14. Wahlperiode

Drucksache **14/4159**

# HESSISCHER LANDTAG

16. 09. 98

## Vorlage
## der Landesregierung
**betreffend den Elften Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden**

Vorgelegt mit der Stellungnahme zum Sechsundzwanzigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten - Drucks. 14/3697 - nach § 30 Abs. 2 des Hessischen Datenschutzgesetzes vom 11. November 1986.

Eingegangen am 16. September 1998 · Ausgegeben am 29. September 1998

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

## Inhaltsverzeichnis

## 1. Bearbeitung von an die Behörde herangetragenen Datenschutzbeschwerden nach § 38 Abs. 1 BDSG

Die Regierungspräsidien überprüfen als Aufsichtsbehörden 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 gingen bei den Aufsichtsbehörden 231 Beschwerden gegen Stellen ein, 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.

Alle Beschwerden führten zur Überprüfung der datenverarbeitenden Stellen durch die Aufsichtsbehörde.

Die Beschwerden betrafen:

- Unternehmen der Direktmarketing- und Werbebranche in 67 Fällen,
- Kreditinstitute und Banken in 26 Fällen,
- Versicherungsgesellschaften in 24 Fällen,
- Handels- und Wirtschaftsauskunfteien in 16 Fällen,
- die Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA) in 13 Fällen,
- das Gesundheitswesen (Kliniken, Apotheken, Ärzte) in 11 Fällen,
- Versandhandelsunternehmen in 9 Fällen,
- den Handel und Einzelhandel in 8 Fällen,
- Interessenverbände und eingetragene Vereine in 7 Fällen,
- Vermieter, Hausverwaltungen und Mietervereine in 6 Fällen,
- den Datenschutz in Arbeitsverhältnissen in 5 Fällen,
- Reiseveranstalter und Fluglinien in 5 Fällen,
- Kreditkartenunternehmen in 4 Fällen,
- politische Parteien in 4 Fällen,
- Adreßverlage in 2 Fällen,
- Markt- und Meinungsforschungsunternehmen in 2 Fällen,
- Telefonmarketingunternehmen in 2 Fällen,
- Zeitungsverlage in 2 Fällen,
- sonstige Unternehmen (z.B. Telediensteanbieter, Filmtheater, Unternehmensberatung) in 18 Fällen.

In 94 Fällen waren die Beschwerden begründet.
Davon betrafen allein 65 Beschwerden ein Unternehmen der Direktmarketing- und Werbebranche. Die weiteren begründeten Eingaben richteten sich gegen Versicherungen und Banken, gegen Einzelhandelsunternehmen, gegen Stellen, die Personal- und Bewerberdaten verarbeiten, sowie in je einem Fall gegen die SCHUFA, ein Versandhandelsunternehmen, einen Mieterverein, eine Fluggesellschaft, eine politische Partei, einen Verein und ein Kreditkartenunternehmen.

Bei neun Eingaben an die Datenschutzaufsichtsbehörde im Berichtsjahr konnte der den Beschwerden zugrunde liegende Sachverhalt nicht mehr vollständig aufgeklärt werden, so daß eine abschließende Beurteilung, ob die Datenverarbeitung in zulässiger oder in unzulässiger Weise erfolgt war, nicht getroffen werden konnte.

In 31 Fällen sind die Ermittlungen der Aufsichtsbehörde noch nicht abgeschlossen.

Von den noch aus den Vorjahren anhängigen Beschwerden wurden 22 Fälle abgeschlossen. Die Beurteilung dieser in der Regel nur mit hohem Ermittlungsaufwand aufklärbaren Fälle durch die Aufsichtsbehörde ergab, daß davon acht Beschwerden begründet waren. Dabei hatten in je zwei Fällen Kreditinstitute und Versicherungen und in jeweils einem Fall eine Wirtschaftsauskunftei, ein Adreßhändler, ein Hospital und ein Einzelhandelsunternehmen personenbezogene Daten unzulässig verarbeitet oder genutzt.

Bei sieben 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 Überprüfungen von Stellen, die nach § 32 Abs. 2 Ziff. 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 1998 waren 705 meldepflichtige Unternehmen im Register der Aufsichtsbehörden eingetragen. Den größten Anteil hieran haben mit rund 80 v.H. der Meldungen die nach § 32 Abs. 1 Ziff. 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 rund 9 v.H. der Meldungen haben die nach § 32 Abs. 1 Ziff. 2 BDSG meldepflichtigen Unternehmen der Markt- und Meinungsforschung, die personenbezogene Daten zum Zwecke der anonymisierten Übermittlung speichern, den zweitgrößten Anteil am Melderegisterbestand.
Den geringsten Anteil haben die nach § 32 Abs. 1 Ziff. 1 BDSG gemeldeten Unternehmen, die personenbezogene Daten zum Zwecke der Übermittlung speichern.

### 2.2 Prüfungsübersicht

Im Berichtsjahr wurden 28 Prüfungen nach § 38 Abs. 2 BDSG durchgeführt. Davon betrafen Datenverarbeiter nach § 32 Abs. 1 Ziff. 3 BDSG insgesamt 25, nämlich

- Datenerfasser und Schreibbüros 7
- Telemarketingunternehmen 4
- Datenträgervernichter 3
- Adreßhändler 2
- Servicerechenzentren 2
- Konzerndatenverarbeiter 1
- Sonstige 6

Des weiteren wurden drei Unternehmen aus dem Bereich der Markt- und Meinungsforschung geprüft.

Die Prüfungen brachten folgendes Ergebnis:

- Beanstandungen 18
- Empfehlungen 6
- ohne wesentliche Beanstandungen 4

Folgende wesentliche Mängel wurden am häufigsten festgestellt:

1. keine bzw. verspätete oder unvollständige Registermeldung nach § 32 BDSG
2. keine bzw. unvollständige Weisungen des Auftraggebers nach § 11 BDSG
3. kein Datenschutzbeauftragter, Mängel in der Aus- und Fortbildung, Mängel in der Tätigkeit
4. fehlende bzw. unvollständige Dokumentation
5. mangelhafte Zugriffskontrolle, unzureichende Paßwortverwendung
6. unvollständige Zugangskontrolle, mangelhafte Datenträgerverwaltung

Zusätzlich zu den dargestellten 28 Überprüfungen vor Ort wurden 55 Überprüfungen auf schriftlichem Wege (mittels Fragebogen) durchgeführt. Insoweit wird auf die gesonderte Darstellung unter Nr. 2.3 verwiesen.

### 2.3 Datenschutzüberprüfung nach § 38 Abs. 2 BDSG bei Volksbanken

Volksbanken bieten Vereinen, deren Konten sie führen, auch eine Dienstleistung zur Mitgliederverwaltung an. Diese Auftragsdatenverarbeitung hat nach § 32 Abs. 1 Ziff. 3 BDSG zur Eintragung im Register der meldepflichtigen Stellen geführt.

Im Laufe der letzten Jahre hat es durch Fusionen und andere Veränderungen eine Reihe von entsprechenden Änderungsmitteilungen nach § 32 Abs. 4 BDSG gegeben.

Bei Überprüfungen nach § 38 Abs. 2 BDSG waren bisher nur wenige Volksbanken mit einbezogen worden, da die Auftragsdatenverarbeitung im Verhältnis zur eigentlichen Banktätigkeit nur einen relativ geringen Umfang einnimmt.

Die Überprüfung anderer Unternehmen wird als vorrangig angesehen.

Hinzu kommt, daß diese Dienstleistung für ortsansässige Vereine über ein zentrales Rechenzentrum der Volksbanken abgewickelt wird, so daß lediglich die Datenerfassung und die Überprüfung der Ergebnisse bei den einzelnen gemeldeten Volksbanken erfolgt.

Um jedoch zu verhindern, daß die Überprüfung nach § 38 Abs. 2 BDSG in diesem Bereich brach liegt, sind 55 Volksbanken mit einem Fragebogen angeschrieben worden.

Die Auswertung der Fragebögen, die, bis auf wenige Ausnahmen, rasch und vollständig ausgefüllt zurückkamen, bestätigte das bisherige positive Bild hinsichtlich der Datenverarbeitung durch die Volksbanken. Dies ist sicherlich auch dadurch bedingt, daß das System zentral verwaltet ist und somit eine gewisse Struktur vorgegeben ist. Auch werden vom Verband der Volksbanken Schulungen im Bereich Datenschutz und Datensicherheit angeboten, auf denen sich die Datenschutzbeauftragten entsprechend weiterbilden können. Bei den Zugriffsregelungen nutzen die meisten Banken das von der Zentrale vorgegebene System. Die Vergabe der Nutzungsrechte der einzelnen Mitarbeiter wird von den Datenschutzbeauftragten überwacht. In der Regel sind im Bereich der Auftragsdatenverarbeitung auch urlaubs- und krankheitsbedingte Vertretungen geregelt.

In wenigen Fällen mußte allerdings die mangelnde Fortbildung der Datenschutzbeauftragten beanstandet werden. Vereinzelt mußte die Bestellung eines Datenschutzbeauftragten beanstandet werden, weil dieser im Rahmen seines persönlichen beruflichen Aufstiegs inzwischen eine Position im Vorstand eingenommen hatte und somit nicht mehr Datenschutzbeauftragter sein konnte. Die Bestellung eines neuen Datenschutzbeauftragten wurde in diesen Fällen umgehend der Aufsichtsbehörde angezeigt.

## 3. Bearbeitung von Anfragen zu Problemen des Datenschutzes

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten mit Mitteln der modernen Informations- und Kommunikationstechnologie findet heute in fast allen Lebensbereichen statt.

Dies zeigt sich auch an der hohen Anzahl von 173 eingegangenen Anfragen beim Regierungspräsidium Darmstadt und der großen Bandbreite der Themen, zu denen die Datenschutzaufsichtsbehörde von betroffenen Bürgern, Datenschutzbeauftragten und Unternehmen um Rat und datenschutzrechtliche Stellungnahme gebeten wurde.

Zusätzlich zu den Fragestellungen aus den Bereichen Gesundheitswesen, Werbewirtschaft und Adreßhandel, Wirtschaftsauskunfteien, Banken, Versicherungen, Arbeitnehmerdatenschutz, Wohnen und Miete, Markt- und Meinungsforschung, Reisen und Touristik, Verkehr und den Problemen bei der Datenverarbeitung durch Dienstleistungsunternehmen, hatte die Aufsichtsbehörde branchenunabhängig einen Anstieg der Datenschutzfragen im Zusammenhang mit der gestiegenen Nutzung neuer Datenträger (CD-ROM) und neuer Kommunikationstechnologien und -strukturen (Internet) zu verzeichnen. Insbesondere die erhebliche Sicherheitsproblematik bei der Datenübermittlung via Internet führte verstärkt zu Fragen über geeignete sichere kryptographische Verfahren und die Abschottung von Unternehmensnetzen durch Firewallsysteme. (Firewall ist ein System, bestehend aus Software und Hardware, mit welchem das Eindringen Fremder, über die Vernetzung in das eigene Rechnersystem, verhindert werden soll.)

Ein weiterer zentraler Punkt der Beratungsaktivitäten der Aufsichtsbehörde war die Beurteilung der Zulässigkeit geplanter Datenverarbeitungsvorhaben von Konzernen, Einzelunternehmen und Vereinen, die im Regelfall über ihre betrieblichen Datenschutzbeauftragten anfragten. Diese Hilfestellung bei der datenschutzrechtlich unbedenklichen Ausgestaltung neuer automatisierter Verfahren kann helfen, kostenintensive Fehlinvestitionen der Unternehmen und später eventuell notwendige Korrekturmaßnahmen bereits im Vorfeld eines Projektes zu vermeiden. Unter Berücksichtigung des Aspekts der Eigenverantwortlichkeit der Unternehmen für die Gewährleistung datenschutzrechtlicher Standards können sich Hilfestellungen jedoch grundsätzlich nur auf die Beurteilung bereits erarbeiteter Grundkonzepte beziehen.

Die Tendenz zur Globalisierung wirtschaftlicher Beziehungen war bei den Fragen deutlich spürbar. So bezogen sich vermehrt Anfragen auf die datenschutzrechtlich oftmals problematische Übermittlung personenbezogener Daten von Kunden oder Arbeitnehmern ins Ausland.

Zahlreiche Vereine, die sportliche, kulturelle, soziale und andere Ziele verfolgen, benötigen dazu je nach Vereinszweck die unterschiedlichsten Daten ihrer Mitglieder und gegebenenfalls auch weiterer Personen. Da diese Daten auch in Vereinen fast vollständig automatisiert und damit dateimäßig verarbeitet werden, hat die Aufsichtsbehörde im Berichtsjahr einen weiteren Schwerpunkt auf die Beratung und Information dieser Stellen und vor allem ihrer hessischen Spitzenverbände gelegt. Gesprächsangebote und Informationsmaterial wurden von den Dachorganisationen der Vereine positiv aufgenommen. In der Folge wurden auch die kommunalen Spitzenverbände entsprechend informiert und mit Material ausgestattet. Die Aufsichtsbehörde verbindet damit die Erwartung, daß diese Stellen die Informationen weitergeben und damit zur Gewährleistung der Sicherheit und Ordnungsmäßigkeit der Verarbeitung personenbezogener Daten in Vereinen beitragen.

## 4. Banken

### 4.1 Datenerhebung bei der Kontoeröffnung

Nicht nur beim Kreditkartenantrag (vgl. 10. Tätigkeitsbericht, 6.2), sondern auch bei der Girokontoeröffnung versuchen Banken, möglichst viel vom neuen Kunden zu erfahren und diese Kenntnisse für die unterschiedlichen Geschäftsfelder zu nutzen.

Diese Datenerhebungen sind teilweise notwendig und auch gesetzlich vorgeschrieben (Kreditwesengesetz). Allerdings werden nach Feststellung der Aufsichtsbehörde oftmals erheblich mehr Daten erhoben, als im Einzelfall tatsächlich für die Vertragsabwicklung erforderlich sind.

Schon jetzt erfordert es der Grundsatz von Treu und Glauben (vgl. § 28 Abs. 1 letzter Satz BDSG), daß der Kunde erkennen kann, welche Daten für den einzelnen Vertrag notwendig sind und welche Daten von ihm lediglich freiwillig genannt werden können. Nach der Novellierung des Bundesdatenschutzgesetzes entsprechend der EG-Datenschutzrichtlinie werden hier insgesamt schärfere Maßstäbe anzulegen sein.

Es empfiehlt sich deshalb, beim Entwurf von Datenerhebungsformularen eindeutig zwischen notwendigen und freiwilligen Daten zu unterscheiden. Zumindest müßten entsprechende mündliche Erläuterungen gegeben werden. Ebenso sollte bereits auf dem Formular, zumindest aber mündlich, auf die Zweckbestimmung der Daten hingewiesen werden.

### 4.2 Datenerhebung nach dem Wertpapierhandelsgesetz

Auch beim Wertpapierkauf werden Datenerhebungen häufig zu großzügig vorgenommen. Für den Kauf von mündelsicheren Anleihen werden in der Regel keine genauen Analysen der Vermögensverhältnisse des Anlegers erforderlich sein.

Eine Bank im Aufsichtsbereich hat die Problematik insoweit gut gelöst, als sie die verschiedenen Anlagen in Risikoklassen einteilt und auch die Risikoabsichten des Anlegers erfaßt. Abhängig vom jeweiligen Risiko wird dann der Informationsbedarf näher benannt.

Eine umfassende Wertpapierberatung kann natürlich nur erfolgen, wenn der Berater die finanziellen Verhältnisse seines Kunden näher kennt. Nur so kann definiert werden, in welchem Umfang die einzelnen Engagements abgesichert werden müssen. Diese Erfordernisse und die Vorschriften des Wertpapierhandelsgesetzes gehen jedoch nicht so weit, daß der Kunde gezwungen ist (wird), seine finanziellen Verhältnisse offenzulegen. Es wurde von Betroffenen mehrfach berichtet, daß sogar der Kauf von Bundesobligationen verweigert wurde, wenn der Kunde nicht zu Auskünften bereit war.

Es ist zu begrüßen, wenn statt dessen auf dem Datenerhebungsbogen der Bank auf die Freiwilligkeit der Einzelangaben zu den Vermögensverhältnissen hingewiesen wird. Eine andere Form der Datenerhebung würde gegen Treu und Glauben verstoßen (§ 28 Abs. 1 letzter Satz BDSG).

### 4.3 Erteilung von Bankauskünften an den Ehepartner

Personenbezogene Daten über die Vermögensverhältnisse sind bei Ehestreitigkeiten von besonderer Bedeutung. In einem Fall hatte die getrennt lebende Ehefrau zwei Depotauszüge von den Banken des Ehemannes erhalten, obwohl angeblich keine Kontovollmacht mehr bestand. Bei der ersten Bank konnte nicht mehr festgestellt werden, welcher Mitarbeiter den Depotauszug erstellt hatte. Die zweite Bank legte eine neue Vollmacht für die Ehefrau vor, die vom betroffenen Ehemann bestritten wurde. Er erstattete Strafanzeige nach § 43 BDSG und wegen Urkundenfälschung, leider teilte er das Ergebnis des Strafverfahrens nicht mit.

Die betreffenden Banken haben aus den Beschwerden die Konsequenz gezogen, daß die Bankbeschäftigten nochmals auf das Bankgeheimnis und eventuelle strafrechtliche Konsequenzen nach dem Bundesdatenschutzgesetz hingewiesen wurden.

Nicht autorisierte Auskünfte lassen sich grundsätzlich nur durch solche organisatorischen Maßnahmen eingrenzen, da Wertpapierberater natürlich darauf angewiesen sind, jederzeit für Beratungszwecke auf die Depotbestände ihrer Kunden zugreifen zu können.

### 4.4 Einholung von Bankauskünften über einen im Unternehmen tätigen Ehepartner

Der Beschwerdeführer hatte als Unternehmer Konkurs beantragen müssen und arbeitete nun in einem vergleichbaren Unternehmen der Ehefrau. Seine als Mithilfe verstandene Tätigkeit umfaßte auch Kreditverhandlungen mit der Hausbank der Ehefrau.

Der beantragte Kredit wurde abgelehnt, wobei der Ehemann vermutete, daß sein negativer Kreditruf die Absage der Bank für das Unternehmen der Ehefrau verursacht habe. Die Bank - so vermutete der Beschwerdeführer - habe über ihn unzulässigerweise Auskünfte eingeholt, obwohl ausschließlich seine Ehefrau die potentielle Kreditnehmerin sei.

Die Nachprüfungen ergaben, daß über den Ehemann keine Auskünfte eingeholt worden waren.

Allerdings war zu berücksichtigen, daß der Ehemann offenbar eine führende Rolle im Unternehmen der Ehefrau spielte. Die Kreditverhandlungen sind ein Beispiel hierfür. Es wäre für die Bank deshalb durchaus auch von Bedeutung gewesen, zu erfahren, welchen Kreditruf der Ehemann hatte, weil dessen einflußreiche - einem Geschäftsführer vergleichbare Stellung - die Geschicke des Unternehmens erheblich beeinflussen kann. In diesem Einzelfall wäre die Bank deshalb sogar berechtigt gewesen, auch über den Ehemann Auskünfte einzuholen.

Der Fall verdeutlicht jedoch die Schwierigkeit der Abwägung der berechtigten Interessen des Kreditgebers mit den schutzwürdigen Belangen des Betroffenen. Häufig verfügt der Kreditgeber gar nicht über ausreichende Informationen, um wirklich beurteilen zu können, ob hier schutzwürdige Belange beeinträchtigt sein könnten. Es ist deshalb notwendig, erst die näheren Umstände beim Kreditnehmer zu klären und danach eventuell weitere personenbezogene Auskünfte einzuholen.

### 4.5 Organisation der Anfragen an Auskunfteien bei einer Bank

Unzureichende Gesetzeskunde verrieten die verantwortlichen Mitarbeiter einer Bank hinsichtlich der Vorschrift des § 29 Abs. 2 Nr. 1a BDSG, welche die Zulässigkeit einer Datenübermittlung von der glaubhaften Darlegung des berechtigten Interesses des Empfängers abhängig macht.

Bei Auskunftsersuchen an Auskunfteien wurde automatisch vom Anwendungsprogramm für solche Auskunftsersuchen als berechtigtes Interesse immer das gleiche, nämlich "Geschäftsanbahnung", eingetragen und an die Auskunfteien weitergegeben. Auch wenn tatsächlich in einer Bank häufig das gleiche berechtigte Interesse für Auskunftsersuchen vorliegt, so ändert dies nichts daran, daß eine individuelle Bearbeitung und Überprüfung erforderlich ist und das berechtigte Interesse exakt dem jeweiligen Anfragegrund entsprechen muß. Das Unternehmen wurde aufgefordert, das Verfahren entsprechend zu ändern.

Der leichtfertige Umgang mit Betroffenendaten im Hinblick auf Anfragen bei Auskunfteien spiegelte sich auch darin wider, daß beliebige Mitarbeiter eine Anfrage an eine Auskunftei über die zuständige Sachbearbeitung der Bank richten konnten. Noch erstaunlicher aber war, daß die interne Revision der Bank das Verfahren zunächst nicht für überdenkenswert hielt, obwohl sich herausstellte, daß eine Mitarbeiterin, die nach ihrem Aufgabengebiet an sich überhaupt nicht hätte autorisiert sein dürfen, die Einholung von Auskünften zu verlangen, Anfragen zu privaten Zwecken veranlaßt hatte. Die Beschwerde des Betroffenen hatte die Aufsichtsbehörde zur Überprüfung veranlaßt und damit zur Aufdeckung der Mißstände geführt. Es zeigten sich also sowohl bei der Revision als auch beim Datenschutzbeauftragten, der das Verfahren ebenfalls gebilligt hatte, Wissenslücken hinsichtlich der Vorschriften zum Datenschutz und zur Datensicherheit.

## 5. Schufa

### 5.1 Entgelt für die SCHUFA Auskunft

Die (Selbst-)Auskunft an den Betroffenen ist grundsätzlich unentgeltlich, vgl. § 34 Abs. 5 Satz 1 BDSG.

Im Falle der SCHUFA werden die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert. Der Betroffene kann in der Regel die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen. Die SCHUFA darf deshalb nach § 34 Abs. 5 Satz 2 BDSG ein Entgelt für die Auskunftserteilung verlangen. Die Höhe dieses Entgeltes darf die direkt zurechenbaren Kosten nicht überschreiten.

Ist die Auskunftserteilung jedoch nicht unentgeltlich, so muß dem Betroffenen nach § 34 Abs. 6 Satz 1 BDSG die Möglichkeit gegeben werden, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis zu verschaffen. Der Betroffene ist vorher in geeigneter Weise hierauf hinzuweisen, vgl. § 34 Abs. 6 BDSG.

In der jeweiligen SCHUFA Geschäftsstelle kann der Betroffene gratis mündliche Auskünfte erhalten, der zusätzliche Ausdruck der Daten wird jedoch mit einem Entgelt in Rechnung gestellt.

Ein Beschwerdeführer wies darauf hin, daß er von der SCHUFA aber weder einen Hinweis auf die Möglichkeit einer unentgeltlichen mündlichen Auskunft noch auf die Entgeltpflicht bei schriftlicher Auskunftsart erhalten habe. Mit der Auskunft sei ihm vielmehr zugleich die Rechnung übersandt worden.

Die berechtigte Beschwerde veranlaßte die SCHUFA, in diesem Einzelfall auf ein Entgelt zu verzichten. Für zukünftige Fälle wurde die Informationsbroschüre der SCHUFA überarbeitet; es wird damit vorab auf die Entgeltpflicht hingewiesen.

### 5.2 Speicherung von Widersprüchen trotz Bezahlung

Bei der SCHUFA wurde ein Mahnbescheid und der Widerspruch des Betroffenen eingetragen. In der Folge einigte sich der Schuldner mit seinem Gläubiger im Wege des Vergleiches und bezahlte den überwiegenden Teil der Forderung.

Der Gläubiger meldete daraufhin den Kontoausgleich an die SCHUFA.

Bei der Eintragung des Kontoausgleichs wurde dieses Datum von der SCHUFA automatisch als Anerkenntnis der Forderung gewertet und der vorherige Widerspruch des Schuldners gelöscht. Die Datenspeicherung gibt insoweit generell nur noch verkürzt die tatsächlichen Abläufe wieder.

Die von Betroffenen in solchen Fällen gewünschte vollständige Löschung des Negativmerkmals wird von der SCHUFA allgemein nicht vollzogen. Da die SCHUFA - von Kommentarzeilen abgesehen - keine differenzierte Darstellungsmöglichkeit des vollständigen Ablaufs vorsieht, begehrte der Betroffene jedoch zumindest die Wieder-Eintragung seines Widerspruchs. Diese berechtigte Forderung erledigte sich lediglich dadurch, daß durch den Zeitablauf die Negativdaten automatisch gelöscht wurden.

Zu berücksichtigen ist, daß viele Schuldner erst einmal gegenüber ihren Gläubigern die Forderungen bestreiten und versuchen, einen Zahlungsaufschub zu erreichen, obwohl die vorgebrachten Gründe - zumindest bei den Bankforderungen - in der Regel nicht anerkannt werden können.

Wenn aber, wie im geschilderten Fall, das Bestreiten der Forderung zumindest teilweise Erfolg hat und der Schuldner nur einen Teilbetrag zahlen muß, so ist auch diese Tatsache zusätzlich zur Zahlung zu speichern. Die Differenz zwischen Forderungsbetrag und Zahlungsbetrag relativiert den Sachverhalt für einen Auskunftsempfänger dahingehend, daß er erkennen kann, in welchem Umfang tatsächlich Zahlungen hinausgezögert wurden.

### 5.3 Adressenspeicherung über mehr als 10 Jahre

Ein Koch wechselte berufsbedingt sehr häufig seinen Wohnort; seine jeweiligen Adressen wurden bei der SCHUFA von 1980 bis 1997 fortlaufend aufgezeichnet. Gläubiger konnten so jederzeit den Aufenthaltsort des Betroffenen feststellen. Finanzielle Schwierigkeiten, die Ende der Neunziger Jahre mit einer eidesstattlichen Versicherung dokumentiert wurden, belegten, daß hier durchaus für Gläubiger auch ein berechtigtes Interesse an der Wohnortfeststellung bestand.

Bei der Abwägung zwischen den berechtigten Interessen der Gläubiger einerseits und den schutzwürdigen Belangen des Betroffenen andererseits konnten jedoch keine Anhaltspunkte dafür gefunden werden, daß die Adreßaufzeichnung über einen Zeitraum von 17 Jahren wirklich notwendig war. Sobald ein Gläubiger mit Zugriffsberechtigung auf die SCHUFA-Daten den Schuldner aus dem Auge verliert, kann er mit einem Suchauftrag die aktuelle Adresse erfahren.

Ältere Forderungen waren nicht dokumentiert; die Aufzeichnung der zurückliegenden Adressen über einen Zeitraum von 5 Jahren erschien als völlig ausreichend. Die SCHUFA Niederlassung Frankfurt hat daraufhin auch umgehend alle älteren Adressen gelöscht.

Insgesamt konnte positiv festgestellt werden, daß die SCHUFA bemüht ist, auch den Interessen der persönlich Betroffenen zu entsprechen.

## 6. Auskunfteien

### 6.1 Datenverarbeitung einer Auskunftei in der europäischen Union

Die Internationalisierung der Datenverarbeitung ist ein Trend, der schon seit einigen Jahren zu beobachten ist. Mit der absehbaren Umsetzung der europäischen Datenschutzrichtlinie wird der Gesetzgeber diesen Entwicklungen teilweise Rechnung tragen. Langfristig ist eine Harmonisierung der Datenschutzvorschriften aller Industriestaaten erstrebenswert.

Eine große Auskunftei hat den überwiegenden Teil der Datenverarbeitung in ein Mitgliedsland der Europäischen Union verlagert. Die Kontrolle über die Datenbestände, die Auskunft an den Betroffenen, die Fortschreibung der Daten, die Sperre, die Korrektur und Löschung der Daten verbleiben aber weiterhin bei der Auskunftei in Deutschland. Den persönlich Betroffenen entstehen deshalb keine Nachteile durch zeitliche Verzögerungen oder sprachliche Barrieren. Der Sicherheitsstandard in dem genannten Unternehmen ist allgemein hoch; die internationale Konzernrevision leistet nach den eingesehenen Prüfberichten eine gründliche Datenverarbeitungskontrolle. Es ist deshalb auch von einer sicheren Datenverarbeitungsumgebung auszugehen. Bei dem derzeitigen Geschäftsablauf waren bisher keine größeren Probleme feststellbar. In besonderen Fällen wäre es zusätzlich möglich, die nationale Datenschutzaufsichtsbehörde in dem jeweiligen EU-Partnerland auf Kontrollerfordernisse hinzuweisen und auf eine Verbesserung des Datenschutzstandards hinzuwirken.

### 6.2 CD-ROM mit Unternehmensprofilen

Eine Wirtschaftsauskunftei stellte Erwägungen an, eine CD-ROM mit Unternehmensprofilen "Kreditregister" zu vertreiben und bat um Stellungnahme aus datenschutzrechtlicher Sicht.

Dabei wies die Auskunftei darauf hin, daß der Zeitfaktor bei geschäftlichen Transaktionen eine immer größere Rolle spiele, weshalb der Kunde zur Absicherung einer Kreditentscheidung oftmals sofort Wirtschaftsinformationen benötige und ihm mit der schriftlichen Einholung einer Wirtschaftsauskunft nicht mehr gedient sei. Neben dem bereits bestehenden Online-Verfahren beabsichtigte die Auskunftei daher den Vertrieb einer CD-ROM. Der Kunde sollte von dieser CD-ROM jederzeit selbst Unternehmensprofile mit Bonitätsbewertungen abfragen können.

Dabei sollte der Kunde vor Zugriff auf die Einzelinformation in einer besonderen Maske dazu aufgefordert werden, sein berechtigtes Interesse anzugeben.
Durch Allgemeine Geschäftsbedingungen solle der Kunde verpflichtet werden, wahrheitsgemäße Angaben zu machen und einen Abruf von Informationen nur dann vorzunehmen, wenn ein berechtigtes Interesse i.S.d. § 29 BDSG im konkreten Einzelfall gegeben ist.
Sollten sich Daten, die auf der CD-ROM gespeichert sind, als nicht (mehr) zutreffend erweisen, so sollte die dann bestehende gesetzliche Berichtigungspflicht nach § 35 Abs. 1 BDSG und die entsprechende Unterrichtungspflicht nach § 35 Abs. 6 BDSG nach den Vorstellungen der Auskunftei in der folgenden Weise erfüllt werden: Den CD-ROM-Nutzern sollten in regelmäßigen Abständen Schreiben zugesandt werden, in welchen die Auskunftei - nur unter Angabe einer Kennummer, nicht der Firmierung des Unternehmens - darüber informiert, daß die betreffenden Wirtschaftsinformationen widerrufen würden.

Hinsichtlich der Erfüllung der Auskunftspflicht nach § 34 BDSG hatte die Auskunftei erwogen, den Betroffenen eine Liste aller CD-ROM-Kunden auszuhändigen.

Trotz dieser beabsichtigten Vorkehrungen und Verfahrensweisen wurde der Vertrieb einer solchen CD-ROM als unzulässig bewertet, soweit darauf Daten von natürlichen Personen gespeichert sind, was bei Einzelpersonen-Unternehmen (beispielsweise bei der Ein-Mann-GmbH) der Fall wäre.

Die Voraussetzungen des § 29 BDSG für die geschäftsmäßige Übermittlung personenbezogener Daten sind nicht erfüllt: Es ist nicht gewährleistet, daß ein Zugriff auf die gespeicherten Informationen nur erfolgt, wenn ein berechtigtes Interesse an der konkreten Information auch tatsächlich vorliegt.

Das geplante Verfahren weist zwar Parallelen zu dem in § 10 BDSG geregelten automatisierten Abrufverfahren (Online-Abfragen) auf, bei dem auf eine vorherige Überprüfung des berechtigten Interesses verzichtet wird. Aber die Anforderungen des § 10 Abs. 2 BDSG, wonach die beteiligten Stellen durch geeignete Maßnahmen sicherzustellen haben, daß die Zulässigkeit des automatisierten Abrufs kontrolliert werden kann, werden nicht erfüllt: Da die CD-ROM nicht nachträglich beschreibbar ist, kann bei einem konkreten Abruf auch nicht dokumentiert werden, welches berechtigte Interesse der Nutzer angegeben hat. Infolgedessen kann auch nicht mehr kontrolliert werden, ob einem Abruf tatsächlich ein berechtigtes Interesse zugrunde lag.

Auf eine Bewertung der vorgesehenen Verfahren zur Erfüllung der Betroffenenrechte (Berichtigung, Auskunft) kam es nicht mehr an, da bereits die Voraussetzungen des § 29 BDSG nicht erfüllt sind.

Die Auskunftei teilte mit, sie habe den Datenbestand auf der CD-ROM entsprechend der Forderung der Aufsichtsbehörde reduziert. Ob die CD-ROM letztlich auf den Markt gebracht werden wird, war noch offen.

### 6.3 Erfinden von Daten

Auf eine besonders dreiste Methode der Datenerhebung durch eine Handels- und Wirtschaftsauskunftei im Regierungsbezirk Darmstadt wurde die Aufsichtsbehörde durch die Eingabe der Geschäftsführerin eines kleinen Datenerfassungsgewerbes aufmerksam.

Der Auskunftei waren lediglich Name und Anschrift des Betriebes und der Geschäftsführerin bekannt. Um nun auch schnell und günstig die für eine am Markt verwertbare Auskunft benötigten Bonitätsdaten (z.B. Umsatz, Bilanzzahlen, Verbindlichkeiten) zu erfahren, wurde die Gewerbetreibende gebeten, der Auskunftei die gewünschten Daten selbst freiwillig mitzuteilen. Bis zu diesem Punkt ist dieses Verfahren im Bereich der Handelsauskunfteien durchaus üblich.

Unüblich und datenschutzrechtlich unzulässig ist es allerdings, dieser Bitte dadurch Nachdruck zu verleihen, daß dem Schreiben eine komplett erfun-

dene Bonitätsauskunft zu dem Datenerfassungsbetrieb beigefügt wurde. Dies erfolgte mit der Aufforderung, die vollkommen aus der Luft gegriffenen gespeicherten Daten zu ergänzen bzw. zu korrigieren. Die Auskunftei war offensichtlich der Ansicht, daß der Anblick der unrichtigen Angaben zur Branche, den Betriebsräumen, den Mitarbeitern, dem Jahresumsatz, den Aktiva und Passiva und der Zahlungsweise, die ansonsten auskunftsunwillige Geschäftsführerin des Unternehmens motivieren könnte, die korrekten Daten mitzuteilen. Der Auskunftei wären auf diese Weise aufwendige Ermittlungsarbeiten erspart geblieben.

Die Aufsichtsbehörde hat die Wirtschaftsauskunftei auf die Unzulässigkeit dieses Vorgehens hingewiesen und das Unternehmen aufgefordert, die unrichtigen und bestrittenen Daten bis zu einer eventuellen Berichtigung des Datenbestandes nach § 35 Abs. 4 BDSG zu sperren oder auf Dauer zu löschen. Die anfragenden Firmen, an die bereits falsche Daten zu dem Datenerfassungsbetrieb übermittelt wurden, erhielten nach § 35 Abs. 6 BDSG einen entsprechenden Nachtrag.

## 7. Werbewirtschaft

### 7.1 Bundesweite Befragungen

Eine bundesweit durchgeführte Haushaltsbefragung eines hier ansässigen Unternehmens führte - ebenso wie die fast zeitgleich durchgeführte Befragung eines Unternehmens aus Baden-Württemberg - zu zahlreichen Eingaben von Bürgerinnen und Bürgern. Auch die Medien interessierten sich sehr für die datenschutzrechtliche Bewertung der Aufsichtsbehörde und beschäftigten sich ausgiebig mit der Thematik.

Bei der Befragungsaktion wurden mittels eines per Postwurf zugestellten Fragebogens detailliert Lebensumstände und Lebensgewohnheiten erfragt, wie beispielsweise die Einkommens- und Vermögensverhältnisse, die Ausbildungs- und Berufssituation, die Wohnverhältnisse, die Familiensituation, die regelmäßigen Freizeitaktivitäten, die Lese- und Fernsehkonsumgewohnheiten, die Verwendung einzelner Produkte, die Teilnahme an Lotteriespielen, die Spendenbereitschaft und die Kundenbeziehungen zu Banken und Versicherungen.

In der Vergangenheit wurden Verbraucherbefragungen vorwiegend für Zwecke der Markt- und Meinungsforschung durchgeführt, bei der die Daten ausschließlich anonymisiert verwendet werden, d.h. die Auswertungsergebnisse enthalten keinen Personenbezug.
Die anonymisierte Verwendung sollte nach Äußerungen des Unternehmens auch der Hauptzweck der bundesweiten Haushaltsbefragung sein, allerdings war darüber hinaus eine personenbezogene Weitergabe der allermeisten Daten für Direktmarketingzwecke beabsichtigt. Die Befragung diente also der Beschaffung differenziert auswertbaren Adreßmaterials, mit dessen Hilfe potentielle Verbraucher möglichst zielgenau beworben werden können.

Aus datenschutzrechtlicher Sicht sind an solche Umfragen im wesentlichen folgende Anforderungen zu stellen:

- Es muß klar erkennbar sein, daß die Angaben nicht nur anonym, sondern auch personenbezogen ausgewertet werden.

- Es muß ferner erkennbar sein, für welche Zwecke die Angaben verwendet werden, z.B. für persönlich adressierte Werbung.

- Weiter muß eine unterschriebene Einwilligung auf dem Fragebogen erfolgen, und zwar von allen volljährigen bzw. einsichtsfähigen Betroffenen.

Diese Rechtsauffassung ist mit allen obersten Aufsichtsbehörden der Länder abgestimmt.

Die im Januar veröffentlichten BDSG-Hinweise des Innenministeriums Baden-Württemberg, in dessen Zuständigkeit das andere Unternehmen fällt,

enthalten weitere Präzisierungen dieser Anforderungen (Staatsanzeiger Nr. 2 vom 19. Januar 1998, S. 7).

Das Erfordernis einer klaren und verständlichen Information über die beabsichtigte personenbezogene Verwendung für persönlich adressierte Werbung ergibt sich aus dem bei Datenerhebungen zu beachtenden Grundsatz von Treu und Glauben (§ 28 Abs. 1 Satz 2 und § 29 Abs. 1 Satz 2 BDSG).

Das Erfordernis einer unterschriebenen Einwilligung ergibt sich daraus, daß keine gesetzliche Erlaubnis für die Verarbeitung und Nutzung besteht:

§ 29 BDSG ist nämlich keine ausreichende Rechtsgrundlage für die Speicherung, Übermittlung und Nutzung von Daten, wenn es sich um sensible Daten handelt oder wenn sich aus der Gesamtheit der erfragten Lebensumstände, Fähigkeiten, Neigungen, Einstellungen und Konsumgewohnheiten ein relativ detailliertes Gesamtbild der Persönlichkeit der Befragten im Sinne eines Persönlichkeitsprofiles erstellen läßt. Daher ist die Speicherung, Übermittlung und Nutzung der Daten nur auf der Grundlage einer Einwilligung der Betroffenen zulässig.

Die genannten Anforderungen wurden von der Haushaltsumfrage des hier ansässigen Unternehmens nicht in allen Punkten erfüllt. Jedenfalls sah der Fragebogen keine Einwilligung vor. Auch hinsichtlich der erforderlichen Aufklärung über die Verwendungszwecke bestand Anlaß zur Kritik.

Veranlaßt durch zahlreiche Bürger- und Medienanfragen, hat sich die Aufsichtsbehörde öffentlich zu der Angelegenheit geäußert; unter anderem hat sie eine Presseerklärung herausgegeben, in der sie über ihre rechtliche Bewertung informierte.

Die Beschwerdeführer wurden von der Aufsichtsbehörde im übrigen darauf hingewiesen, daß Betroffene ihre Rechte selbst geltend machen müssen, da die Aufsichtsbehörde in solchen Fällen auf die argumentative Auseinandersetzung mit dem Unternehmen angewiesen ist und keine Anordnungsbefugnisse o.ä. hat. Diejenigen, die den Fragebogen bereits ausgefüllt hatten, wurden auf das Widerspruchsrecht nach § 29 Abs. 3 BDSG i.V.m. § 28 Abs. 3 BDSG aufmerksam gemacht, auf welches allerdings auch das Unternehmen schon hingewiesen hatte.
Wenn ein Betroffener nach § 28 Abs. 3 BDSG der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung bzw. der Markt- und Meinungsforschung widerspricht, hat dies zur Folge, daß die Verwendung der Daten für die genannten Zwecke unzulässig ist. Die - vorsorgliche - Einlegung eines solchen Widerspruchs wurde den Betroffenen empfohlen, obwohl das Unternehmen nach Auffassung der Aufsichtsbehörde - wie oben dargelegt - eine vorherige Einwilligung hätte einholen müssen.

Das Unternehmen teilt die oben dargelegte Rechtsauffassung nicht. In Gesprächen mit der Aufsichtsbehörde wurden die gegensätzlichen Rechtsstandpunkte erörtert. Bei Abfassung dieses Berichts war noch keine Einigung erzielt.

Mittlerweile hat der Verbraucherschutzverein Berlin - wie aus dessen Presseverlautbarungen bekannt wurde - eine wettbewerbsrechtliche Unterlassungsklage gegen das Unternehmen erhoben und diese mit den datenschutzrechtlichen Vorschriften begründet. Die Entscheidung des Gerichts bleibt abzuwarten.

### 7.2 Nichtbeachtung von Widersprüchen gegen die Nutzung von Daten zu Werbezwecken

Auch in diesem Berichtsjahr wurden der Aufsichtsbehörde Beschwerden von Empfängern unverlangter Werbezusendungen gegen Unternehmen vorgetragen, die den Widerspruch der Betroffenen gegen die werbliche Nutzung der Empfängeranschrift im Sinne des § 28 Abs. 3 BDSG nicht beachteten. Die mehrfachen Protestschreiben der umworbenen Bürgerinnen und Bürger mit der Aufforderung, die unverlangte Zusendung von Werbematerial doch nun endlich einzustellen, wurden in vielen Fällen trotz der Drohung, die Aufsichtsbehörde einzuschalten, nicht beachtet.

Die werbenden Unternehmen stammten aus den unterschiedlichsten Branchen. Sowohl Versandhäuser und Versicherungen als auch kleinere Dienstleister und Einzelhandelsunternehmen waren betroffen. Alle Unternehmen reagierten allerdings umgehend auf die Hinweise und Forderungen der Aufsichtsbehörde.

In einem Versandhandelsunternehmen konnte so ein technischer Fehler im Adreßverwaltungssystem entdeckt und beseitigt werden, der dazu geführt hatte, daß unter bestimmten Bedingungen trotz gesetzter Werbesperre weiterhin Werbematerial versandt wurde. Bei einer Versicherung, die zunächst einer Bürgerin die Beachtung des Werbewiderspruchs und die Löschung ihrer Daten zugesagt hatte, danach aber dennoch weiterhin Werbematerial versandte, führte die Beschwerde zu einer Überprüfung der Beschwerdebearbeitung und des EDV-Systems und einer nochmaligen Schulung der Mitarbeiter. Ein großes Möbelhaus erklärte sich auf Verlangen der Aufsichtsbehörde bereit, eine eigene Sperrdatei einzurichten und diese regelmäßig gegen angemietete Adreßdateien des Adreßhandels abzugleichen.

Bei einem Hilfsunternehmen der Presse, das die Betreuung von Zeitschriftenabonnements und den Vertrieb der Presseerzeugnisse abwickelt, wurde der Widerspruch des Betroffenen gegen die unverlangte Werbung von der Marketingabteilung mißachtet und nie dem betrieblichen Datenschutzbeauftragten vorgelegt.

Diese Konstellation, die nicht selten bei werbenden Unternehmen anzutreffen ist, macht deutlich, daß die betrieblichen Datenschutzbeauftragten oftmals unter erschwerten Bedingungen und in ständiger Auseinandersetzung mit anderen marktorientierten Fachabteilungen ihres Unternehmens ihren gesetzlichen Pflichten nachkommen müssen. Die Aufsichtsbehörde versucht in diesen Fällen regelmäßig, bei den verantwortlichen Geschäftsführern der Unternehmen der Stimme der betrieblichen Datenschutzbeauftragten mehr Gehör zu verschaffen.

### 7.3 Mangelhafte Erteilung von Auskünften über die Herkunft von Adreßdaten

Nach § 34 Abs. 1 BDSG haben Betroffene das Recht, von der speichernden Stelle Auskunft über die zu ihrer Person gespeicherten Daten und deren Herkunft zu verlangen. Auch diese gesetzliche Regelung wird, ähnlich wie der Widerspruch gegen die werbliche Nutzung der Adreßdaten nach § 28 Abs. 3 BDSG (s.o.), von einigen werbenden Unternehmen nicht ernst genommen und ist in diesen Fällen leider nur mit Unterstützung der Aufsichtsbehörde durchsetzbar. Dieses Phänomen ist vereinzelt auch bei großen und gut organisierten Unternehmen zu beobachten, was im Berichtsjahr unter anderem die Beschwerden gegen eine Bank und ein Kreditkartenunternehmen zeigten.

Auch hier war festzustellen, daß die Schreiben der Bürgerinnen und Bürger nicht immer den zuständigen betrieblichen Datenschutzbeauftragten in den Unternehmen vorgelegt werden, da die Auskunftssuchenden ihre Anfragen fast immer an die Fachabteilungen "Kundenbetreuung" oder "Marketing" adressieren, die als Absender auf den Werbesendungen angegeben sind. In diesen eher kaufmännisch orientierten Abteilungen der Unternehmen ist nicht immer die erforderliche Sensibilität für datenschutzrechtliche Problemstellungen vorhanden.

Die betrieblichen Datenschutzbeauftragten der Bank und des Kreditkartenunternehmens haben dieses Problem erkannt und der Aufsichtsbehörde sowohl geeignete organisatorische Maßnahmen zur Optimierung der Bearbeitung datenschutzrechtlicher Beschwerden als auch eine intensivere Schulung der betroffenen Mitarbeiter zugesagt.

Betroffenen ist in diesem Zusammenhang allgemein zu empfehlen, sich gleich direkt an den betrieblichen Datenschutzbeauftragten des auskunftspflichtigen Unternehmens zu wenden.

### 7.4 Unglückliche, problematische und unzulässige Werbekonzeptionen

Die an die Aufsichtsbehörde im Berichtsjahr herangetragenen Beschwerden zeigen, daß viele Unternehmen heute versuchen, die weitere Bindung ihrer Kunden mit Hilfe professioneller Dienstleister aus dem Direktmarketingbereich zu optimieren. Diese Marketingexperten stellen sich dabei mit viel Phantasie ihrer Aufgabe. Leider werden die datenschutzrechtlichen Aspekte dieser Tätigkeit, die eben nicht nur mit einem perfekten Werbelayout, sondern auch mit der Verwendung personenbezogener Daten der Kunden verbunden ist, von den Marketingagenturen oftmals ungenügend berücksichtigt.

Die Kundin einer Bank beschwerte sich darüber, daß ihr die Höhe ihrer Erträge aus einer Geldanlage in einem Investmentfond in einem Werbeschreiben mitgeteilt wurde. Dieses Schreiben der Bank war wie die übliche Massenwerbung gestaltet und somit als konkrete Bankmitteilung kaum zu erkennen. Die Kundin befürchtete, daß dieses Schreiben beim oberflächlichen Postsortieren ausgesondert und so in den Papierkorb oder sogar in die Hände Unberechtigter gelangen könne. Die Datenschutzaufsichtsbehörde konnte jedoch keine Verletzung des Bankgeheimnisses oder des BDSG feststellen, da das Schreiben an die Bankkundin in einem verschlossenen Umschlag zugestellt wurde und keine unzulässige Datenübermittlung an Dritte durch das Unternehmen vorlag. Gestaltung und Layout des Werbeschreibens waren zwar unglücklich gewählt, dies war datenschutzrechtlich allerdings nicht relevant.
In einem weiteren Fall hatte der Kunde eines Autohauses festgestellt, daß auf dem Versandaufkleber der Kundenzeitschrift neben seiner Anschrift auch eine verkürzte Form der Fahrgestellnummer seines Fahrzeuges angebracht war. Die Verwaltung und Pflege der Kundenanschriften und die Versendung der Kundenzeitschrift erfolgte durch einen externen Dienstleister, der die Fahrgestellnummer zur einfachen Identifikation von Versand-Rückläufern nutzte. Nach der Beanstandung dieser Versendepraxis durch die Aufsichtsbehörde wurde das Verfahren umgestellt.
Die Datenschutzorganisation des Unternehmens wurde als Folge der Beschwerde vor Ort überprüft. Bei der Auftragsvergabe an das externe Mailing-Unternehmen war offensichtlich nicht geprüft worden, ob der Auftragnehmer seinen Meldepflichten nach § 32 BDSG nachgekommen war. Der nicht gemeldete Dienstleister wurde nachträglich in das Register der nach § 32 Abs. 1 BDSG meldepflichtigen Stellen aufgenommen. Ein Bußgeldverfahren nach § 44 Abs. 1 Nr. 2 BDSG wegen der Nichtmeldung zum Register wurde eingeleitet.

Eine im Regierungsbezirk Darmstadt ansässige Versicherung ging sogar noch weiter. Um einer Verwechslung mit üblichen Werbesendungen vorzubeugen, ließ das Unternehmen von einem externen Dienstleister die kompletten Kfz-Kennzeichen der Autos der Versicherten auf dem Briefumschlag einer Mitteilung über eine Vertragsänderung außen anbringen. Alle Personen, die diese Schreiben auf dem Postweg sehen konnten, also z.B. Nachbarn, Hausmitbewohner oder auch deren Besucher, waren daher - je nach den örtlichen Gegebenheiten - in der Lage, die vor dem Haus stehenden Kraftfahrzeuge eindeutig zuzuordnen. Die Aufsichtsbehörde hat diese Werbekonzeption beanstandet. Bei künftigen Versandaktionen wird die Versicherung den datenschutzrechtlichen Erfordernissen Rechnung tragen.

## 8. Arbeitnehmerdatenschutz

### 8.1 Globales Personalinformationssystem

Eine große deutsche Unternehmensgruppe aus dem Bankbereich beabsichtigt, im Rahmen ihrer weltweiten Aktivitäten auch die Tätigkeit des Unternehmensbereiches "Konzerndienste Personal" global auszurichten. Zu diesem Zweck soll in allen inländischen und ausländischen Konzernunternehmen und Filialen ein einheitliches Personalinformationssystem verwendet werden. Dieses bildet alle personalwirtschaftlichen Kernprozesse, wie z.B. die Personalstammdatenverwaltung, Einstellungen, Stellendatenverwaltung und Personalentwicklung auf der Grundlage einer zeitgemäßen Informationstechnologie (Client-Server-Technologie) ab. Ziel einer konzernweit einheitlichen Einführung ist es, über eine gesteigerte Servicequalität personal-

wirtschaftlicher Prozesse zu einer wirtschaftlicheren und den zukünftigen Anforderungen der Unternehmensbereiche entsprechenden Ausrichtung der Personalfunktion zu kommen.
Das Konzept soll zeitlich gestaffelt umgesetzt werden.
In einer ersten Ausbaustufe sollte es in einem wirtschaftlich besonders bedeutsamen Unternehmensbereich eingesetzt werden, in welchem die Mitarbeiter durch ein erfolgsbezogenes Bonussystem zusätzlich entlohnt werden sollen. Das neue Personalinformationssystem soll hier insbesondere der Umsetzung dieses Bonussystems dienen. Im Zuge der Einführung des neuen Personalinformationssystems sollten erstmals Daten von in Deutschland tätigen Mitarbeitern auch ins Ausland übermittelt werden. Im Rahmen der ersten Ausbaustufe beschränken sich die Übermittlungen auf das europäische Ausland. Im Rahmen der letzten Ausbaustufe hingegen sollen die Übermittlungen von Deutschland aus auch ins nichteuropäische Ausland erfolgen.

Auf Initiative des betrieblichen Datenschutzbeauftragten wurde eine umfangreiche Vereinbarung zwischen der Konzernzentrale in Deutschland und den Globalen Koordinationsstellen für die Auslandsregionen zum grenzüberschreitenden Datenschutz getroffen. Ferner wurde mit dem Konzernbetriebsrat eine Betriebsvereinbarung geschlossen.

Die Auslandsstellen des Konzerns sind überwiegend keine eigenständigen juristischen Personen, sondern nur unselbständige Filialen. Zu Recht ist das Unternehmen aber gleichwohl davon ausgegangen, daß jede Übermittlung von personenbezogenen Daten ins Ausland, unabhängig davon, ob die empfangende Stelle eine unselbständige Filiale oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit ist, grundsätzlich als eine Übermittlung an einen Dritten zu bewerten ist.

Die Vereinbarungen tragen den Datenschutzbelangen der Mitarbeiter Rechnung und sind insgesamt als vorbildlich zu bewerten. So haben sich die Auslandsstellen des Konzerns den Regeln des Bundesdatenschutzgesetzes unterworfen. Der Datenkatalog wurde verbindlich festgelegt, es wurde eine strikte Zweckbindung vereinbart und es wurden Regelungen zur Datensicherheit getroffen. Ferner wurden die Rechte der Mitarbeiter auf Auskunft, Berichtigung, Löschung oder Sperrung geregelt. Besonders zu begrüßen war, daß dem betrieblichen Datenschutzbeauftragten auch gegenüber den Auslandsstellen Kontrollbefugnisse zugewiesen wurden und daß er bei der Wahrnehmung seiner Prüfungsaufgaben vom Stabsbereich Revision unterstützt werden soll. Unterstützung erhalten soll der Konzerndatenschutzbeauftragte auch von örtlichen Datenschutzverantwortlichen, die nach Maßgabe der Regelungen des Bundesdatenschutzgesetzes für den betrieblichen Datenschutzbeauftragten von den Globalen Koordinationsstellen für die Auslandsregionen zu bestellen sind.

Positiv zu vermerken ist ferner, daß sich die Auslandsstellen grundsätzlich der örtlichen Überprüfung durch die deutschen Aufsichtsbehörden unterworfen haben. Ob eine solche tatsächlich erfolgen wird, ist freilich eine andere Frage.
Kritisch hinterfragt wurde lediglich hinsichtlich des für die erste Ausbaustufe vorgesehenen Datenkatalogs, ob die Erforderlichkeit besteht, bei allen betroffenen Mitarbeitern sämtliche Daten des Katalogs zu übermitteln oder ob hier je nach Funktion des Mitarbeiters eine Differenzierung möglich wäre.
Von einer abschließenden Klärung dieser Frage konnte aber abgesehen werden, da gerade der Datenkatalog Bestandteil der Betriebsvereinbarung war.

Diese diente somit der Konkretisierung des Rechtsbegriffs der "Erforderlichkeit" unter Berücksichtigung der betrieblichen Gegebenheiten und war nicht zu beanstanden.

### 8.2 Nutzung der privaten Mitarbeiteradressen

In der Vergangenheit wurde bereits beanstandet, daß in Listen zur Betriebsratswahl auch die Privatadressen von Betriebsangehörigen genannt wurden. Für diesen Zweck waren die privaten Adressen nicht erforderlich; nach dem Hinweis der Aufsichtsbehörde wurde die Liste der Wahlberechtigten bereinigt.

Vergleichbar restriktive Maßstäbe gelten aber auch unmittelbar für den Arbeitgeber, der die von den Mitarbeitern erhaltenen Daten nur zur Erfüllung des Arbeitsvertrages nutzen darf.

Ein Arbeitnehmer muß die Möglichkeit haben, sich in seinem Privatbereich gegen die Zusendung von Schriften der Gewerkschaften und der Arbeitgeber gleichermaßen zu schützen.

Im konkreten Fall hatten zahlreiche Mitarbeiter der Übersendung einer überbetrieblichen Arbeitgeberzeitschrift an ihre Privatanschrift widersprochen. Der nicht näher genannte Grund für den Widerspruch war wohl, daß die Qualität der Zeitschrift nicht zufriedenstelle. Nun wollte der Vorgesetzte der betroffenen Mitarbeiter von der Personalabteilung erfahren, welche Mitarbeiter denn die Zeitschrift nicht zugesandt haben wollten. Erfreulicherweise hat der Datenschutzbeauftragte des Unternehmens einer derartigen innerbetrieblichen Datenweitergabe sofort widersprochen. Es war zu befürchten, daß die Nichtempfänger der Arbeitgeberzeitschrift einem psychologischen Druck ausgesetzt worden wären, der sie gezwungen hätte - im Interesse der Wahrung ihrer innerbetrieblichen Chancen - die Zeitschrift doch zu beziehen.

Im Falle einer Datenweitergabe wären eindeutig schutzwürdige Belange der Betroffenen beeinträchtigt worden. Der Arbeitgeber hat jederzeit die Möglichkeit, die Verbandszeitschrift im Betrieb zur Mitnahme auszulegen oder auch innerhalb des Betriebes direkt zuzustellen. Eine Beeinträchtigung der Privatsphäre ist mithin nicht erforderlich. Ein berechtigtes Interesse des Arbeitgebers an der gewünschten Information über die Nichtbezieher ist daher nicht gegeben.

Soweit bekannt ist, wurde dem Arbeitgeber - dank des Einsatzes des betrieblichen Datenschutzbeauftragten - die Auskunft über die Nichtbezieher der Verbandszeitschrift nicht erteilt.

### 8.3 Zeiterfassungssysteme

Über die Einführung eines datenschutzrechtlich bedenklichen Zeiterfassungssystems beschwerte sich ein Mitarbeiter eines Unternehmens.

Das PC-gestützte System sah vor, daß jeder Mitarbeiter in seinem eigenen elektronischen "Zeitzettel" seine täglichen Arbeitszeiten selbst einträgt. Ferner war eine Eintragung der Gründe für eine Abwesenheit vorgesehen (Krankheit, Urlaub, Arztbesuch etc.).

Diese Zeiterfassung sollte in einem sogenannten öffentlichen Pfad angelegt werden, d.h., alle an dem PC-Netz des Unternehmens angeschlossenen Mitarbeiter sollten jeweils den Zeitzettel der Kollegen lesen können.

Die Aufsichtsbehörde bewertete dies als unzulässig. Die Kenntnis der genauen Anwesenheitszeiten und die Gründe einer Abwesenheit sollte der Personalabteilung und den unmittelbaren Vorgesetzten vorbehalten bleiben. Und auch bei dieser Personengruppe wäre ergänzend zu prüfen, inwieweit ein jederzeitiger Einblick in sämtliche "Zeitzettel" erforderlich ist.

## 9. Medizinischer Bereich

### 9.1 Arzneimittelstudien bei Apotheken

Bei der Auswertung der Kassen-Rezeptdaten werden auch die Apotheken statistisch erfaßt. Die Apotheken als Auftraggeber der Apothekenrechenzentren haben jedoch jederzeit die Möglichkeit, die Verwertung der sie betreffenden Daten zu unterbinden. Die Verträge des Servicerechenzentrums mit den Apotheken müssen so gestaltet werden, daß die statistischen Auswertungen für Markt- und Meinungsforschungsunternehmen auf einer gesicherten Rechtsgrundlage erfolgen. Ein Rezeptabrechnungsauftrag würde allein noch nicht zur weiteren Nutzung der Rezeptdaten berechtigen.

In einem Fall wurden die bei den Apotheken zurückgegebenen Altarzneimittel nach Art und Menge erfaßt. Derartige Zahlen lassen sich aber nur sinnvoll einordnen, wenn gleichzeitig die Größe der Apotheke erfaßt wird. Die Richtgröße für eine Apotheke wird durch die Gesamtstundenzahl der Apothekenmitarbeiter festgestellt.
Im konkreten Fall wurde vergessen, auch die Apothekengröße zu erheben. Es versteht sich von selbst, daß diese Zahl nur mit dem Einverständnis der Betroffenen erhoben werden konnte. Schon aus rein praktischen Gründen sollte deshalb bereits bei Beginn einer Studie geprüft werden, welche Daten insgesamt benötigt werden, damit organisatorische und datenschutzrechtliche Probleme vermieden werden. Im Extremfall hätten bei einem unzureichenden Rückfluß aus der zweiten statistischen Erhebung die Daten aus der ersten Erhebung nicht verwendet werden können.

### 9.2 Anfragen an einen Ärzteverband

Eine Kassenärztliche Vereinigung wollte von einem Ärzteverband eine Auflistung aller Mitglieder und weitere Informationen bis zu den Namen der von den Ärzten betreuten Patienten. Besonders die zuletzt genannte Anforderung war völlig überzogen und hätte die Ärzte in Konflikt mit ihrer Schweigepflicht gebracht.

Die Kassenärztliche Vereinigung besaß zwar ein berechtigtes Interesse daran, die Namen von spezialisierten Ärzten zu erfahren, die gleichzeitig auch Kassenärzte sind; ein darüber hinausgehendes Informationsbedürfnis wurde jedoch nicht festgestellt. Es bleibt der Kassenärztlichen Vereinigung unbenommen, soweit erforderlich, Daten bei ihren Kassenärzten direkt zu erheben. Ein als Verein organisierter Ärzteverband kann aber allgemein nicht beurteilen, welche Informationen er über seine Mitglieder (Kassenärzte) herausgeben kann, ohne die schutzwürdigen Belange seiner Mitglieder zu beeinträchtigen. Datenübermittlungen im Zusammenhang mit der ärztlichen Tätigkeit der Vereinsmitglieder sind, ohne deren ausdrückliche Zustimmung, im Regelfall ausgeschlossen.

### 9.3 Übermittlung von Blutspenderdaten

Ein Blutspendedienst teilte mit, es bestünde der Verdacht, daß ein Patient durch eine seiner Blutkonserven eine HIV-Infektion erlitten habe. Um welche Konserve es sich handelte, konnte der Blutspendedienst ermitteln, es war ihm daher auch der Blutspender bekannt.

Die Krankenkasse des Patienten machte Regreßforderungen geltend und bat den Blutspendedienst in diesem Zusammenhang um eine Kopie des vor der Spende auszufüllenden Anamnesebogens. Dieser Bogen enthält außer Namen und Anschrift des Spenders auch medizinische Daten.

Der Datenschutzbeauftragte des Blutspendedienstes wandte sich an die Aufsichtsbehörde mit der Frage, ob diese Daten an die Krankenkasse übermittelt werden dürfen.

Die Aufzeichnungen auf dem Anamnesebogen vom bzw. über den Spender unterliegen der ärztlichen Schweigepflicht.

Sie dürfen nur insoweit offenbart werden, als der Betroffene, hier der Spender, das ärztliche Personal von seiner Schweigepflicht entbunden hat, oder wenn die Offenbarung zum Schutz eines höheren Rechtsgutes erforderlich ist.

Dem Recht des Spenders auf Geheimhaltung seiner Daten steht ein mögliches Interesse der Krankenversicherung des Geschädigten auf Schadensausgleich gegenüber.

Da sich aber herausstellte, daß der Blutspendedienst die Schadensersatzpflicht anerkannt hatte und damit die Krankenkasse und der betroffene Patient (Geschädigter) bereits ihre finanziellen Interessen durchsetzen konnten, entfiel das berechtigte Interesse an der Offenlegung der Daten des Spenders.

## 10. Datenschutz bei Telediensten

### 10.1 Anonyme und pseudonyme Kommunikation

Ein Anbieter von Telediensten im Aufsichtsbereich ermöglichte es nicht, daß Teilnehmer Angebote anonym oder mit einem Pseudonym nutzen konnten. Auf Veranlassung der Aufsichtsbehörde hin kann ein Nutzer dieses Teledienstes inzwischen ein Pseudonym verwenden.

Grundsätzlich müssen (Dienste)Anbieter nach § 13 Abs. 1 Mediendienste-Staatsvertrag bzw. § 4 Abs. 1 Teledienstedatenschutzgesetz eine anonyme oder pseudonyme Nutzung von Telediensten ermöglichen. Die anonyme Nutzung des Internets ist schon seit längerem mit sogenannten Schnupperangeboten - z.B. die ersten 50 Stunden gratis mit einer Kennung von der CD-ROM - möglich. Eine mißbräuchliche Nutzung von Diensten läßt sich bei derartigen Angeboten gar nicht oder nur erheblich erschwert einem Täter zuordnen.
Bei der Verwendung eines Pseudonyms kann der Anbieter jedoch im Bedarfsfall das Pseudonym dem Nutzer von Telediensten zuordnen. Die Verwendung eines Pseudonyms wird insoweit als vorteilhafter angesehen, als die mögliche Deanonymisierung bei dem Anbieter Mißbräuchen vorbeugt.
In diesem Zusammenhang muß dann in Kauf genommen werden, daß Pseudonyme dem Anbieter wiederum eine mißbräuchliche personenbezogene Auswertung des Nutzungsverhaltens ermöglichen. Die Gefährdung durch einen Anbieter wird jedoch als relativ gering eingeschätzt, da derartige Auswertungen über einen längeren Zeitraum kaum geheim bleiben können und neben den Maßnahmen der Aufsichtsbehörden der Wettbewerb die Korrektur mißbräuchlichen Verhaltens erzwingen wird.

### 10.2 Impressumspflicht bei einer Homepage im Internet

Bei geschäftsmäßigen Angeboten ist der Anbieter nach § 6 Teledienstegesetz verpflichtet, ein Impressum in sein Angebot aufzunehmen.

Wie die Beschwerde eines Finanzkaufmanns zeigte, ist die Abgrenzung zwischen privaten und geschäftsmäßigen Angeboten mitunter schwer zu definieren. Da im Beschwerdefall der Finanzkaufmann auch einen Link auf seine Finanzangebote und entsprechende Beispielrechnungen hatte, mußte er sich - trotz des im übrigen privaten Angebots - der Impressumspflicht unterwerfen.
Erfreulicherweise verlangt ein großer Serviceprovider im Zuständigkeitsbereich bereits in den Geschäftsbedingungen in jedem Fall ein Impressum. Zumindest hier sorgt damit bereits der Provider für klare Verhältnisse.

## 11. Versendung von Kreditkartenabrechnungen und Kontoauszügen innerhalb der Europäischen Union

a) Postgebühren sind im Ausland zum Teil niedriger als im Inland. Dies hat Unternehmen bewogen, Briefe an ihre Kunden vom Ausland aus zu versenden. So wunderte sich ein Bürger, daß er seine Kreditkartenabrechnungen von Dänemark aus erhielt. Auf den Abrechnungen war vermerkt, daß diese im Auftrag des Kreditkartenunternehmens in Dänemark hergestellt worden waren.
Der Bürger beklagte, daß man ihn weder um sein Einverständnis gefragt noch ihn benachrichtigt habe, bevor seine Daten ins Ausland transferiert wurden.
Aufgrund des dänischen Datenschutzgesetzes und der vertraglich getroffenen Regelungen über den Datenschutz ist die Aufsichtsbehörde zu der Einschätzung gelangt, daß kein Grund zu der Annahme besteht, daß ein überwiegendes schutzwürdiges Interesse der Betroffenen am Ausschluß der Datenübermittlung nach Dänemark vorhanden sei. Das Kreditkartenunternehmen hat bereits mehrfach Überprüfungen vor Ort durchgeführt und dabei nach eigenen Angaben keinen Grund zur Beanstandung gehabt. Daher war eine Einwilligung der Betroffenen nicht erforderlich.

Von einer separaten Benachrichtigung der Betroffenen konnte das Kreditkartenunternehmen absehen.

b) Ähnlich zu beurteilen ist auch die Auftragsvergabe einer Großbank an die Dänische Post zum Versenden von Kontoauszügen. Der Beschwerdeführer führte auch hier an, daß er vorab nicht informiert worden sei und daß er eine erhebliche Gefährdung der Sicherheit darin sehen würde, daß Angaben zu seiner Person - auch noch sein Kontostand - in Dänemark verarbeitet würden.

Es bleibt noch hinzuzufügen, daß sich bei der Aufklärung des Sachverhaltes herausstellte, daß es sich um eine einmalige Versuchaktion der Bank gehandelt hatte. Derzeit werden Kontoauszüge wieder unter Zuhilfenahme der Deutschen Post AG versandt.

Dem Beschwerdeführer wurde wie im Fall a) mitgeteilt, daß auch Dänemark datenschutzgesetzliche Regelungen hat und daß nach Einschätzung der Aufsichtsbehörde letztlich keine höhere Gefährdung als bei einer Versendung durch die Deutsche Post AG gegeben ist.

## 12. Datei über Stadionverbote

Ein großer deutscher Sportverband verarbeitet für seine angeschlossenen Vereine eine Datei, in der alle Personen gespeichert sind, die ein bundesweites Stadionverbot erhalten haben. Bisher ist diese Datenverarbeitung nur für Bundesligavereine durchgeführt worden.

Zur inhaltlichen Gestaltung sind Absprachen zwischen den Innenministern der Länder, der zuständigen Polizeibehörde und den Verbandsvertretern getroffen worden. Jedoch sind Vertreter der Datenschutzaufsichtsbehörden bei der Einrichtung und Einführung der Warndatei nicht zur Beurteilung der datenschutzrechtlichen Vertretbarkeit hinzugezogen worden.

Die Aufsichtsbehörde konnte im Nachhinein aufgrund ihrer Erfahrungen aus anderen Bereichen (z.B. Warndatei im Versandhandel, Versicherungsbereich) das Verfahren so umgestalten helfen, daß auch datenschutzrechtliche Belange Berücksichtigung finden. So gab es zuvor keine Einschränkung des zugriffsberechtigten Personenkreises in den einzelnen Vereinen. Hier konnte z.B. Konsens darüber gefunden werden, daß - ohne Einschränkung der Sicherheit - nur ein ausgewählter Personenkreis eine Zugriffsberechtigung erhalten hat. Andere Regelungen wurden im Bereich der Übermittlung getroffen, da festzustellen war, daß nicht alle gespeicherten Daten auch in jedem Fall zu übermitteln sind.

Nun erfüllt diese Verarbeitung personenbezogener Daten die Vorschriften des BDSG.

Mittlerweile hat die Erfahrung ergeben, daß bei Bundesligaspielen auffällig gewordene Täter auch im Bereich der Regionalliga-Veranstaltungen auffällig werden und umgekehrt. Die Stadionverbote werden daher sowohl für Bundesliga- als auch für Regionalliga-Veranstaltungen ausgesprochen. Aufgrund der bereits im Bundesligabereich getroffenen Maßnahmen kann die Ausdehnung der Datei der ausgesprochenen Stadionverbote auf den Regionalligabereich akzeptiert werden.

## 13. Videoüberwachung

Bedauerlicherweise unterliegen Aufzeichnungen von Videokameras auf herkömmlichen Bändern nicht den Vorschriften des BDSG, obwohl unter Umständen erhebliche Beeinträchtigungen der Persönlichkeitsrechte durch Videoaufzeichnungen vorliegen können.

Ob bei einer größeren Sportveranstaltung, im Kaufhaus, am Geldautomaten, an einer größeren Straßenkreuzung oder in Garagen und bei überwachten Zugängen zu Geschäften, der Bürger wird immer häufiger gefilmt.

Sicherlich erfüllen alle diese Einrichtungen auch einen sinnvollen Zweck. Sie dürfen aber nicht dazu führen, daß jeder Schritt des Bürgers anhand der Aufnahmen aufgezeichnet wird und nachvollziehbar ist.

Nur bei einer digitalen Aufnahme und Speicherung ist jedoch der Dateibegriff des § 3 Abs. 2 Nr. 1 BDSG erfüllt. Bei einer Speicherung auf herkömmlichen Videobändern ist das BDSG nicht anwendbar. Die Videoaufnahmen können jedoch unter Umständen eine so schwerwiegende Verletzung des allgemeinen Persönlichkeitsrechts darstellen, daß die Betroffenen auf dem Zivilrechtsweg Unterlassung verlangen können (BGH, NJW 1995, 1955).

Folgender Fall, bei dem der Dateibegriff nicht erfüllt war, wurde der Aufsichtsbehörde vorgetragen:

Ein Unternehmen hatte eine Videokamera zur Überwachung seines Eingangsbereichs installiert. Die Videoüberwachung schloß aber zwangsläufig auch den Zugang zur Wohnung der Beschwerdeführer mit ein. Das heißt, jedes Betreten und Verlassen der Wohnung wurde auf Videoband aufgezeichnet. Daß sich die Betroffenen dadurch in ihrer Entfaltung beeinträchtigt sehen, ist nachvollziehbar.

Die Aufsichtsbehörde regte an, daß das Unternehmen, das die Kamera installiert hatte, sich mit den Betroffenen auseinandersetzt und eine einvernehmliche Lösung findet.

Generell sollte bei vergleichbaren Situationen vor der Installierung der Kamera mit eventuell Betroffenen offen darüber gesprochen werden. Einvernehmlich sind dann die Aufnahmezeiten und eine eventuelle Löschung zu vereinbaren.

Mangels Zuständigkeit konnte die Aufsichtsbehörde - abgesehen von solchen allgemeinen Anregungen und Hinweisen - den Betroffenen nur auf die zivilrechtlichen Vorschriften verweisen.

## 14. Speicherung und Nutzung der Personalausweisnummer

Der Besitzer von zwei Videotheken speicherte unter anderem die Personalausweisnummer seiner Entleiher. Mit der Personalausweisnummer konnte er die Datenbestände miteinander abgleichen. Ziel der Datenspeicherung soll jedoch nicht der gezielte Abgleich, sondern die Identitätsfeststellung gewesen sein.

Die Personalausweisnummer hatte für den Videothekbesitzer in diesem Zusammenhang keinerlei Wert, da er hiermit bei keiner Behörde Auskünfte erhalten hätte. Zur Identitätsfeststellung konnte die Ausweisnummer keinen Beitrag leisten. Es fehlte damit an einem berechtigten Interesse für die Datenspeicherung; statt der Personalausweisnummer hätte ebenso eine Kundennummer vergeben und gespeichert werden können.
Die zumindest mögliche Verbindung von zwei Kundenkarteien über die Seriennummer des Personalausweises hätte darüber hinaus auch gegen § 4 Abs. 2 PAuswG verstoßen.

Erst nach mehrfacher Aufforderung wurden die Personalausweisnummern der Videothekkunden gelöscht. Es galt in diesem Fall generell zu verhindern, daß die Seriennummer des Personalausweises die Rolle einer persönlichen Identifikationsnummer erhielt, die dann auch in anderem Zusammenhang genutzt werden könnte.

## 15. Einwilligung beim Lastschriftverfahren

Zahlreiche Unternehmen nutzen das für sie kostengünstige Lastschriftverfahren der Banken. Da hierfür keine Persönliche Identifikationsnummer (PIN) eingegeben werden muß, erfolgt die Belastung nicht sofort automatisiert, sondern, vergleichbar einer Überweisung, zeitverzögert.
Der Einreicher einer Lastschrift bekommt von seiner Bank den Betrag sofort gutgeschrieben in der Erwartung, daß die Lastschrift bei der belasteten Bank anerkannt wird. Der belastete Bankkunde hat entsprechend den Abkommen der Banken sechs Wochen Zeit, der Belastung seines Bankkontos zu widersprechen. Gelegentlich widersprechen die Bankkunden der Kontobelastung, obwohl sie die Lieferung und Leistung für die Zahlung erhalten haben. Die

Bank ist in diesem Fall bereits aufgrund der Einwilligungserklärung des Schuldners auf dem Lastschriftauftrag berechtigt, dem Gläubiger Name und Adresse des Schuldners mitzuteilen.

Laut den im Beschwerdefall auf dem Lastschriftbeleg aufgedruckten Hinweisen wird der betreffende Kontoinhaber (Schuldner) bei der Nichteinlösung von Lastschriften auf Veranlassung des Gläubigers in eine Sperrdatei aufgenommen; die Löschung erfolgt erst mit der Begleichung des Rechnungsbetrages.
Unter diesen Voraussetzungen werden in der Regel keine schutzwürdigen Belange beeinträchtigt, selbst wenn die Sperrdatei mehreren Unternehmen des gleichen Konzerns zugänglich ist. Mit der Unterschrift auf dem Lastschriftbeleg hat sich der Kunde zur Zahlung verpflichtet; Negativfolgen wegen Nichtzahlung müssen von ihm getragen werden.

## 16. Datennutzung entgegen Hessischem Meldegesetz

Nach dem Hessischen Meldegesetz dürfen Parteien in den sechs einer Wahl vorausgehenden Monaten bestimmte Auskünfte aus dem Melderegister verlangen: Sie dürfen die Adressen von Wahlberechtigten einer Altersgruppe anfordern, etwa von Erstwählern oder Senioren, um gezielt Wahlkampf betreiben zu können.

Die Adreßdaten dürfen nur zweckgebunden verwendet werden, also für eine bestimmte Wahl, für die sie übermittelt wurden (§ 35 Abs. 5 HMG i.V.m. § 34 Abs. 4 HMG).
Diese Verpflichtung war einer örtlichen Parteigliederung wohl nicht hinreichend bekannt. Sie hatte sich für die Kommunalwahl vom März 1997 Erstwählerlisten geben lassen, diese aber damals nicht verwendet. Im Rahmen des Wahlkampfes für die Bürgermeisterwahl vom November 1997 griff sie auf die Listen aus der Kommunalwahl zurück. Dies war unzulässig, die Listen hätten nur für die Kommunalwahl verwendet werden dürfen.

Als unerheblich mußte dabei der Hinweis der Partei, daß der Wahlleiter der Gemeinde über ihre Absichten informiert gewesen sei, bewertet werden. Dessen Schweigen konnte keine Aufhebung des gesetzlichen Zweckbindungsgebotes bewirken.

## 17. Stellung des Datenschutzbeauftragten in der Hierarchie des Unternehmens

Bei größeren Unternehmen ist der Datenschutzbeauftragte häufig in der internen Revision angesiedelt bzw. kennt das Unternehmen aus seiner früheren Revisionstätigkeit. Die Interessenkonflikte von Revisionsmitarbeitern, die die Funktion eines Datenschutzbeauftragten ausüben, werden als tolerierbar angesehen, insbesondere da der häufig anzutreffende gute Informationsfluß zur Revision Vorteile verschafft. Rivalitäten zwischen der internen Revision und dem Datenschutzbeauftragten bezüglich der jeweiligen Rangordnung sollte es jedoch nicht geben.

Die interne Revision ist in der Regel als Stabsabteilung direkt der Geschäftsleitung unterstellt. Gleiches gilt für den Datenschutzbeauftragten, wobei seine unmittelbare Zuordnung zur Geschäftsführung nach § 36 Abs. 3 BDSG zwingend erforderlich ist.

Die Kontrolle der Revision obliegt der Unternehmensführung. Gleiches gilt für die Kontrolle des betrieblichen Datenschutzbeauftragten, da die Unternehmensführung bei eventuellen Verstößen gegen datenschutzrechtliche Bestimmungen auch die Verantwortung trägt.

Wie der Vorstand diese Kontrollen durchführt, muß er eigenverantwortlich entscheiden. Eine institutionalisierte Kontrolle der Tätigkeiten des Datenschutzbeauftragten durch die Revision wäre nicht gerechtfertigt, weil hierbei ein höherer Rang der Revision - und dadurch eine vom Gesetzgeber nicht gewollte Stellung des betrieblichen Datenschutzbeauftragten in der zweiten Hierarchiestufe - festgeschrieben würde.

Es wäre allenfalls denkbar, daß die Revision im Einzelfall einen besonderen Prüfungsauftrag von der Unternehmensleitung erhält. Im übrigen ist davon auszugehen, daß der Vorstand des Unternehmens die Tätigkeit im Bereich des betrieblichen Datenschutzes grundsätzlich selbst bewertet und kontrolliert.
Die Weisungsfreiheit des Datenschutzbeauftragten nach § 36 Abs. 3 Satz 2 BDSG darf durch eine einzelne Prüfung der Revision nicht beeinträchtigt werden. Dem Vorstand steht als Verantwortlichem für die Verwirklichung des Datenschutzes auch das Recht zu, die Tätigkeit des Datenschutzbeauftragten zu kontrollieren, sich also zu vergewissern, inwieweit er den ihm vom Gesetz zugewiesenen Aufgaben nachkommt. In diesem Rahmen ist der Vorstand durchaus befugt, Weisungen zu erteilen, die darauf abzielen, festgestellte Mängel zu beseitigen. Wenn sich der Vorstand zur Kontrolle des Datenschutzbeauftragten im Einzelfall der Revision bedient, dann darf deren Prüfung aber nicht so weit gehen, daß eine inhaltliche Bewertung der Kontroll- und Beratungstätigkeit des Datenschutzbeauftragten dergestalt erfolgt, daß dessen Funktion als unabhängiger Berater in Frage gestellt würde.

Eine Kontrolle der Tätigkeiten der Revision durch den betrieblichen Datenschutzbeauftragten ist dagegen regelmäßig erforderlich, da bei Revisionstätigkeiten Datenverarbeitungsprogramme eingesetzt und personenbezogene Dateien (Karteien) eingesehen werden. Die Revisionstätigkeiten berühren im Kunden- und Personalbereich sehr vertrauliche Daten, und es muß sichergestellt werden, daß Prüfungshandlungen vom jeweiligen Prüfungsauftrag gedeckt sind. Ebenso müssen sich Dokumentationen von Prüfungen auf das Wesentliche beschränken.
Einen vor dem betrieblichen Datenschutzbeauftragten abgeschotteten Bereich - abgesehen von möglichen Ausnahmen beim Betriebsrat (nach der Rechtsprechung des Bundesarbeitsgerichts, Beschluß vom 11. Nov. 1997 - 1 ABR 21/97) - darf es nicht geben, wenn der Datenschutzbeauftragte seinen in § 37 BDSG beschriebenen Aufgaben nachkommen soll.

## 18. Datensicherheit

### 18.1 Mensch und Maschine: Als Risikofaktor nie auszuschließen

Eine auffällige Häufung mußte die Aufsichtsbehörde im Berichtsjahr bei Beschwerden feststellen, denen fehlerhafte maschinell gesteuerte Verarbeitungen oder die mangelnde Sorgfalt von Mitarbeitern zugrunde lagen. Die Eingaben betrafen drei Banken, ein Kreditkartenunternehmen und eine Versicherung bzw. deren externe Dienstleister, welche die Postversendungen nach § 11 BDSG als Auftragnehmer abwickelten.

Durch Fehlfunktionen von Kuvertiermaschinen und anderen Geräten, die die Sortierung und Kuvertierung mehrseitiger Rechnungen steuern, wurden in mehreren Fällen Kontoauszüge und Rechnungsbelege verschiedener Kunden vermischt oder nicht einkuvertiert. Vorgesehene manuelle Kontrollen versagten. Die Unterlagen wurden abgesandt und damit personenbezogene Daten der jeweiligen Kunden unzulässig an andere Kunden übermittelt. In einem Fall wurde ein Kontoauszug dem Bankkunden sogar ohne Umschlag zugestellt.
Als Folge der Beanstandungen durch die Aufsichtsbehörde wurden bei zwei Banken bzw. deren Dienstleistern neue Kuvertiersysteme beschafft und die defekten Geräte ersetzt. Eine weitere Bank beließ es nicht hierbei, sondern beendete sofort die Zusammenarbeit mit dem mit der Versendung beauftragten Dienstleistungsbetrieb. Zusätzlich wurden in allen Unternehmen weitere Maßnahmen zur Qualitätskontrolle eingeführt.

Menschliches Versagen und mangelnde Sorgfalt war in zwei Fällen Ursache für Beschwerden gegen ein Versicherungsunternehmen. Bedingt durch das Vertauschen zweier Ziffern der Versicherungsnummer erhielt ein Versicherter eine bereits erstellte Leistungsabrechnung einer anderen Kundin mit personenbezogenen Daten aus dem medizinischen Bereich. Einem anderen Versicherungskunden wurden seine eingereichten Rechnungsbelege zurückgeschickt und dabei so ungeschickt kuvertiert, daß im Anschriftenfeld sogar die Diagnose des Arztes lesbar war. Beide Vorgänge wurden beanstandet. Die Versicherung bedauerte die Vorfälle und hat ihre Mitarbeiter zu größerer Sorgfalt angewiesen.

## 18.2 Datensicherheit - Laptop

Eine speichernde Stelle fragte nach erforderlichen Sicherheitseinrichtungen für tragbare PC's, auf denen Gesundheitsdaten verarbeitet werden sollen. Die Laptops werden den Außendienstmitarbeitern zur Verfügung gestellt und in regelmäßigen Abständen werden die erfaßten Daten mit dem Datenbestand abgeglichen. Da Gesundheitsdaten hochsensibel sind, sind entsprechende sichere Verfahren auszuwählen. Welches Verfahren nun die optimale Sicherheit bietet, kann von der Aufsichtsbehörde nicht vorgegeben werden. Zunächst ist zu bedenken, daß der Verlust von tragbaren Geräten eher gegeben ist als bei festinstallierten Geräten. Allein aus diesem Grund sind höhere Anforderungen an die Absicherung zu stellen. Trotz des erhöhten Risikos ist bedauerlicherweise von den Herstellern bisher versäumt worden, die tragbaren Geräte mit einem Mindestmaß an Sicherheitsvorkehrungen auszustatten und so dem Nutzer einfache Möglichkeiten zur Verfügung zu stellen, die auf den Geräten befindlichen Daten vor unbefugtem Zugriff zu schützen. So aber muß der Nutzer alleine für die entsprechende Absicherung sorgen.

Zu fordern sind eine hinreichend sichere Verschlüsselungstechnik zur Verschlüsselung der Festplatte und eventuell die Verschlüsselung von Daten auf Disketten. Zusätzlich ist der Einsatz einer Sicherheitssoftware empfehlenswert, die die unbefugte Kenntnisnahme und das unbefugte Eingeben von Daten oder Programmen verhindert. Sie sollte auch eine sichere Benutzersteuerung beinhalten und zusätzlich zur Paßwortverwaltung eine persönliche Identifizierungsnummer oder ein biometrisches Verfahren liefern. Bei der Anwendung im Rahmen von Gesundheitsdaten hält die Aufsichtsbehörde die Kombination von verschließbarem Gerät und Verschlüsselung durchaus für angemessen. Die Entscheidung, welches bzw. welche Verfahren letztendlich zum Einsatz gelangen, verbleibt natürlich bei der speichernden Stelle. Die Aufsichtsbehörde kann und soll weder besondere Produkte noch eine bestimmte Verfahrensweise vorgeben.

## 18.3 Sicherer Zugang zum Internet

Einige Male sind Datenschutzbeauftragte von Unternehmen an die Aufsichtsbehörde herangetreten mit der Frage, wie ein sicherer Zugang zum Internet für das Unternehmen zu erreichen sei.
Insbesondere wurde gefragt, inwieweit die Aufsichtsbehörde die Einrichtung einer Firewall für erforderlich ansehen würde.
Je höher der Sicherheitsstandard einer Firewall ist, desto eingeschränkter ist allerdings auch die Möglichkeit, externe Dienste zu nutzen.

Bisher wurde bei allen Anfragen vorgeschlagen, soweit die Organisation der Datenverarbeitung dies zuläßt, für den Zugang speziell zum Internet einen Rechner zu nutzen, der außerhalb des eigenen Rechnersystems arbeitet und an dieses in keiner Weise angeschlossen ist. Nur so ist es möglich, das Eindringen Externer in ein Rechnersystem vollständig zu verhindern. So ist es z.B. möglich, Daten und Programme aus dem Internet herunterzuladen und auf dem eigenen System zu verarbeiten. Die Authentizität dieser Daten ist allerdings nur dann zu gewährleisten, wenn Sender und Empfänger ein sicheres kryptografisches Verfahren nutzen. Beim Austausch von Dokumenten sollten die Normen des Signaturgesetzes zur digitalen Unterschrift erfüllt sein, damit die Sicherheit gewährleistet ist.

## 18.4 Dokumentation

Im Rahmen des immer weiter gehenden Einsatzes von PC in allen Unternehmensbereichen ist das Erstellen einer anspruchsvollen Dokumentation der Datenverarbeitung in den Hintergrund getreten.

Nur in sehr seltenen Fällen sind die datenverarbeitenden Stellen in der Lage, eine aussagefähige Dokumentation zu ihren Datenverarbeitungsaktivitäten vorzulegen. Eine ordnungsgemäße Datenverarbeitung ist aber ohne eine ausführliche Dokumentation nicht möglich. Auch reichen die zur Standardsoftware gehörenden Dokumentationen in der Regel nicht aus bzw. sie sind viel zu allgemein und umfassend. Hier verkennen die Anwender, daß eine Dokumentation den Ablauf der Datenverarbeitung nachvollziehbar und erkenn-

bar erläutern soll. Dabei ist das Führen einer Dokumentation nicht alleine eine Frage des Datenschutzes, sondern eine Dokumentation dient in erster Linie den Eigeninteressen der datenverarbeitenden Stellen. So sind Änderungen in bestehenden Verfahren wesentlich einfacher und fehlerfreier durchzuführen. Neue Mitarbeiter sind rascher in die Verfahren einzuarbeiten. Systemwechsel sind ebenfalls wirtschaftlicher durchzuführen. Dies sind nur wenige der Vorteile einer ordnungsgemäßen Datenverarbeitung. Zugegebenermaßen bieten die komfortablen Systeme und Techniken, die mittlerweile für alle PC-Systeme vorhanden sind, die Möglichkeit, kurzfristig Auswertungen zu erstellen. Bedauerlicherweise wird dann aber nicht festgelegt, für welchen Zweck diese Auswertung erstellt wird, wer verantwortlich für diese ist, wie lange und in welcher Form sie aufzubewahren ist.
Entsprechende zusätzliche Dokumentationen sind erforderlich.

### 18.5 Der Nutzen von Paßwörtern

Im Rahmen von Jahresberichten kann nur auf gravierende Mängel hingewiesen werden; im übrigen ist der EDV-Benutzer auf die jeweils einschlägige spezielle Fachliteratur angewiesen.
Bereits im vorangegangenen Tätigkeitsbericht wurden Ausführungen zum Thema Paßwörter gemacht. Der Leichtsinn in bezug auf Paßwörter hat sich jedoch noch nicht gebessert.

Wer sein Auto abschließt und den Schlüssel stecken läßt, braucht sich über plötzliche Veränderungen der Besitzverhältnisse zu seinen Ungunsten nicht zu wundern.
Durchaus vergleichbar haben einzelne Benutzer ihre Paßwörter im Rechner gespeichert, weil es ja viel bequemer ist, mit einer Funktionstaste oder einem Mausklick eine Anwendung zu starten. Besonders Leichtsinnige speichern auch noch ihre Persönliche Identifikationsnummer (PIN) und ihre Transaktionsnummern (TAN) ebenfalls im Rechner. Der Wunsch des Kunden, nach "Benutzerfreundlichkeit" veranlaßte die Programmhersteller, hierfür die Möglichkeiten zu schaffen. Derartiges ist jedoch unverantwortlich.

Sicherheit ist derzeit nur mit Unbequemlichkeiten, d.h. manuelle Eingabe von Paßwort, PIN, TAN oder mit finanziellem Aufwand - z.B. mit einer Chipkarte - zu erhalten.
Es wäre schön, wenn nächstes Jahr zu diesem Thema einmal Positives gemeldet werden könnte. Ein Dauerthema wird es wohl bleiben.

## 19. Ordnungswidrigkeitenverfahren

Ein bereits im letzten Tätigkeitsbericht aufgeführtes Bußgeldverfahren nach § 44 Abs. 1 Ziff. 2 BDSG gegen die Geschäftsführerin einer Direktmarketinggesellschaft konnte, nachdem das zuständige Amtsgericht die Rechtsauffassung der Aufsichtsbehörde bestätigt hatte, im Berichtsjahr 1997 rechtskräftig mit einem Bußgeld in Höhe von 2.500,-- DM abgeschlossen werden.

Das Unternehmen, auf das die Aufsichtsbehörde durch die Eingabe eines betroffenen Bürgers aufmerksam gemacht wurde, hatte bereits mehrere Monate rechtswidrig entgegen § 915 Abs. 2 ZPO in erheblichem Umfang personenbezogene Daten aus den Schuldnerverzeichnissen der Amtsgerichte im Auftrag als Dienstleistungsunternehmen zu Werbezwecken verarbeitet und war auch seiner Meldepflicht nach § 32 Abs. 1 Ziff. 3 BDSG gegenüber der Aufsichtsbehörde nicht nachgekommen. Das Unternehmen hat seine unzulässige Tätigkeit aufgrund der Aktivitäten der Aufsichtsbehörde und der eingeschalteten Staatsanwaltschaft inzwischen eingestellt.
Im Berichtsjahr 1997 wurden von der Aufsichtsbehörde sechs Ordnungswidrigkeitenverfahren nach § 44 BDSG eingeleitet.

Ein von der Aufsichtsbehörde gegen ein Schreib- und Datenerfassungsbüro nach § 44 Abs. 1 Ziff. 6 BDSG eingeleitetes Ordnungswidrigkeitenverfahren wegen der trotz mehrfacher Aufforderung nicht erfolgten Erteilung von Auskünften entgegen § 38 Abs. 3 Satz 1 BDSG wurde, nachdem die Geschäftsführerin Einspruch gegen den Bußgeldbescheid erhoben hatte, vom zuständigen Amtsgericht eingestellt, weil das Gericht den Verstoß als geringfügig bewertete.

Zwei weitere Ordnungswidrigkeitenverfahren nach § 44 Abs. 1 Ziff. 6 BDSG wegen der nicht erfolgten Erteilung von Auskünften an die Aufsichtsbehörde entgegen § 38 Abs. 3 Satz 1 BDSG richteten sich gegen die Geschäftsführer eines Datenverarbeitungs-Dienstleistungsunternehmens für die Reise- und Touristikbranche, die mehrere Monate die Aufforderungen der Datenschutzaufsichtsbehörde zur Auskunftserteilung ignorierten. Beide Bußgeldbescheide haben noch während des Berichtsjahres Rechtskraft erlangt.

Gegen drei Geschäftsführer von Firmen aus dem Bereich der Dienstleistungsdatenverarbeitung wurden Ordnungswidrigkeitenverfahren nach § 44 Abs. 1 Ziff. 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 aus, ohne eine entsprechende Meldung zum Register der meldepflichtigen Stellen bei der Aufsichtsbehörde abgegeben zu haben.

Auch in diesen Fällen erhielt die Aufsichtsbehörde die entscheidenden Hinweise auf die Tätigkeit der Unternehmen durch die Eingaben von Bürgern. Die drei erlassenen Bußgeldbescheide wurden ebenfalls noch im Berichtsjahr bestandskräftig.

Wiesbaden, den 11. September 1998

Der Hessische Ministerpräsident
**Eichel**

Der Hessische Minister des Innern
und für Landwirtschaft, Forsten
und Naturschutz
**Bökel**