter Kapitel 10.1).

11. Arbeitnehmerdatenschutz

11.1 Unzulässige Fragen an Bewerber

Die Rechtsprechung hat sich schon vielfach damit beschäftigt, welche Fragen an Arbeitsplatzbewerber gestellt werden dürfen. Leider werden diese Vorgaben nicht immer beachtet. Diese Erfahrung hat auch eine Frau gemacht, die sich um eine Tätigkeit bei einer Zeitarbeitsfirma beworben hatte. Der Personalfragebogen enthielt unter anderem die Frage nach dem Bestehen einer Schwangerschaft.

Nach der arbeitsgerichtlichen Rechtsprechung ist diese Frage jedoch nur zulässig, wenn ein befristetes Arbeitsverhältnis begründet werden soll und die Aufnahme der Tätigkeit während der Laufzeit des Vertrages gegen Schutzvorschriften des Mutterschutzgesetzes verstößt, sodass die Arbeitnehmerin während der Dauer des Arbeitsverhältnisses nicht arbeiten könnte (Westenberg, NJW 1995, S. 761 mit Nachweisen zur BAG und EuGH – Rechtsprechung; Palandt, Kommentar zum Bürgerlichen Gesetzbuch, 56. Aufl., Anm. 1 d zu § 123 BGB).

Diese Voraussetzungen waren nicht erfüllt, sodass eine Datenerhebung zwecks nachfolgender dateimäßiger Speicherung unzulässig gewesen wäre (§ 28 Abs. 1 Satz 2 BDSG).

Die Zeitarbeitsfirma verwies zwar darauf, dass sie ein besonderes Interesse daran habe, dass die Bewerberinnen für jede Tätigkeit einsetzbar seien, da zum Zeitpunkt der Einstellung oftmals nicht feststehe, welche konkrete Arbeit wahrzunehmen sei. Dies rechtfertigt jedoch keine Privilegierung von Zeitarbeitsfirmen. Vielmehr ist bei diesen die Gefahr eines erheblichen oder völligen Fehlschlagens der Einstellung aufgrund der vielfältigen Einsatzmöglichkeiten der Arbeitnehmerinnen gerade geringer. Die Frage nach einer Schwangerschaft wäre also nur zulässig, wenn aufgrund der eigenen Angaben der Bewerberin zur gewünschten Tätigkeit oder bei einer gezielten speziellen Ausschreibung einer Tätigkeit, die den Beschäftigungsverboten des Mutterschutzgesetzes unterliegt, nach den obigen Kriterien davon auszugehen ist, dass die Einstellung fehlschlagen würde.
Die Zeitarbeitsfirma hat die Frage letztlich aus dem Personalfragebogen herausgenommen.

Sie hat jedoch in einem separaten Informations- und Erhebungsbogen, der Fragen enthält, welche für die Abwicklung des Vertrages nach erfolgter Einstellung relevant sind (z.B. Kontonummer), folgenden Passus aufgenommen:

"Soweit Sie aufgrund zwingender gesetzlicher Bestimmungen, wie beispielsweise der §§ 3 und 4 Mutterschutzgesetz, für bestimmte Einsatzbereiche nicht in Frage kommen, bitten wir um ergänzenden Hinweis."

Dieser Zusatzbogen wird zwar bereits mit dem Personalfragebogen ausgehändigt, in der Überschrift wird jedoch darauf hingewiesen, dass Ausfüllung und Abgabe vor dem Zeitpunkt der Einstellung freiwillig seien. Vorausgesetzt, es wird auch tatsächlich entsprechend gehandhabt, das heißt, es wird

kein Zwang ausgeübt, kann dies nicht beanstandet werden. Sollten wider Erwarten Einstellungen unterbleiben, nur weil der Zusatzbogen nicht ausgefüllt wurde, wäre diese Handhabung zu beanstanden.

11.2 Umgang mit Daten aus der betrieblichen Telefondatenerfassung

Die private Nutzung betrieblicher Telefonanlagen und die Kontrolle der Einhaltung von betrieblichen Nutzungsvereinbarungen durch den Arbeitgeber führt regelmäßig zu Beschwerden und Anfragen der Betroffenen bei der Aufsichtsbehörde. Teilweise werden in diesen Fällen die Unternehmen und Arbeitgeber nicht benannt, da die Beschwerdeführer Nachteile im Betrieb befürchten, wenn die Aufsichtsbehörde bei dem Unternehmen vorstellig wird.

So schilderte im Berichtsjahr ein Arbeitnehmer, in dessen Betrieb die privaten Telefonate zu Abrechnungszwecken getrennt erfasst und ausgedruckt werden, dass sich die Geschäftsführung Listen aller geführten Privat- und Dienstgespräche mit vollständiger Zielnummer zu Kontrollzwecken vorlegen lässt. Weitere Ausdrucke werden in der Buchhaltung des Unternehmens und der Personalakte des Mitarbeiters abgelegt. Zusätzlich werden veraltete Ausdrucke in einem offenen Container deponiert oder als Büro-Schmierzettel benutzt.

Da eine Telefonanlage eine technische Einrichtung darstellt, die geeignet ist, Verhalten und Leistung der Arbeitnehmer zu überwachen, unterliegt sie der Mitbestimmung des Betriebsrates nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz. Eine harmonische Lösung dieser und ähnlicher Konflikte gelingt in der Regel mit dem Abschluss einer Betriebsvereinbarung zur Nutzung der betrieblichen Telefonanlage zwischen Arbeitgeber und Mitarbeitervertretung im Sinne des § 87 Betriebsverfassungsgesetz.

Der betriebliche Datenschutzbeauftragte des Unternehmens hat nach § 37 Abs. 1 Satz 1 BDSG die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz sicherzustellen. Eine Mitwirkung bei der Gestaltung einer geeigneten Betriebsvereinbarung im Sinne des Arbeitnehmerdatenschutzes gehört damit auch zu seinen Aufgaben. Dem Arbeitnehmer wurde vor diesem Hintergrund empfohlen, zusammen mit dem betrieblichen Datenschutzbeauftragten und der Mitarbeitervertretung im Unternehmen auf den Abschluss einer entsprechenden Vereinbarung zu drängen und dabei - insbesondere unter Beachtung der datenschutzrechtlichen Belange des Angerufenen - geeignete Regelungen (z.B. Kürzung der Zielrufnummer) festzuschreiben.

Die Ablage der veralteten Telefonausdrucke mit allen Daten sämtlicher geführter Gespräche in einem offenen Container oder deren Nutzung als Schmierzettel im Büro ist offensichtlich unzulässig. Falls es überhaupt erforderlich ist, die Datenträger aufzubewahren, sind angemessene technische und organisatorische Maßnahmen nach § 9 BDSG und der Anlage zu § 9 Abs. 1 BDSG notwendig, um Unbefugten den Zugriff auf vorhandene Informationen zu verwehren. Sollten die Daten nicht mehr erforderlich sein, sind sie entsprechend § 35 Abs. 2 BDSG zu löschen bzw. die Datenträger datenschutzgerecht zu entsorgen.

11.3 Offenbarung von Lohn- und Gehaltsdaten

In einem kleinen Gewerbebetrieb wurden die monatlichen Lohnabrechnungen des Personals regelmäßig offen und für alle Mitarbeiter einsehbar im Personalraum des Betriebes zum Heraussuchen auf den Tisch gelegt. Eine Beschäftigte fühlte sich durch dieses Verfahren in ihren schutzwürdigen Belangen beeinträchtigt und hatte sich schon mehrfach bei ihrem Arbeitgeber gegen diese Offenlegung der Gehaltsdaten gegenüber ihren Kolleginnen und Kollegen ausgesprochen. Der Betriebsinhaber ignorierte die Forderungen der Beschwerdeführerin, worauf diese sich an die Aufsichtsbehörde mit der Bitte um Unterstützung bei der Wahrung ihrer Rechte wandte.

Personaldaten sind vom Arbeitgeber grundsätzlich vertraulich zu behandeln. Eine Offenbarung der Personaldaten gegenüber unberechtigten Personen - dazu können auch Kolleginnen und Kollegen gehören - durch den Arbeitgeber ist unzulässig. Die Aufsichtsbehörde hat den Betriebsinhaber außerdem darauf hingewiesen, dass der Arbeitgeber neben der Beachtung des Gebotes

der Vertraulichkeit auch aufgrund seiner Fürsorgepflicht die ihm vorliegenden Personaldaten immer gemäß ihrer Zweckbestimmung behandeln muss. Gegebenenfalls müssen geeignete organisatorische Maßnahmen getroffen werden, die gewährleisten, dass personenbezogene Daten nicht unbefugten Dritten offenbart werden. Im vorliegenden Fall würde hier schon die unmittelbare Aushändigung oder die Hinterlegung der Gehaltsabrechnung im verschlossenen Briefumschlag genügen. Der Betriebsinhaber hat die Hinweise und Anregungen der Aufsichtsbehörde aufgenommen und zugesagt, den Anspruch seiner Beschäftigten auf sichere Aushändigung der Lohnabrechnungen künftig durch Übergabe in verschlossenem Umschlag zu beachten.

11.4 Datenschutz ist kein Täterschutz

Leider muss die Aufsichtsbehörde immer wieder feststellen, dass in manchen Fällen von Petenten versucht wird, datenschutzrechtliche Regelungen im eigenen - meist finanziellen - Interesse zu instrumentalisieren und mit falschen Behauptungen oder unvollständigen Angaben die Datenschutzaufsichtsbehörde zur Einleitung von Nachforschungen bei unliebsamen Geschäftspartnern oder auch Arbeitgebern zu veranlassen.

Beispielhaft sei hier nur die Eingabe eines aushilfsweise als Fahrer beschäftigten Arbeitnehmers genannt, der die Aufsichtsbehörde aufforderte, gegen ein Unternehmen vorzugehen, das seine Lohndaten aus diesem geringfügigen Beschäftigungsverhältnis unbefugt in eine zentrale Meldedatei bei einer ihm angeblich unbekannten Stelle übermitteln würde. Außerdem erhalte er von seinem Arbeitgeber entgegen § 34 BDSG keine Auskunft über die beim Arbeitgeber zu seiner Person gespeicherten Daten und die Empfänger der übermittelten Daten.

Die Nachforschungen der Aufsichtsbehörde bei dem Unternehmen ergaben allerdings ein vollkommen anderes Bild. Es zeigte sich, dass der Petent mit seiner Eingabe vor allem versuchte, die Rückforderung von Sozialleistungen durch das Arbeitsamt zu erschweren. Bei der angeblich unbefugten Datenübermittlung handelte es sich um eine zulässige Beantwortung einer Anfrage des zuständigen Arbeitsamtes durch das Unternehmen. Vom Arbeitsamt hatte der Beschwerdeführer für den fraglichen Zeitraum der geringfügigen Beschäftigung auch Leistungen nach dem Arbeitsförderungsgesetz bezogen, ohne dort seinen Nebenjob als Fahrer anzugeben. Das Arbeitsamt war auf diese Unregelmäßigkeit aufgrund einer Kontrollmitteilung der gesetzlich für Geringverdiener zuständigen Krankenkasse aufmerksam geworden, bei der geringfügige Beschäftigungsverhältnisse nach den Bestimmungen des Vierten Buches des Sozialgesetzbuches zu melden sind. Die Beantwortung der Anfrage des Arbeitsamtes durch das Unternehmen und damit die Übermittlung der genauen Lohndaten für den Zeitraum des Bezuges von Leistungen war somit durchaus zulässig, da die Datenübermittlung zur Erfüllung der gesetzlichen Aufgaben des Datenempfängers notwendig war.

Wie sich schließlich herausstellte, hatte der Petent auch nie nach § 34 BDSG bei seinem Arbeitgeber um Auskunft nach den gespeicherten und übermittelten Daten ersucht und daher von diesem auch keine Antwort erhalten. Der Petent hatte die Datenschutzbeschwerde offensichtlich nur flankierend zu einer laufenden arbeitsrechtlichen Auseinandersetzung um Lohnnachzahlungen eingereicht, in der Hoffnung, seinen Forderungen an seinen ehemaligen Arbeitgeber in einem Verfahren vor dem Arbeitsgericht Nachdruck verleihen zu können.

11.5 Datenübermittlung Lohnpfändungsbeschluss

Den pfändbaren Teil ihres Einkommens hatte eine Arbeitnehmerin an eine Bank A abgetreten.
Eine andere Bank B betrieb nun die Zwangsvollstreckung gegen die Arbeitnehmerin und erwirkte einen Pfändungsbeschluss über den pfändbaren Teil des Einkommens.
Der Arbeitgeber informierte die Bank B über die bereits erfolgte Abtretung an die Bank A.

Hierüber beschwerte sich die Arbeitnehmerin. Sie war der Auffassung, der Arbeitgeber habe die Bank B zwar über die Tatsache der Abtretung informieren dürfen, nicht aber darüber, an wen diese erfolgt war.
Zur Begründung erläuterte sie, sie habe mit der Bank A nach der Abtretung vereinbart, dass ein Teil der Forderung, deren Befriedigung die Abtretung dienen sollte, "aus anderen Quellen" beglichen werde, sodass die Bank A insoweit von der Abtretung keinen Gebrauch machen sollte. Die Arbeitnehmerin wünschte daher, dass der Arbeitgeber den abgetretenen Betrag nicht voll an die Bank A auszahle, sondern zum Teil, wie bisher, an sie selbst.
Gegenüber der Bank B sollte der Arbeitgeber nur erklären, dass der pfändbare Teil des Einkommens abgetreten sei.
Ob der Arbeitgeber bereits von der Sondervereinbarung mit der Bank A und dem Wunsch der Arbeitnehmerin, den abgetretenen Betrag nicht voll an die Bank A auszuzahlen, informiert war, blieb offen.

Die Arbeitnehmerin wurde jedenfalls von der Aufsichtsbehörde darauf hingewiesen, dass ihre Täuschungsabsichten gegenüber der Gläubigerbank B kein schutzwürdiges Interesse darstellen kann.

Aus § 840 Abs. 1 Nr. 2 und 3 ZPO ergibt sich eindeutig, dass der Gläubiger bei einer Lohnpfändung das Recht hat, vom Drittschuldner, also dem Arbeitgeber, zu erfahren, ob und welche Ansprüche andere Personen an die Forderung machen bzw. ob und wegen welcher Ansprüche die Forderung bereits für andere Gläubiger gepfändet wurde.
Der Arbeitgeber muss daher Name, Anschrift, Grund und Betrag der Forderung der Bank A angeben.
Wenn im konkreten Fall letztlich nur ein Teilbetrag des ursprünglich an die Bank A abgetretenen Betrages ausgezahlt werden sollte, musste auch dies, also die wahre Höhe der Forderung, mitgeteilt werden.

11.6 Private e-Mail-Nutzung im Betrieb

Das Internet wird von Mitarbeitern zunehmend nicht nur geschäftlich, sondern auch privat genutzt. Die private Nutzung des e-Mail-Dienstes ist in den meisten Betrieben nicht geregelt.
Wünschenswert ist eine mit dem Betriebsrat abgestimmte Regelung, vergleichbar den Vereinbarungen zur privaten Nutzung des dienstlichen Telefons.

Bei den zurzeit ungeklärten Verhältnissen in den Betrieben stellt sich die Frage, inwieweit der Arbeitgeber die eingehenden e-Mails kontrollieren darf.
Kontrollen in Einzelfällen sind sicher möglich, solange es sich nicht um eine zustimmungspflichtige Verhaltens- und Leistungskontrolle handelt.
Das Problem sind hierbei private e-Mails, vor allem, weil der Empfänger nicht immer beeinflussen kann, dass ihm derartige private e-Mails nicht an seine Arbeitsstelle gesandt werden.
Eine Lösung des vielfach noch nicht bewältigten Problems kann deshalb nur sein, dass entweder private e-Mails völlig untersagt werden oder dass für private e-Mails besondere betriebliche Regelungen getroffen werden (vgl. Tätigkeitsbericht für 1996, Kapitel 9.1).
Am besten lassen sich private e-Mails mit einer gesonderten Mailadresse abgrenzen. Die dort eingegangene Mail sollte dann ähnlich wie persönliche, vertrauliche Briefe einer betrieblichen Kontrolle entzogen sein.

12. Medizinischer Bereich: Patientendaten auf Alt-PC nicht gelöscht

Von einer Fernsehgesellschaft erhielt die Aufsichtsbehörde einen Hinweis zu einem Sachverhalt, der immer häufiger Anlass zu erheblichen Bedenken hinsichtlich der Verarbeitung besonders zu schützender Daten, in diesem Fall medizinische Daten, liefert. Der zugrunde liegende Tatbestand konnte durch sofortiges Tätigwerden der Aufsichtsbehörde vor Ort rasch und lückenlos aufgeklärt werden.

Dem Fernsehsender waren Patientendaten einer Arztpraxis und Daten von Familienmitgliedern der Ärztin übersandt worden. Diese überwiegend hochsensiblen personenbezogenen Daten befanden sich auf einer Festplatte. Die Herkunft dieser Festplatte ließ sich aufgrund der auf ihr gespeicherten Daten eindeutig bestimmen. Nun musste nur noch festgestellt werden, auf welchen

Wegen Festplatte und Daten in falsche Hände gelangt waren. Nach Aussage der Ärztin war der veraltete PC in der Entsorgungsstelle eines städtischen Bauhofes abgegeben worden. Vorher aber seien alle Daten mit den vom System und den Programmen dafür vorgesehenen Befehlen gelöscht worden. Familienmitglieder bestätigten die Aussagen der verantwortlichen Ärztin.

Der Weg der Entsorgung auf dem Bauhof ließ sich rasch nachvollziehen. Privatpersonen können ihren Elektronikschrott in einem dafür bestimmten Container entsorgen. Dieser Container wird von einem Recyclingunternehmen abgeholt. Beim Recyceln entnommene Festplatten, deren Verwendung noch möglich erscheint, werden in den Handel gebracht. Beschäftigt sich dann zufälligerweise eine technisch versierte Person mit einem derartigen gebrauchten Datenträger, ist das Lesen der Daten auf diesem Datenträger sehr leicht, wenn die Daten nicht oder unvollständig gelöscht wurden. So war es auch im konkreten Fall: Die Ärztin hatte lediglich einen "Delete"-Befehl eingegeben. Dies war völlig unzureichend, da die Daten zugänglich bleiben. (Welche Maßnahmen erforderlich gewesen wären, ist in Kapitel 20.2 ausführlich beschrieben. Insoweit wird auf die dortige Darstellung verwiesen.)

Es stellte sich zusätzlich heraus, dass die Person, welche die Daten dem Fernsehsender übergeben hatte, per Annoncen in Fachpublikationen nach gebrauchten Datenträgern (mit Dateninhalt) gesucht hatte, um diese gegen Entgelt unter Hinweis auf die gespeicherten Daten anzubieten.

Welche Gefahren sich durch derartige Fahrlässigkeit bei der Entsorgung von alten PCs ergeben können, lässt sich unschwer erahnen. Aber nicht nur der fahrlässige Umgang hinsichtlich des Löschens und der Entsorgung gab im vorliegenden Fall Anlass zur Kritik, sondern auch der Umgang mit dem Gerät überhaupt.

Die Ärztin, die hier gleichzeitig die verantwortliche Daten verarbeitende Stelle repräsentierte, hatte ihren Familienangehörigen die private Nutzung des Gerätes ermöglicht. Angesichts der geringen Kenntnisse der Ärztin über das Datenverarbeitungssystem ist unterstellbar, dass eine wirksame Absicherung der durch die ärztliche Schweigepflicht (§ 203 StGB) geschützten Daten ebenfalls nicht vorgelegen haben konnte.

Zwar wird die Bedienung und Nutzung von Computern immer einfacher, doch sollten Anwender, die diese Geräte zu beruflichen Zwecken nutzen, zumindest Grundkenntnisse besitzen, durch die sie in die Lage versetzt werden, ordnungsgemäß mit einem Computer und den darauf befindlichen Daten umzugehen.

13. Direktmarketing und Werbung

13.1 Bundesweite Haushaltsbefragung

Im letzten Tätigkeitsbericht wurde unter Kapitel 7.1 dargestellt, welche datenschutzrechtlichen Anforderungen an Haushaltsbefragungen zu stellen sind, wie sie von einem im Regierungsbezirk Darmstadt ansässigen Unternehmen durchgeführt wurden und werden.

Kennzeichen dieser Befragungen ist, dass sie der Beschaffung differenziert auswertbaren Adressmaterials dienen, mit dessen Hilfe potenzielle Verbraucher möglichst zielgenau beworben werden können.

Während die im Herbst 1997 durchgeführte Befragung datenschutzrechtliche Anforderungen - wie berichtet - nicht erfüllte, konnte die Aufsichtsbehörde aufgrund intensiver Auseinandersetzung mit dem Unternehmen erreichen, dass bei der im Herbst 1998 durchgeführten weiteren Befragung eine Verbesserung zu verzeichnen war:

Das Unternehmen setzte bei der Umfrage von 1998 zwei Varianten von Anschreiben ein.

Die Variante I enthielt eine verbesserte Aufklärung über die Verwendungszwecke. Der Begriff der "Werbung" wurde ausdrücklich genannt. Auch eine bildliche Darstellung (überfüllter Briefkasten etc.) wies darauf hin, dass es

um die zielgenaue Direktwerbung geht. Außerdem wurde unterschieden zwischen der Verarbeitung der Daten in anonymisierter Form für die empirische Marktforschungsanalyse und der Weitergabe der Daten für Direktmarketing und Werbung.

Die Variante II des Anschreibens hingegen blieb hinsichtlich der Transparenz des Verarbeitungszweckes (deutlich) hinter der Variante I zurück, war aber immer noch besser als das Anschreiben vom Herbst 1997.

Der Fragebogen selbst enthielt am Ende eine vorformulierte Einwilligungserklärung, um deren Unterzeichnung der Fragebogen-Ausfüller gebeten wurde.

Im Anschreiben wurde darauf Bezug genommen.

Außerdem hieß es, dass die Angaben in diesem Fragebogen verarbeitet und genutzt werden dürften, wobei die Weitergabe ausschließlich auf die Organisationen und Unternehmen beschränkt sei, die den erkennbaren Interessen und Wünschen der Betroffenen entgegenkommen würden.

Im Fragebogen wurde - bis auf eine Ausnahme - die frühere Differenzierung der Antworten zwischen der ausfüllenden Person und den "anderen Erwachsenen im Haushalt" aufgegeben.
Stattdessen bezogen sich die Fragen im Wesentlichen auf die ausfüllende Person oder den "Haushalt".

Mit diesen Änderungen wurden die datenschutzrechtlichen Hauptanforderungen

- klare Erkennbarkeit, dass die Angaben nicht nur anonym, sondern auch personenbezogen ausgewertet werden, insbesondere
- Erkennbarkeit der Verwendung für den Zweck der persönlich adressierten Werbung
- unterschriebene Einwilligung aller volljährigen bzw. einsichtsfähigen Erwachsenen

weitgehend erfüllt – soweit die Variante I des Anschreibens verwendet wurde.

Kritisch betrachtete die Aufsichtsbehörde die Fragen zu sonstigen Betroffenen bzw. die Möglichkeit von Rückschlüssen auf andere Haushaltsmitglieder.

Sie stellte folgende Mindestforderungen auf:

- Keine Herstellung des Namensbezuges.
- Verwertung nur im Lettershop- und Listbroking-Verfahren.
- Keine Übermittlung von Daten in der Weise, dass ein Rückschluss auf das Einkommen nicht befragter Haushaltsangehöriger möglich ist.
- Nur statistische Verwendung der Fragen zum Kreditkarteneinsatz "anderer Erwachsener im Haushalt".

Die Einwilligungserklärung ist so zu formulieren, dass die personenbezogene Verwendung für Werbezwecke explizit genannt wird.

Eine optimale Transparenz wäre gewährleistet, wenn dem Einzelnen am Ende des Fragebogens die Wahl zwischen:

1. Meine Angaben dürfen zu Werbezwecken genutzt werden

   und

2. Ich bitte um eine anonyme Auwertung

eröffnet werden würde.

Kurz nach der Durchführung der Umfrage vom Herbst 1998 wies das Landgericht Darmstadt die Klage eines Verbraucherschutzvereines gegen das Unternehmen ab.

Der Verbraucherschutzverein hatte - wie bereits im letzten Tätigkeitsbericht dargestellt -, unter Berufung auf das Gesetz gegen unlauteren Wettbewerb

beantragt, dem Unternehmen zu untersagen, derartige Befragungen ohne unterschriebene Einwilligung der Betroffenen durchzuführen und hatte sich damit der Kernforderung der Aufsichtsbehörde angeschlossen.
Das Gericht war hingegen der Auffassung, dass eine Einwilligung nicht erforderlich sei. Der Betroffene sei umfassend und wahrheitsgemäß informiert. Über die Berufung des Verbraucherschutzvereins ist noch nicht entschieden.

Ein baden-württembergisches Gericht hatte hingegen in einem ähnlichen Verfahren eine Einwilligung für erforderlich gehalten.

Vor Fertigstellung dieses Berichtes hat das hier ansässige Unternehmen eine weitere Befragung durchgeführt. Zwar war wieder eine Einwilligungserklärung enthalten, aber die Aufklärung im Anschreiben entsprach im Wesentlichen derjenigen vom Herbst 1997. Dies bedeutet wieder einen Rückschritt, der wohl auf der oben zitierten Urteilsbegründung beruht.

Für künftige Befragungen legte das Unternehmen aber bereits einen verbesserten Entwurf vor, sodass zu hoffen bleibt, dass künftig dauerhaft ein datenschutzgerechter Standard eingehalten wird.

13.2 Verfahren bei Widerspruch und Auskunftserteilung

Direktwerbemaßnahmen werden teilweise wie folgt abgewickelt:

Unternehmen (beispielsweise Versandhäuser), die über Adressbestände verfügen, welche sie im Rahmen der Datenverarbeitung für eigene Geschäftszwecke erworben haben, stellen diese Daten auch anderen Unternehmen zur Verfügung.
Dies geschieht dadurch, dass bei Anfrage durch das werbende Unternehmen einem dritten Unternehmen (Werbedienstleister) der Auftrag erteilt wird, den gewünschten Datenbestand mit den Datenbeständen anderer Unternehmen (Adresseigner) zu vermischen.
Dieser Datenbestand wird dann in die Werbung gegeben und verarbeitet. Dabei sind die Werbeschreiben so gestaltet, dass das werbende Unternehmen als Absender erscheint. Tatsächlich erhält es jedoch erst durch etwaige Rückantworten der Adressaten (Ausfüllen von Bestell- oder Anmeldeformularen etc.) Kenntnis von deren Daten.

Ein Betroffener, der sich über eine Werbemaßnahme beschwerte, musste die Erfahrung machen, dass es in solchen Konstellationen äußerst schwer ist, das Recht auf Auskunft und Widerspruch auszuüben:

Das Unternehmen, für das geworben wurde (im konkreten Fall eine Versicherung) sagte, es wisse nichts, da es keine Daten gespeichert habe. Der Werbedienstleister (im konkreten Fall ein Tochterunternehmen der Versicherung) verwies darauf, dass er gemäß Vertrag mit den Adresseignern keine Auskünfte geben dürfte.

Der Bevollmächtigte der Versicherung vertrat die Auffassung, dass

- das Unternehmen, für dessen Produkte geworben wurde (Versicherung), nicht zur Auskunft verpflichtet sei, da es nicht speichernde Stelle sei

  und

- der Werbedienstleister (selbstständiges Rechenzentrum der Versicherung) Auftragnehmer der Adresseigner i.S.d. § 11 BDSG sei.

  Als Auftragnehmer sei der Dienstleister bereits nach § 11 Abs. 1 Satz 2 BDSG nicht zur Auskunft verpflichtet; außerdem sei er - jedenfalls im konkreten Fall - aufgrund ausdrücklicher Weisungen der Auftraggeber, die Herkunft der Daten nicht bekannt zu geben, nach § 11 Abs. 3 Satz 1 BDSG gehindert, dem Betroffenen entsprechende Auskünfte zu geben.

Die Aufsichtsbehörde vertrat hingegen folgende Auffassung:

Auch wenn das werbende Unternehmen die Daten der Betroffenen nicht selbst speichert, muss es dafür sorgen, dass die Betroffenen ihren Auskunftsanspruch (in angemessener Zeit) verwirklichen können. Hierzu muss es sich entweder die Herkunftsangaben beschaffen oder seine Vertragspartner vertraglich verpflichten, Auskunftsansprüche der Betroffenen zu erfüllen (siehe

bereits Tätigkeitsbericht des Innenministeriums Baden-Württemberg von 1995, S. 134 f; Dr. Thilo Weichert, WRP 1996, S. 522 ff (532)).

Das Unternehmen, von dem die Daten stammen, muss die vertraglichen Beziehungen mit dem Auftragnehmer (hier: Rechenzentrum) so gestalten, dass der Auskunftsanspruch verwirklicht werden kann.

Wenn die Geltendmachung des Auskunftsrechts (und demzufolge auch des Widerspruchsrechts nach § 28 Abs. 3 BDSG) nicht gewährleistet ist, wäre die Datenverarbeitung bzw. -nutzung unzulässig.

Es besteht nämlich Grund zur Annahme, dass schutzwürdige Belange des Betroffenen entgegenstehen bzw. überwiegen, wenn er bereits in seinen elementaren Rechten, die das BDSG ihm zugesteht (Auskunft, Berichtigung, Löschung und Widerspruch), in erheblichem Maße behindert wird oder aber aufgrund der Aufteilung der Datennutzung und -verarbeitung auf verschiedene Unternehmen sogar ganz von seinen Rechten ausgeschlossen zu werden droht. Nach § 6 BDSG ist das Recht des Betroffenen auf Auskunft, Berichtigung und Löschung oder Sperrung unabdingbar und kann selbst durch Rechtsgeschäft nicht ausgeschlossen werden. Dies muss bei der gesamten Gestaltung der Werbemaßnahme berücksichtigt werden.

Trotz divergierender Auffassungen will sich der Bevollmächtigte erfreulicherweise dafür einsetzen, dass sich die Unternehmen in der ganzen Branche an folgende, von ihm formulierte Empfehlung halten, die im Wesentlichen den behördlichen Anforderungen Rechnung trägt:

"Alle Unternehmen, die Direktwerbung unter Einsatz von Fremdadressen betreiben oder die eigene Adresse (z.B. von Kunden) für Direktwerbemaßnahmen Dritter zur Verfügung stellen, sollten darauf bedacht sein, dass den datenschutzrechtlichen Ansprüchen der Betroffenen in ausreichendem Umfang Rechnung getragen wird (§§ 6; 28 Abs. 3; 29 Abs. 3 BDSG). Das gilt in besonderem Maß für den Anspruch auf Auskunft über die Datenherkunft (§ 34 BDSG). In der Praxis kann dies bedeuten:

Setzt ein Werbungstreibender Fremdadressen ein, deren Herkunft (Name des "Adresseneigners") ihm bekannt ist, hat er einem Betroffenen, der aus dieser Liste angeschrieben wurde, auf dessen Verlangen hin Auskunft auch über die Herkunft seiner Anschrift und sonstiger Daten zu erteilen.

Werden Fremdadressen unter Inanspruchnahme eines Auftragsdatenverarbeiters (z.B. Lettershops) verarbeitet und genutzt, ohne dass der Werbungstreibende selbst die Herkunft eindeutig bestimmen kann (z.B. einem Listenmix), sollte er darauf hinwirken, dass die Auskunftserteilung durch den Adresseneigner als "Herrn der Daten" erfolgt. Häufig wird der Auftragnehmer feststellen können, aus welchem Datenbestand die Anschrift des Betroffenen stammt. In einem derartigen Fall sollte vertraglich zwischen den Beteiligten (Werbungtreibender-Adresseneigner-Auftragsdatenverarbeiter) geregelt werden, dass Anfragen beim Werbungtreibenden über den Auftragnehmer an den Adresseneigner weitergeleitet werden und von diesem die Auskunfterteilung veranlasst wird.

Bescheidet ein Werbungtreibender den Auskunft begehrenden Betroffenen dahingehend, er könne aufgrund eingeschalteter Auftragnehmer keine Angaben über die Herkunft der Adresse machen, hat er das Auftragsunternehmen zu benennen. Dieses sollte aufgrund der vertraglichen Abmachungen gehalten sein, den Adresseneigner über das Auskunftsverlangen zu unterrichten. Ohne ausdrückliche Anordnung darf das Auftragsunternehmen von sich aus keine Auskünfte erteilen."

Auch wenn die Empfehlung viele Soll-Bestimmungen enthält und insoweit verbindliche Formulierungen vermissen lässt, so handelt es sich doch um eine sehr zu begrüßende Initiative, um tatsächlich eine Verbesserung zu erzielen.

Wünschenswert wäre, dass in der Novelle des BDSG noch eindeutigere Regelungen getroffen werden.

13.3 Nicht-Beachtung von Widersprüchen

Ein Kunde eines Autohändlers hatte wiederholt Werbung von dem Händler bzw. dem Herstellerunternehmen erhalten, obwohl er mehrfach nach § 28 Abs. 3 BDSG Widerspruch gegen die Verwendung seiner Daten für diese Zwecke eingelegt hatte. Die Daten verarbeitende Stelle versuchte, ihn mit dem Hinweis abzufertigen, das Datenverarbeitungssystem könne eine zuverlässige Sperrung seiner Daten für die werbliche Nutzung nicht leisten. Ein Mitarbeiter des Autohändlers wollte sich mit Hilfe dieser Aussage Arbeit ersparen. Der Kunde wurde als lästig empfunden, da hier nicht nur eine Eingabe in das eigene Datenverarbeitungssystem vor Ort hätte erfolgen müssen, sondern auch noch eine Meldung an die zentrale Werbeabteilung. Selbst auf das Anschreiben der Aufsichtsbehörde erfolgte der telefonische Hinweis, dass das Setzen eines Merkmals und gleichzeitig eine Meldung an die Zentrale so aufwändig und schwierig seien, dass man gerne darauf verzichten wolle. Erst auf den Hinweis, dass der Betroffene ein Recht hierzu habe und ggf. die Aufsichtsbehörde mit Hilfe einer Anordnung auch für die Durchsetzung dieses Rechtes generell bzw. für die Schaffung der erforderlichen organisatorischen/programmtechnischen Vorkehrungen im Betrieb sorgen werde, bequemte sich die Daten verarbeitende Stelle, die erforderlichen Maßnahmen durchzuführen.

Der geschilderte Fall ist leider kein Einzelfall.

Häufig basieren Eingaben von Betroffenen auf unqualifizierten Äußerungen von Mitarbeitern von Unternehmen. Hier ein kleiner Auszug aus derlei Ausreden: "Das geht in unserem Datenverarbeitungssystem nicht anders", "Ohne dieses Datum nimmt der Computer die Daten nicht an", "Löschen ist in unserem PC nicht vorgesehen", "Ihre Daten kann unser Computer nicht ausdrucken" usw.

Widerspricht ein Betroffener der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- und Meinungsforschung nach § 28 Abs. 3 BDSG, hat die Daten verarbeitende Stelle unverzüglich dafür Sorge zu tragen, dass er keine Werbung mehr erhält. Häufig gibt eine speichernde Stelle dann den Hinweis, die Daten seien gelöscht. Unabhängig davon, inwieweit eine Löschung erlaubt sein könnte (Aufbewahrungspflichten), ist aber jedenfalls durch organisatorische/programmtechnische Vorkehrungen sicherzustellen, dass der Betroffene zukünftig ebenfalls keine Werbung mehr erhält. In der Regel kann dies durch Setzen eines Merkmals im Kundenstammsatz erreicht werden oder aber auch durch Erstellen einer Datei, in der erfasst ist, welche Personen keine Werbung erhalten dürfen.

In einem zweiten Fall hat ein Verein die unerfreuliche Eigenschaft entwickelt, auf Anschreiben Betroffener zunächst einmal nicht zu reagieren. Sowohl bei der Inanspruchnahme des Rechtes auf Auskunft über die zur Person gespeicherten Daten als auch bei dem Einlegen des Widerspruchs gegen die Verwendung personenbezogener Daten für Werbezwecke, ist der Verein in den vorliegenden Fällen erst dann auch nur sehr zögerlich tätig geworden, als sich die Aufsichtsbehörde aufgrund der Eingabe der Betroffenen eingeschaltet hatte.

Hinsichtlich der Auskunftserteilung konnte das Verfahren noch nicht abgeschlossen werden. Das Ergebnis wird in den nächsten Tätigkeitsbericht einfließen.

Bei den Widersprüchen argumentiert der Verein zunächst mit Verwaltungsproblemen, mit der Krankheit von Mitarbeitern und ähnlichem und zögert somit die Bearbeitung in die Länge. Ein besonderes Problem ist dann gegeben, wenn Anschriften an die ausländischen Dachverbände übermittelt wurden. Betroffene erfahren davon erst, wenn sie Werbung von dort erhalten. Dem Verein bereitet es dann - nach eigener Darstellung - große Schwierigkeiten festzustellen, ob und an welche Stelle er Daten übermittelt hat, und wie er nun dafür Sorge zu tragen hat, dass das Widerspruchsrecht der Betroffenen auch gewahrt wird.

Die mangelnde Kooperationsbereitschaft des Vereins führt zu einem unerfreulichen Verwaltungsaufwand bei der Aufsichtsbehörde, da der Verein mehrmals angeschrieben werden muss. Es müssen Fristen gesetzt werden und erst kurz vor der Einleitung eines Ordnungswidrigkeitenverfahrens geht eine entsprechende Antwort ein. Der Bürger sollte bei einem Verein, dessen

Strukturen er nicht genau kennt, zurückhaltend mit der Preisgabe von Angaben zu seiner Person sein.

13.4 Rätselhaftes Verschwinden von Widersprüchen gegen unverlangte Werbung

Die Aufsichtsbehörde wurde öfters mit dem Phänomen konfrontiert, dass die Widerspruchsschreiben der Betroffenen bei den speichernden Stellen angeblich nie ankamen oder auf unerklärliche Weise im Geschäftsgang verschwunden waren. Die nachforschenden Schreiben der Aufsichtsbehörde konnten diesem eigenartigen branchenübergreifenden Schicksal der Beschwerdebriefe allerdings glücklicherweise entgehen und wurden von den betrieblichen Datenschutzbeauftragten der betroffenen Banken, Versicherungen und Einzelhandelsunternehmen in der Regel umgehend beantwortet.

Allzu oft muss festgestellt werden, dass die Werbewidersprüche bei den Kunden- und Marketingabteilungen der Werbetreibenden missachtet werden.

Um dem Widerspruch gegen die Nutzung der personenbezogenen Daten zu Zwecken der Werbung und der Markt- und Meinungsforschung nach § 28 Abs. 3 BDSG umgehend und zuverlässig bei der speichernden und der ausführenden Stelle Geltung zu verschaffen, empfiehlt es sich nach den Erfahrungen der Datenschutzaufsichtsbehörde, den Widerspruch direkt an den betrieblichen Datenschutzbeauftragten des jeweiligen werbenden Unternehmens zu richten.

14. Datenverarbeitung und Beauskunftung im Versandhandel

Das Recht auf Auskunft über die zur Person gespeicherten Daten ist nach § 6 BDSG ein unabdingbares Recht der Betroffenen. Wenn ein Bürger zu der Auffassung gelangt, dass von einem Unternehmen Daten zu seiner Person verarbeitet werden, die er nicht kennt oder die unter Umständen nicht richtig sind, kann er mit Hilfe des Auskunftsrechtes zunächst feststellen, welche Daten zu seiner Person verarbeitet werden. Ohne eine vollständige Auskunft kann die Richtigkeit und Ordnungsmäßigkeit der Datenverarbeitung von den Betroffenen nicht überprüft werden. Eine Reihe von Eingaben über die Datenverarbeitung durch Versandhandelsunternehmen enthielten die Frage nach der Vollständigkeit einer Auskunft.

Der Versandhandel bietet seinen Kunden zahlreiche Möglichkeiten zur Bezahlung der Ware an. Eine beliebte Form der Bezahlung ist der Kauf auf Rechnung. Der Besteller erhält zunächst die Ware und hat dann einige Tage Zeit, bis er die Rechnung begleichen sollte. Diese Form der Bezahlung bietet gegenüber einer Nachnahme für den Kunden den Vorteil, dass er die Ware erst einmal in Augenschein nehmen kann und bei einer Rücksendung/Rückgabe nicht - wie häufig - Monate auf die Erstattung des bezahlten Betrages warten muss.

Aber nicht bei allen Bestellern handelt es sich um Personen, die Ware in der Absicht, diese auch zu bezahlen, bestellen. Dem Versandhandel werden durch Betrügereien erhebliche Verluste zugefügt. Aus diesem Grund ist es legitim, dass die Unternehmen versuchen, sich weitgehend gegen Betrügereien zu schützen. So sind mittlerweile mit Hilfe der modernen Datenverarbeitung Systeme entstanden, mit deren Hilfe Daten über Bestellungen zusammengetragen und ausgewertet werden und auf statistisch zuverlässige Weise vorhergesagt werden kann, welche Art der Bestellung mit ziemlicher Sicherheit zu einem Verlust führen wird. Diese so genannten Scoring-Verfahren enthalten die Erfahrung der Unternehmen über viele Jahre und versuchen, daraus sichere Analysen zu erstellen. Z.B. wird überprüft, welche Waren in welchem Zusammenhang, in welcher Menge, in welcher Preiskategorie bestellt werden. Aber auch der Wohnort und die Straße und unter Umständen das Gebäude des Bestellers werden in die Überprüfung mit einbezogen. In den Dateien sind sowohl die Anschriften von Justizvollzugsanstalten wie aber auch von Wohngebieten mit hauptsächlich sozial schwachen Bewohnern enthalten. Natürlich wird auch bei bereits vorhandenen Bestellern das bisherige Zahlungsverhalten mit eingebracht.

Häufig aber führt bei Neubestellern bereits die angegebene Anschrift dazu, dass der Besteller ein Schreiben erhält, in welchem er darauf hingewiesen

wird, dass ihm die Ware nur per Nachnahme geliefert werden kann. Dem betroffenen Bürger selbst ist aber, wenn er z.B. in einen größeren Wohnblock umzieht, nicht immer bekannt, ob in dieser Wohneinheit auch Sozialwohnungen vorhanden sind. Die schlechten Erfahrungen eines Versandhändlers mit Kunden unter einer bestimmten Anschrift können jedoch zu einer Aufforderung zur Zahlung per Nachnahme führen. Regelmäßig erstaunt waren die Bürger dann, wenn auf ihre Anfrage zur Auskunft nur ihre Bestelldaten und die von ihnen angegebenen Daten genannt wurden. Die Bürger vermuteten daraufhin, dass die Versandhändler weitere Daten zur Person verarbeitet hätten, ohne ihnen diese mitzuteilen. Die Versandhäuser vertreten die Auffassung, zu einer Auskunft bezüglich des Scoring-Verfahrens nicht verpflichtet zu sein, da die entsprechenden Daten nicht personenbezogen verarbeitet würden. Die Verarbeitung der Daten im Scoring-Verfahren erfolgt in der Tat in einer eigenen Datei. Die Daten der Besteller werden mit dieser Datei abgeglichen. Je nach Ergebnis des Abgleiches erscheint dann der Hinweis 'per Nachnahme' oder 'Kauf auf Rechnung'. Mag auch der Begriff der personenbezogenen (direkten) Speicherung nicht erfüllt sein, so ist es doch im Ergebnis nicht akzeptabel, dass der Betroffene keine Informationen über das für ihn bedeutsame Verfahren erhält. Der Besteller sollte auf ein derartiges Verfahren hingewiesen und über die Verfahrensweise ausreichend informiert werden.

Die einzelnen vorliegenden Beschwerden führten zwar zu einem Ergebnis, das in der Regel auch bei den Betroffenen auf Verständnis gestoßen ist, doch sind weitere Gespräche mit Versandhändlern geplant, um zukünftigen Beschwerden vorzubeugen und zu einer generell befriedigenden Verfahrensweise zu gelangen.
Dabei wird vor allem die Umsetzung des Art. 15 der EU-Richtlinie durch die BDSG-Novelle von Bedeutung sein, wonach automatisierten Einzelentscheidungen nur unter bestimmten Voraussetzungen zulässig sind, insbesondere wenn der Betroffene die Möglichkeit hat, seinen Standpunkt geltend zu machen. Dies setzt entsprechende Informationen voraus.

15. Datenverarbeitung in Vereinen

15.1 Datenschutz bei der Vereinsdatenverarbeitung

In zahlreichen eingetragenen Vereinen mit kulturellen, sozialen oder sportlichen Vereinszwecken werden die jeweils benötigten Daten der Vereinsmitglieder automatisiert und dateimäßig im Sinne des § 3 Abs. 2 Nr. 1 BSDG verarbeitet. Dabei kann es sich lediglich um Name, Anschrift und Geburtsdatum handeln. Viele Vereine erfassen und nutzen auf den Standard-PCs in den Geschäftsstellen der Vereine und ihrer Dachverbände allerdings auch die Telefonnummer, Spenden-, Beitrags- und Zahlungsdaten, Daten über den Trainingsbesuch, Funktionen im Verein, die Teilnahme an Veranstaltungen und Projekten, geleistete Arbeitseinsätze, sportliche Leistungen, Gesundheitsdaten und - je nach Vereinszweck - andere Angaben über ihre Mitglieder.

Aber auch für die Verarbeitung der Mitgliederdaten auf den heimischen PCs ehrenamtlicher Vereinsfunktionäre gelten die datenschutzrechtlichen Bestimmungen des BDSG. Bei der Vereinsmitgliedschaft handelt es sich um ein vertragsähnliches Vertrauensverhältnis im Sinne des § 28 Abs. 1 BDSG. Die Persönlichkeitsrechte der Mitglieder müssen daher bei der Verarbeitung, Nutzung, Übermittlung oder Veröffentlichung der Mitgliedsdaten angemessen und den detaillierten Schutzregelungen des § 28 BDSG entsprechend - unabhängig von der Vereinsgröße oder dem Standort des PCs - berücksichtigt werden.

Bei der Beurteilung der Zulässigkeit des Umfanges der Mitgliederdatenverarbeitung ist regelmäßig auf den Zusammenhang der Verarbeitung mit dem Vereinszweck und den in der Vereinssatzung festgelegten Regelungen zur ordnungsgemäßen Datenverarbeitung abzustellen. Leider musste die Aufsichtsbehörde feststellen, dass viele Vereinssatzungen keine geeigneten Bestimmungen (beispielsweise Angaben zum Umfang der Speicherung oder Löschfristen beim Ausscheiden) enthalten und in dieser Hinsicht noch ergänzungsbedürftig sind.

Oftmals war selbst in großen Organisationen die gesetzliche Vorschrift des § 36 BDSG zur Bestellung eines Datenschutzbeauftragten und des § 5 BDSG über die Verpflichtung der zugriffsberechtigten Beschäftigten und Funktionäre auf das Datengeheimnis unbekannt. Auch bezüglich technischer und organisatorischer Sicherheitsmaßnahmen nach § 9 BDSG (Schutz vor missbräuchlicher Verwendung, Datensicherung, datenschutzgerechte Datenträgerentsorgung) konnte die Aufsichtsbehörde mithelfen, bestehende Defizite abzubauen.

15.2 Unberechtigte Veröffentlichung von Mitgliederdaten

Dass auch relativ kleine Vereine bei automatisierter Datenverarbeitung unter die Bestimmungen des BDSG fallen, ist noch nicht zu allen Vorständen vorgedrungen. Wenn dann, was bei Vereinen vorkommt, Streitigkeiten der Mitglieder untereinander oder auch zwischen Vorstand und Mitgliedern entstehen, ist darauf zu achten, dass nicht gedankenlos mit den vorhandenen personenbezogenen Daten umgegangen wird.

Aufgrund einer Eingabe wurde bei einem Kleingartenverein festgestellt, dass Mitglieder des Vorstandes Daten aus dem Mitgliederbestand ungerechtfertigt veröffentlicht hatten.

In der Satzung dieses Vereines war festgelegt, dass die Mitglieder zu bestimmten Arbeiten im Bereich des öffentlichen Teiles der Kleingartenanlage verpflichtet sind. Die Stunden werden automatisiert verwaltet, sodass am Ende eines Jahres eine Aufstellung erfolgt, aus der ersichtlich ist, welche Mitglieder entsprechend der Satzung ihre Arbeiten abgeleistet haben. Wer sein Arbeitssoll nicht erfüllt hat, ist verpflichtet, einen bestimmten Geldbetrag in die Vereinskasse zu zahlen. Aufgrund einiger Vorkommnisse hielt es ein Vorstandsmitglied für geboten, die Aufstellung der Stunden auszudrucken und auf dem öffentlich zugänglichen Gelände unter Angabe der Person des Mitgliedes auszuhängen, um die "faulen" Mitglieder an den Pranger zu stellen.
Außerdem ließ der Vorstand an dieser öffentlich zugänglichen Stelle auch Schriftsätze und Gerichtsentscheidungen, welche Vereinsstreitigkeiten einzelner Mitglieder betrafen, anbringen. Wenngleich insoweit der Dateibegriff zweifelhaft ist, zeigt dies doch die mangelnde Sensibilität im Umgang mit personenbezogenen Daten.

Die beschwerdeführende Person bat allerdings darum, dass die Aufsichtsbehörde lediglich ihre Rechtsauffassung mitteile und diese nicht dem Vorstand des Vereines zukommen lasse, da sie weiter gehende Probleme befürchtete. Zwar darf niemand, der sich an die Aufsichtsbehörde wendet, dadurch Nachteile erleiden, doch war hier vorhersehbar, dass der Vorstand zumindest bestimmten Personen unterstellen würde, dass diese als Beschwerdeführer in Betracht kommen. Somit wäre die bereits persönlich unerfreuliche Situation noch verschlechtert worden.

15.3 Herausgabe von Verzeichnissen und Listen der Vereinsmitglieder

Mehrfach wurden im Berichtsjahr von Vereinen unterschiedlichster Ausrichtung Fragen an die Aufsichtsbehörde zur Zulässigkeit der Herausgabe von Mitgliederverzeichnissen an die Vereinsmitglieder herangetragen.

Die jeweilige Zulässigkeit kann in der Regel nur unter Berücksichtigung des satzungsgemäßen Vereinszwecks, der Vereinsstrukturen und unter Beachtung etwaiger schutzwürdiger Belange der betroffenen Vereinsmitglieder beurteilt werden. Fraglich ist die Zulässigkeit der Herausgabe eines Mitgliederverzeichnisses vor allem bei Vereinen, bei denen der Vereinszweck keine Verbundenheit oder gegenseitiges Kennen der Mitglieder voraussetzt und die Pflege des persönlichen Kontaktes der Mitglieder kein wichtiger Bestandteil des Vereinszwecks ist (z.B. bei Fördervereinen). Insbesondere ist immer zu berücksichtigen, ob es Mitglieder gibt, die ein schutzwürdiges Interesse daran haben, dass ihre Adresse nicht offen gelegt wird (z.B. in Selbsthilfevereinen).

Bei keinem der anfragenden Vereine existierten Satzungsregelungen über die Herausgabe von Mitgliederverzeichnissen. Die Aufsichtsbehörde hat den

Vereinen daher empfohlen, einen Beschluss der Mitgliederversammlung herbeizuführen, der die künftige Herausgabe einer Mitgliederliste oder eines Mitgliederverzeichnisses regelt und eventuell auch in die Vereinssatzung aufgenommen werden sollte. Die Neuregelung ist dann in geeigneter Form im Verein bekannt zu machen. Alle betroffenen Mitglieder sollten die Möglichkeit haben, der Aufnahme in das Mitgliederverzeichnis widersprechen zu können. In Zweifelsfällen sollte die schriftliche Einwilligung der Betroffenen zur Aufnahme in die Mitgliederliste im Sinne des § 4 BDSG eingeholt werden.

15.4 Unzulässige Offenbarung von Beitragsdaten

In einem Fall wurde die Aufsichtsbehörde von einem Petenten auf eine ungewöhnliche Methode hingewiesen, säumige Mitglieder zur Entrichtung eines (in diesem Fall in der Höhe strittigen) Zusatzbeitrages zu bewegen.

Um der Aufforderung zur Zahlung dieses Zusatzbeitrages Nachdruck zu verleihen, wurden während der Übungsstunden in der Trainingsstätte Listen mit den Namen derjenigen Vereinsmitgliedern offen gelegt, die den Zusatzbeitrag noch nicht gezahlt hatten. Statt die vereinsinterne oder zivilrechtliche Klärung der Rechtmäßigkeit der Beitragsforderung abzuwarten, setzte die Vereinsführung ihre Hoffnung eher auf die Wirksamkeit des so entstandenen sozialen Druckes.

Der Vereinsvorstand wurde darauf hingewiesen, dass das bestehende vertragsähnliche Vertrauensverhältnis mit den Mitgliedern, diese nicht nur zur Zahlung der Beiträge, sondern den Verein auch zur Wahrung der Persönlichkeitsrechte seiner Mitglieder verpflichtet. Für den Umgang mit Mitgliederdaten bedeutet dies, dass die jeweiligen Daten nur von den entsprechenden Funktionsträgern des Vereins verarbeitet und genutzt werden dürfen. Die einzelnen vereinsinternen Zuständigkeiten werden durch Satzung, Beitragsordnung, Abteilungsordnung und durch die satzungsgemäßen Organe des Vereins bestimmt. Die für die Beitragsfestsetzung und den Beitragseinzug relevanten Mitgliederdaten müssen z.B. regelmäßig dem Schatzmeister oder auch den Beschäftigten in der Vereinsgeschäftsstelle zur satzungsgemäßen Aufgabenerfüllung zur Verfügung stehen. Die Preisgabe von Beitragsdaten an Personen außerhalb dieses eng umrissenen Personenkreises ist daher unzulässig und wurde bei dem Vereinsvorstand beanstandet.

Auch die schriftliche Verpflichtung der zugriffsberechtigten Personen auf das Datengeheimnis nach § 5 BDSG wurde von der Aufsichtsbehörde angemahnt.

16. Datenerhebung und Speicherung bei Alltagsgeschäften

16.1 Erhebung und Speicherung personenbezogener Daten beim Barverkauf

Bei den Bargeschäften des täglichen Lebens sollten regelmäßig keine personenbezogenen Daten erhoben und gespeichert werden, da dies im Rahmen der Zweckbestimmung dieser Alltags-Kaufverträge nicht notwendig und in den meisten Fällen nicht einmal dienlich ist. Dennoch gingen im Berichtsjahr Beschwerden unter anderem über Datenerhebungen in Großmärkten bei der Aufsichtsbehörde ein, in denen von den Kunden beim Barkauf die Angabe ihrer Personalien verlangt wurde.

Ein Kunde eines Elektro-Marktes wurde beim Kauf eines HiFi-Receivers vom Verkaufspersonal aufgefordert, seinen Namen und seine Anschrift anzugeben. Er verweigerte die Preisgabe seiner Daten, woraufhin ihm das gewünschte Gerät nicht verkauft wurde, ohne dass ihm - trotz Nachfrage - vernünftige Gründe für die zwingende Erhebung und Speicherung seiner Personalien genannt wurden. Von einem Baumarkt-Kunden wurde die Angabe seines Namens und seiner Anschrift anlässlich des Barkaufes einer kleinen Holzfigur verlangt. Auch diesem Kunden konnte man den Zweck dieser Maßnahme nicht erklären.

Da die gewünschten Artikel nicht angeliefert werden sollten und eventuelle Gewährleistungsansprüche nicht vorhanden waren oder im Garantiefall nur

den Hersteller und nicht den Elektro-Großmarkt treffen, waren bereits die Datenerhebungen zur Abwicklung der Alltagskäufe unnötig und überflüssig. Sie können ein treuwidriges, d. h. unzulässiges Verhalten entgegen § 28 Abs. 1 Satz 2 BDSG darstellen, da keine Rechtfertigung für eine anschließende Speicherung und Nutzung gegeben wäre.

Die Marktleiter der betroffenen Großmärkte zeigten sich überrascht von den Nachforschungen der Aufsichtsbehörde und gaben an, dass es sich bei den Vorfällen um Missverständnisse und bedauerliche Fehlleistungen einzelner Mitarbeiter gehandelt haben müsse. Nach umfassender Information und Beratung durch die Aufsichtsbehörde haben die Märkte ihr Personal eingehend darauf hingewiesen, dass die Erhebung personenbezogener Daten bei einfachen Bargeschäften des täglichen Lebens zur Abwicklung des Verkaufs nicht nötig ist und in der Regel - vor allem wenn der Kunde es nicht wünscht - zu unterbleiben hat, soweit nicht ein Gewährleistungsanspruch oder die Anlieferung der Ware damit verbunden ist.

16.2 Dauer der Speicherung bei Zahlung im EC-Lastschriftverfahren

Eine Bürgerin wandte sich an die Aufsichtsbehörde mit dem Hinweis, dass ein Bekleidungshaus die aus der Zahlung per Lastschriftverfahren mit der EC-Karte angefallenen Daten der Kundinnen und Kunden auf Vorrat und ohne Einwilligung speichert und zusätzlich mit dem Lastschriftformular auch noch Name und Anschrift erhebt und unbegrenzt auf Dauer vorhält.

Bei der Zahlung von Waren des täglichen Bedarfs im EC-Lastschriftverfahren ist die Speicherung der Kontenangaben bis zur Gutschrift des Rechnungsbetrages auf dem Konto des Verkäufers nach § 28 Abs. 1 Nr. 1 BDSG zulässig. Das Verfahren ermöglicht dem Unternehmen, das finanzielle Risiko bei Nichteinlösung der Lastschrift zu tragen, und ist Voraussetzung für die Bearbeitung eventueller Lastschriftrückbuchungen.

Die darüber hinausgehende temporäre Speicherung von Name und Anschrift ist im EC-Lastschriftverfahren allerdings nicht zwingend notwendig, da der Kunde mit seiner Unterschrift bereits seiner Bank die Einwilligung erteilt, im Falle der Nichteinlösung seinen Namen und seine Anschrift an den Verkäufer zu übermitteln.

Nach der Zahlungsabwicklung jedenfalls ist die weitere Speicherung und Nutzung der Daten nur solange und in dem Umfange zulässig, wie mögliche Gewährleistungsfristen bestehen. Ist Gewährleistung ausgeschlossen oder nicht möglich, sind die Daten unverzüglich nach Erhalt des Geldes oder der Gutschrift nach § 35 Abs. 2 Nr. 3 BDSG zu löschen, soweit nicht gesetzliche Vorschriften im Sinne des § 35 Abs. 3 Nr. 1 BDSG entgegenstehen. Auch bei langfristigen Kundenbeziehungen sind die jeweils aktuell nicht mehr erforderlichen Daten über einzelne Käufe zu löschen, da sich ansonsten die Kaufgewohnheiten dieser Kunden bei Alltagsgeschäften über Jahre zurückverfolgen ließen.

Das betroffene Bekleidungshaus wurde auf die gesetzlichen Regelungen zur Zulässigkeit der Datenerhebung und Löschung der anfallenden Daten aus dem EC-Lastschriftverfahren hingewiesen und die übermäßige Datenerhebung und -speicherung beanstandet. Das Formular des Unternehmens zum Lastschriftauftrag wurde auf Anregung der Aufsichtsbehörde umfassend inhaltlich und layout-technisch überarbeitet und den datenschutzrechtlichen Erfordernissen angepasst. Die Einwilligungserklärung wurde im äußeren Erscheinungsbild entsprechend § 4 Abs. 2 BDSG hervorgehoben. Die Kundinnen und Kunden werden nun auf die Freiwilligkeit ihrer Adressangaben und deren Verwendungszweck hingewiesen. Die Löschfristen für die Kaufdaten und die Daten aus dem EC-Lastschriftverfahren werden künftig beachtet.

17. Markt- und Meinungsforschungsunternehmen

In der Regel sind die Vorschriften des Bundesdatenschutzgesetzes bei Unternehmen der Markt- und Meinungsforschung bekannt. Insgesamt 58 Markt- und Meinungsforschungsunternehmen sind nach § 32 BDSG im Bezirk des Regierungspräsidiums Darmstadt gemeldet. Eine Eingabe aber verwies auf ein Unternehmen, welches der Aufsichtsbehörde bislang nicht bekannt war,

also nicht nach § 32 Abs. 1 Nr. 2 BDSG gemeldet war. Die Eingabe enthielt den Vorwurf, dass das Unternehmen Personen mehrfach befragt hätte, ohne dazu legitimiert zu sein.
Bei einer Befragung ist der Betroffene über den Zweck der Befragung zu unterrichten. Der Adressteil ist vom Frageteil zu trennen. Auswertungen haben in anonymisierter Form stattzufinden. Werden alle datenschutzrechtlichen Vorgaben berücksichtigt, kann bei einer Einmalbefragung auf die schriftliche Einwilligung der Betroffenen ausnahmsweise verzichtet werden. Die besonderen Umstände (sofortige Anonymisierung nach der Überprüfung der Interviewer) rechtfertigen diesen Verzicht auf die Schriftform.

Besteht aber die Absicht, eine Folgebefragung durchzuführen, muss mit der schriftlichen Einwilligung der Befragten gearbeitet werden. Im Beschwerdefall wurde jedoch eine schriftliche Einwilligung (§ 4 BDSG) - obwohl von vornherein eine zweite Befragung geplant war - nicht eingeholt. Die befragten Personen sollten lediglich mündlich auf eine Folgebefragung verwiesen werden.

Doch damit nicht genug, aufgrund von Unstimmigkeiten und Auswertungsproblemen wurde mit dem Auftraggeber eine weitere Befragung einer bestimmten Anzahl von Personen ausgehandelt und auch durchgeführt. Somit sind einige Befragte ein weiteres Mal angerufen worden. Aus dieser Gruppe haben sich Betroffene an die Aufsichtsbehörde gewandt und um Überprüfung gebeten.

Zum Zeitpunkt dieser Eingaben war die gesamte Marktuntersuchung jedoch bereits abgeschlossen. Die personenbezogenen Teile waren von den auszuwertenden Daten getrennt und bereits gelöscht worden. Insofern konnte das Unternehmen, welches die nicht datenschutzgerechte Arbeitsweise einräumte, nur noch auf die gesetzlichen Vorschriften verweisen und ermahnt werden, diese zukünftig zu beachten. Wegen der fehlenden Anmeldung bei der Aufsichtsbehörde wurde ein Ordnungswidrigkeitenverfahren durchgeführt und eine Geldbuße verhängt.

18. Kreditkartenunternehmen

Ein Kreditkartenkunde beschwerte sich darüber, dass er mehrfach Werbung erhalten habe, bei der wesentliche Teile seiner Kreditkartennummer im Anschriftenfeld der Werbebriefe sichtbar seien.

Das Kreditkartenunternehmen entschuldigte sich damit, dass durch einen Justierungsfehler bei der Kuvertierung auch der Adresscode mit Teilen der Kreditkartennummer sichtbar wurde. Derartige Justierungsfehler kommen leider - nicht nur bei diesem Unternehmen - relativ häufig vor.

Das Kreditkartenunternehmen löste das Problem auf die einfachste Art und Weise: Die Kreditkartennummer wird bei den Mailings nicht mehr verwendet.

19. Datenverarbeitung im Speditionsgewerbe

Der hessische Fachverband des Speditionsgewerbes trug vor, dass es trotz der hohen Arbeitslosenzahlen für Transport-, Speditions- und Logistikunternehmen schwierig sei, qualifiziertes gewerbliches Personal zu erhalten.

Vor dem Hintergrund zeitnaher Einstellungsnotwendigkeiten (durch saisonal und konjunkturell bedingte starke Beschäftigungsschwankungen) sei man darauf angewiesen, aus den wenigen vorhandenen Bewerbungen kurzfristig eine Auswahl und Entscheidung zu treffen.

Das größte Problem bei den Bewerbungen von gewerblichen Mitarbeitern stellten die - im Gegensatz zur Situation bei den kaufmännischen Angestellten - unzureichenden Bewerbungsunterlagen dar. Neben dem Bewerbungsschreiben (zum Teil erfolge auch nur ein Anruf) fehle bereits sehr oft ein aussagefähiger Lebenslauf. Schul-, Ausbildungs- und Arbeitszeugnisse seien nur in seltenen Fällen vollständig von dem Bewerber zu erhalten. Insbesondere sei ein lückenloser Beschäftigungsnachweis über die Arbeitszeugnisse fast nie möglich.

Da den Mitarbeitern sehr hohe Sachwerte anvertraut werden müssten, könne es beim Einsatz unzuverlässigen Personals zu erheblichen Schäden kommen. Schäden in Milliardenhöhe aufgrund Diebstahls, Unterschlagung etc. seien zu beklagen.

Die Rechtsprechung gehe von einem grob fahrlässigen Organisationsverschulden des Spediteurs aus, wenn dieser bei der Einstellung seines Personals nicht die Vorlage eines Führungszeugnisses verlangt oder sich auf sonstige Weise von der Zuverlässigkeit des Personals überzeugt habe. (OLG München, transpR 1993, 436; OLG Düsseldorf, transpR 1995, 169.)

Vor diesem Hintergrund beabsichtigt der Verband, eine zentrale Datei zu führen, in der die Beschäftigungsverhältnisse gespeichert werden sollen:

Wenn ein Arbeitnehmer eine Beschäftigung aufnimmt, meldet der Arbeitgeber dies dem Verband. Ebenso wird die Beendigung des Arbeitsverhältnisses gespeichert.

Bei einer Bewerbung kann ein Unternehmen, das Verbandsmitglied ist, abfragen, wo der Bewerber bisher beschäftigt war. Somit kann er sich ein Bild über den beruflichen Werdegang machen und (erforderlichenfalls) direkte Auskünfte bei den früheren Arbeitgebern einholen.

Die Aufsichtsbehörde wies den Verband darauf hin, dass bereits die Übermittlung an den Verband und die dortige Speicherung ihrer Auffassung nach nur auf der Grundlage einer Einwilligung zulässig ist.

Eine Abfrage, d.h. Auskunftserteilung durch den Verband kommt nur in Betracht, wenn tatsächlich eine Bewerbungssituation gegeben und der Bewerber kein oder kein aussagekräftiges Arbeitszeugnis vorgelegt hat. Der Verband müsste diese Angaben dokumentieren und zumindest stichprobenhaft überprüfen (vgl. § 29 Abs. 2 Satz 3 BDSG).

Außerdem müsste unmittelbar vor der Abfrage ein aktuelles Einverständnis des Bewerbers eingeholt werden, denn es ist nicht vertretbar, dass derartige Anfragen hinter dem Rücken des Betroffenen erfolgen. Da die Abgabe der Einwilligung bei Eingehung des letzten Arbeitsverhältnisses unter Umständen schon lange zurückliegen kann und zu jenem Zeitpunkt die neue Bewerbungssituation nicht genau voraussehbar war, kann diese ein aktuelles Einverständnis in der konkreten Bewerbungssituation nicht ersetzen bzw. abdecken.

Zu beachten ist außerdem, dass Dauer und Umfang der Speicherung begrenzt werden müssen: Maximal fünf Jahre; vorherige Löschung, wenn der Betroffene aus dem Erwerbsleben ausscheidet.

Obwohl der Inhalt der später gegebenenfalls telefonisch eingeholten Auskunft bei dem früheren Arbeitgeber nicht gespeichert wird, hielt es die Aufsichtsbehörde für gerechtfertigt und erforderlich, dass die Betroffenen darauf hingewiesen werden, dass sie arbeitsrechtlich einen Anspruch haben, den Inhalt der Auskunft schriftlich mitgeteilt zu bekommen (BGH, AP 1959 Nr. 2, § 630 BGB).

Die Absicht des Verbandes, die Mitarbeiter von Subunternehmen in der Weise in das gesamte Verfahren einzubeziehen, dass das Speditionsunternehmen auch dann Auskünfte über Mitarbeiter von Subunternehmen erhalten kann, wenn diese sich nicht bei dem Speditionsunternehmen bewerben, sondern nur im Rahmen des Vertrages mit dem Subunternehmer bei ihm eingesetzt sind, kann nach Auffassung der Aufsichtsbehörde nicht realisiert werden.

Zwar ist dem Verband einzuräumen, dass diese Subunternehmer-Mitarbeiter faktisch wie eigene Mitarbeiter eingesetzt werden; rechtlich aber besteht doch ein erheblicher Unterschied:

Eine arbeitsrechtliche Beziehung mit dem (Haupt-)Speditionsunternehmen besteht nicht, sodass die geplante Datei gerade nicht als Kompensation für unzureichende Bewerbungsunterlagen erforderlich ist.

Etwaige Schadensersatzforderungen von Kunden würden die Subunternehmer treffen bzw. könnten vertraglich auf diese abgewälzt werden. In diesem Punkt wurde noch keine Einigung erzielt.

20. Datensicherheit

20.1 Datensicherheit

Bei den Vorkehrungen und Maßnahmen zur Datensicherheit sind im Berichtszeitraum Veränderungen festgestellt worden. Soweit ein allgemeiner Trend erkennbar ist, geht dieser bedauerlicherweise nicht in eine positive Richtung, was eine Verbesserung der Maßnahmen zur Datensicherheit bedeuten würde, sondern häufig - trotz zahlreicher technischer Möglichkeiten - in die entgegengesetzte negative Richtung.

Gründe für diesen Trend sind unter anderem:

Bisher durchgeführte Maßnahmen erfüllen nicht mehr vollständig ihren Sicherungszweck und werden häufig als Behinderung angesehen (z.B. Regelungen der Zugangskontrolle).

Die Verwaltung der Berechtigungen innerhalb größerer Organisationen, bei denen die Zugriffsrechte streng nach der Erforderlichkeit vergeben worden sind, werden vernachlässigt, weil - so die Argumentation der Verantwortlichen - "bisher doch nichts passiert ist" oder weil "die Mitarbeiter sowieso zur Verschwiegenheit verpflichtet [seien] und bisher keine Geschäftsgeheimnisse nach draußen gelangt [seien]".

Durch viele technische Neuerungen und eine nicht mehr überschaubare Datenverarbeitungslandschaft ist die Sicherheitsorganisation problematisch geworden, wenn nicht sogar zusammengebrochen.

Die missbräuchliche Kenntnisnahme von personenbezogenen Daten wird als eine Art Kavaliersdelikt angesehen. Von großen Unternehmen werden ohne Überprüfung und ohne Protokollierung komplette Datenbestände an kleinere Auftragnehmer über eine Datenleitung weitergegeben, ohne dass die Sicherheitsvorkehrungen dieser Auftragnehmer vorab überprüft worden sind. Die auf dem Markt entstandenen sicheren Arbeitsplatzrechner und Software zur besseren Verwaltung und zur Absicherung einer ordnungsgemäßen Datenverarbeitung werden als überflüssige Kosten angesehen.

Besonders im Online-Datenverkehr werden z.B. Verschlüsselungen als zu aufwändig angesehen, als zu lästig abgelehnt und einige Datenverarbeiter lassen wohl den Gedanken an Sicherheit ganz fallen, da eine 100-prozentige Sicherheit ohnehin nicht erreichbar sei.

Es ist als erforderlich anzusehen, dass Unternehmen, die mit mehreren PCs und in Netzwerken arbeiten, Sicherheitsstrategien entwickeln und Sicherheitsmodelle schaffen.

Der betriebliche Beauftragte für den Datenschutz sollte sich mit den Datenverarbeitungsverantwortlichen am Aufbau einer Sicherheitsorganisation beteiligen. Hierzu müssen die Verantwortlichkeiten klar definiert werden.

Weiterhin ist (in einer Prioritätenliste) festzulegen, welche Sicherheitsmaßnahmen als vorrangig anzusehen sind und welche als spätere Aufrüstung möglich sind. Die zu nutzende Sicherheitssoftware, aber auch die entsprechenden organisatorischen Maßnahmen bzw. anderen Techniken sind ebenfalls festzulegen. Daneben sind die Protokollierungen und auch die möglichen durchzuführenden Kontrollen zu verabreden.

Doch alleine das Schaffen einer Sicherheitsorganisation wird in den meisten Fällen nicht als ausreichend anzusehen sein. Vielmehr müssen durch ständige Kontrollen die Maßnahmen überwacht und gegebenenfalls der rasanten technischen Entwicklung angepasst werden.

Die Maßnahmen sollten die menschlichen Unzulänglichkeiten berücksichtigen, die dazu führen, dass einmal eingeführte Maßnahmen nach einer gewissen Zeitspanne vernachlässigt werden. Auf jeden Fall sollte das Thema der Datensicherheit zukünftig weitaus mehr in den Vordergrund gestellt werden als bisher.

20.2 Löschen von Daten auf Festplatten

Nach § 35 Abs. 2 Satz 1 BDSG können personenbezogene Daten, außer in den Fällen des § 35 Abs. 3 Nr. 1 und 2, jederzeit gelöscht werden. Personenbezogene Daten sind unter den in § 35 Abs. 2 Satz 2 BDSG genannten Voraussetzungen zu löschen.

Nach § 3 Abs. 5 Nr. 5 BDSG ist Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

Unkenntlichmachen bedeutet, dass keine Daten mehr einer Person zugeordnet werden können bzw. keine Person mehr zu erkennen sein darf.

Die gebräuchlichen Anwendungsprogramme bieten verschiedene Möglichkeiten zum so genannten "Löschen" von Daten, die jedoch unzureichend sind:
Bei einfachen "Löschbefehlen" wird im Bereich der Dateibeschreibungsdaten/Ordnungskriterien ein Kennzeichen gesetzt, welches für das Anwendungsprogramm die Bedeutung hat, dass die gekennzeichnete Datei nicht mehr zu lesen ist. Die Datei ist für den Anwender nicht mehr sichtbar. Beim Betriebssystem UNIX beispielsweise, wird beim Erstellen einer Datei zunächst ein Verzeichniseintrag erstellt, der umgesetzt für den Anwender den Namen der Datei darstellt, daneben wird ein Ordnungsbegriff um die Ziffer 1 erhöht, der bei der nächsten neuen Datei weiter erhöht wird. Anhand dieser Zähler und des umgesetzten Dateinamens erfolgt auch beim Lesen das Erkennen der Datei.

Je nach Software wird durch den Löschbefehl entweder nur der Zähler verändert oder aber zusätzlich der Name gelöscht. Die Daten bleiben aber physikalisch auf dem Datenträger vorhanden.
Je nach Betriebssystem ist es mit verhältnismäßig einfachen Werkzeugen (Tools) möglich, diese Daten wieder sichtbar zu machen. Das so genannte "Löschen" mit den üblichen Löschbefehlen erfüllt deshalb in keiner Weise die Anforderungen, die das Datenschutzgesetz an eine Löschung stellt.

Bedauerlicherweise verfügen in diesem Bereich der Datenverarbeitung nur wenige Nutzer über die entsprechenden Kenntnisse.
Auch beim Formatieren findet oftmals keine physische Löschung statt. Bei den als "schnellen Formatierungen" angegebenen Möglichkeiten wird nur der zur Verarbeitung zur Verfügung stehende Festplatten- oder Diskettenspeicherplatz neu in bestimmte Sektoren aufgeteilt, die vom Betriebssystem verwaltet werden. Dadurch ist eine bis dahin vorhandene Adressierung nicht mehr gültig und die Datei bzw. die Satzadressen werden vom System nicht mehr erkannt.
Bei anderen Formatierungsprogrammen wird neben der neuen Sektorenaufteilung auch eine Löschung der Kopfsätze (Header) zusätzlich durchgeführt. Die eigentlichen inhaltlichen Daten befinden sich jedoch nach wie vor auf der Festplatte. Es ist zwar schwieriger, eine neu formatierte Festplatte zu rekonstruieren als einen Datenbestand, der durch einen bloßen Löschbefehl bearbeitet worden ist, doch es ist durchaus nicht unmöglich, den Datenträger inklusive Datenbestand vollständig wiederherzustellen. Daher stellt auch das Formatieren oftmals keine Löschung im Sinne des BDSG dar.

Ein datenschutzgerechtes Löschen lässt sich dadurch erreichen, dass stark magnetisiert wird, sodass die Daten physisch gelöscht sind und in keiner Weise mehr rekonstruiert werden können (wobei für die Festplatte die Gefahr der völligen Zerstörung besteht). Eine andere Art und Weise kann das Überschreiben des gesamten Speicherbereiches mit 0 oder anderen besonderen Ziffern darstellen. Ein derartiges Überschreiben sollte allerdings mehrmals hintereinander durchgeführt werden, denn es gibt durchaus Spezialisten, die behaupten, dass ein einmal überschriebener Speicher noch auswertbar ist. Letztendlich bleibt die Methode der totalen Zerstörung, z.B. die Zerkleinerung einer Festplatte.

21. Ordnungswidrigkeitenverfahren

Im Berichtsjahr 1998 wurden von den Aufsichtsbehörden elf Verfahren nach dem Gesetz über Ordnungswidrigkeiten nach § 44 Abs. 1 BDSG gegen die Geschäftsführer bzw. Inhaber Daten verarbeitender Unternehmen und Ge-

werbebetriebe eingeleitet. Neun dieser Verfahren betrafen Unternehmen, die als Dienstleistungsdatenverarbeiter oder Markt- und Meinungsforscher der Meldepflicht zum bei der Aufsichtsbehörde geführten Register nach § 32 Abs. 1 BDSG unterliegen. Sieben der erlassenen Bußgeldbescheide mit einer Gesamtbußgeldsumme in Höhe von 8.700,-- DM haben noch im Berichtsjahr 1998 Rechtskraft erlangt.

Ein von der Aufsichtsbehörde in Folge der Bearbeitung der Beschwerde eines Bürgers gegen einen Zeitschriften-Abonnement-Service nach § 44 Abs. 1 Nr. 6, 1. Alternative BDSG eingeleitetes Ordnungswidrigkeitenverfahren wegen der (trotz mehrfacher Aufforderung) nicht erfolgten Erteilung von Auskünften (entgegen § 38 Abs. 3 Satz 1 BDSG) wurde eingestellt. Die beschuldigte ehemalige Geschäftsführerin konnte glaubhaft nachweisen, dass sie die Geschäftsführung des Unternehmens bereits vor Eintritt des Bußgeldtatbestandes niedergelegt hatte und vorher nur als "Strohfrau" in dem Unternehmen tätig war. Das Unternehmen wechselt seit Jahren sehr routiniert und in kurzen Abständen seinen Geschäftssitz und sein Registergericht, verschleiert dadurch seinen Geschäftssitz und tauscht zudem die verantwortlichen Personen im Unternehmen aus, um die Nachforschungen zu erschweren. Da es dabei auch seiner gewerberechtlichen Anmeldepflicht beim kommunalen Gewerberegister nie nachkam, konnte trotz hohen Ermittlungsaufwandes im Berichtsjahr nicht sicher festgestellt und nachgewiesen werden, welche Person letztlich für den Gewerbebetrieb verantwortlich war und ist. Die Aufsichtsbehörde wird diesen Fall im laufenden Jahr weiter verfolgen.

Drei Ordnungswidrigkeitenverfahren nach § 44 Abs. 1 Nr. 6 BDSG wegen der trotz mehrfacher Erinnerung nicht erfolgten Erteilung von Auskünften an die Aufsichtsbehörde entgegen § 38 Abs. 3 Satz 1 BDSG richteten sich gegen die Geschäftsführer von nach § 32 Abs. 1 Nr. 3 BDG meldepflichtigen Dienstleistungsunternehmen aus dem Direktwerbe- und Marketingbereich. Die Unternehmen, die ihre Dienstleistungen sowohl für die Durchführung von Direktwerbeaktionen zur Neukundengewinnung anbieten, als auch im Rahmen von Kundenbindungsprogrammen als Auftragnehmer die Datenbanken zur Kundenpflege und -betreuung für mehrere große Auftraggeber auf ihren EDV-Systemen verwalten, hatten mehrere Monate die Aufforderungen der Datenschutzaufsichtsbehörde zur Auskunftserteilung ignoriert. Alle drei Bußgeldbescheide haben noch während des Berichtsjahres Rechtskraft erlangt.
Ein ebenfalls nach § 32 Abs. 1 Nr. 3 BDSG meldepflichtiger Datenträgervernichtungsbetrieb, gegen dessen Inhaber auch ein staatsanwaltschaftliches Ermittlungsverfahren wegen Betruges anhängig ist, hat in dem wegen fortgesetzter Auskunftsverweigerung eingeleiteten Ordnungswidrigkeitenverfahren Einspruch eingelegt, der an die Staatsanwaltschaft weitergeleitet wurde. Daher hat der Bußgeldbescheid im Berichtsjahr keine Rechtskraft mehr erlangt.

Gegen vier Geschäftsführer von Firmen aus dem Bereich der Dienstleistungsdatenverarbeitung und der Markt- und Meinungsforschung wurden Ordnungswidrigkeitenverfahren nach § 44 Abs. 1 Nr. 2 BDSG wegen der (entgegen § 32 Abs. 1 BDSG) nicht erfolgten Mitteilung über die Aufnahme einer meldepflichtigen Tätigkeit eingeleitet. Alle Firmen übten bereits mehrere Jahre die meldepflichtige Tätigkeit der Verarbeitung personenbezogener Daten im Auftrag als Dienstleistungsunternehmen oder der Speicherung personenbezogener Daten zum Zweck der anonymisierten Übermittlung aus, ohne die erforderliche Meldung zum Register der meldepflichtigen Stellen bei der Aufsichtsbehörde abgegeben zu haben. In zwei Fällen erhielt die Aufsichtsbehörde die entscheidenden Hinweise auf die Tätigkeit der Unternehmen durch die Eingaben betroffener Bürger, die von der fehlerhaften und unzulässigen Verarbeitung ihrer personenbezogenen Daten direkt betroffen waren und sich an die Datenschutzaufsichtsbehörde mit der Bitte um Abhilfe gewandt hatten.

Wiesbaden, 24. August 1999

Der Hessische Ministerpräsident
Koch

Der Hessische Minister des Innern
und für Sport
Bouffier