



# HESSISCHER LANDTAG

18. 09. 2001

## **Vorlage der Landesregierung**

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

Vorgelegt mit der Stellungnahme zum Neunundzwanzigsten Tätigkeitsbericht  
des Hessischen Datenschutzbeauftragten - Drucks. 15/2500 - nach § 30 Abs. 2  
des Hessischen Datenschutzgesetzes in der Fassung vom 7. Januar 1999.

Inhaltsverzeichnis	Seite
1. Bearbeitung von Datenschutzbeschwerden und sonstige Prüfungen aus besonderem Anlass nach § 38 Abs. 1 BDSG	4
2. Von Amts wegen durchgeführte Regelüberprüfungen von Stellen, die nach § 32 Abs. 1 Nr. 1 bis 3 BDSG geschäftsmäßig personenbezogene Daten verarbeiten oder nutzen	5
2.1 Melderegister	5
2.2 Prüfungsübersicht	6
3. Bearbeitung von Anfragen zu datenschutzrechtlichen Problemstellungen	6
4. 6. Workshop der Datenschutzaufsichtsbehörden am 14./15. September 2000 beim Regierungspräsidium Darmstadt	8
5. Datenverarbeitung bei Banken	8
5.1 Einholung von Auskunft-Daten zu anderen als den angegebenen Zwecken	8
5.2 Unzulässige Speicherung des Warnhinweises "arbeitslos"	9
5.3 Datenweitergabe an einen freigestellten Mitarbeiter	9
5.4 Keine Datenlöschung bei Geschlechtsumwandlung	10
6. SCHUFA	10
6.1 Keine Einwilligung und falscher Eintrag	10
6.2 SCHUFA-Eintrag über beantragte Zwangsvollstreckung	11
6.3 Personenverwechslung und trotzdem Entgeltzahlung für Eigenauskunft	11
6.4 SCHUFA-Anfrage in jedem Fall?	12
7. Videoüberwachung	12
7.1 Auslegung der geplanten Regelung in § 6 b BDSG n.F.	12
7.2 Wohnhaus-Videoüberwachung auf TV-Sonderkanal	14
7.3 Videoüberwachung im Fahrstuhl	15
7.4 Löschung der Videoaufzeichnung und Zugriffsschutz nicht gewährleistet	15
7.5 Überwachung von Schuhreparatur-Filialen in Kaufhäusern	16
7.6 Überwachung von Freizeitanlagen	17
7.7 Webcam	18
8. Neue Medien, Internet-Provider	19
8.1 Unzulässig lange Speicherung von Nutzungsdaten	19
8.2 Angebliche Sicherheitslücke beim Homebanking trotz HBCI	21
8.3 Daten anderer Kunden beim Online-Banking übermittelt	21
8.4 SMS-Nachrichten mit unverlangter Werbung auf dem Handy	22

8.5	Personenverwechslung im Call-Center eines Internet-Providers	23
9.	Auslandsdatenverarbeitung	24
10.	Arbeitnehmerdatenschutz	25
10.1	Werbemaßnahmen von Zeitarbeitsunternehmen	25
10.2	Datenübermittlung an Gewerkschaften	26
10.3	Veröffentlichung der Arbeitszeitabrechnung	27
11.	Medizinischer Bereich	27
11.1	Verwertung der Rezeptdaten von Kassenpatienten	27
11.2	Unzulässige Übermittlung von Patientendaten an ein externes Labor	28
11.3	Datenübermittlung durch Sanitätshaus	29
12.	Versicherungen: Datenübermittlungen im Zusammenhang mit Holocaust-Entschädigungen	29
13.	Werbewirtschaft	30
13.1	Auskunftserteilung beim Listbroking	30
14.	Datenverarbeitung in Vereinen und Verbänden	32
14.1	Bundeseinheitlicher elektronischer Mitgliedsausweis	32
14.2	Verbandszwecke und Versicherungsgeschäfte	32
14.3	Übermittlung von Sammlerdaten	33
14.4	Persönliche Angaben über Jugendliche im Vorraum einer Turnhalle	34
15.	Der betriebliche Datenschutzbeauftragte	34
15.1	Kündigung eines internen Datenschutzbeauftragten, unklare Unternehmensstrukturen	35
15.2	Untätigkeit des externen Datenschutzbeauftragten	37
16.	Datensicherheit	37
16.1	Die günstige Flohmarkt-CD: Betriebsgeheimnisse für 3 DM!	37
16.2	Die ärztliche Schweigepflicht – Ein Fall fürs Altpapier?	38
16.3	Keinerlei Sicherheitskonzept bei Auftragsdatenverarbeiter	39
16.4	Aktionärsdaten ungeschützt im Internet abrufbar	39
17.	Die nicht alltägliche Geschäftsidee	39
18.	Aus dem Alltag einer Datenschutzbehörde	40
18.1	Marktforscher nicht zum Register gemeldet	40
18.2	Name und Anschrift einer Kundin in Fahrplanheft	40
18.3	Offenlegung der Putzfrauenabrechnung gegenüber Mietern	41
19.	Ordnungswidrigkeitenverfahren	41

## 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 wurde. Die Überprüfungen werden insbesondere dann vorgenommen, wenn entsprechende Anhaltspunkte von Betroffenen selbst darlegt werden, aber auch wenn Meldungen in Presse, Fernsehen oder im Internet auf einen Verstoß gegen datenschutzrechtliche Vorschriften hinweisen.

Immer mehr Unternehmen und Privatpersonen bedienen sich heute modernster Informations- und Kommunikationstechnologien. Die rasche Ausbreitung der Nutzung von unterschiedlichsten Internetdiensten und die Spitzenstellung Hessens als Standort für innovative Unternehmen der Internetbranche hat dazu geführt, dass sich die Zahl der Eingaben betroffener Bürger gegen Anbieter von Telediensten im Internet bei den Datenschutzaufsichtsbehörden im Jahr 2000 im Vergleich zum Vorjahr mehr als verdoppelt hat.

Wenn es um die Verarbeitung der eigenen Einkommens-, Vermögens- und Bonitätsdaten geht, zeigen Bürgerinnen und Bürger in Deutschland traditionell eine hohe datenschutzrechtliche Sensibilität. Die herausragende Stellung des internationalen Finanzplatzes Frankfurt am Main mit dem Sitz der Europäischen Zentralbank, den großen deutschen Geschäftsbanken und der Deutschen Börse AG wurde im Berichtsjahr weiter gestärkt. Wie schon in den Vorjahren nimmt die Bearbeitung von Beschwerden gegen Unternehmen aus dem Bereich der Geld- und Kreditwirtschaft (Banken, Auskunfteien, SCHUFA, Kreditkarten, Finanzdienstleister und Vermögensberater) daher weiterhin einen großen Raum insbesondere bei dem für die Rhein/Main-Region zuständigen Regierungspräsidium Darmstadt ein.

Im Berichtsjahr wurden von den Aufsichtsbehörden in 273 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.

Die 273 Überprüfungen von Eingaben, Beschwerden und Pressemeldungen betrafen:

- in 43 Fällen Anbieter von Telediensten (Provider von Internetzugängen und -inhalten),
- in 43 Fällen Kreditinstitute, Banken und EDV-Dienstleister im Zahlungsverkehr,
- in 30 Fällen Unternehmen der Direktmarketing- und Werbewirtschaft,
- in 22 Fällen den Datenschutz in Arbeitsverhältnissen,
- in 14 Fällen Vereine (Sport, Soziales, Kultur) sowie deren Landes- und Bundesverbände,
- in 13 Fällen Adresshändler, Adressverlage und Herausgeber öffentlicher Verzeichnisse,
- in 11 Fällen die Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA),
- in 11 Fällen Handels- und Wirtschaftsauskunfteien,
- in 10 Fällen Versicherungsgesellschaften,
- in 9 Fällen Vermieter, Wohnungs- u. Immobilienverwaltungsfirmen,
- in 9 Fällen das Gesundheitswesen (Ärzte, medizinische Marktforschung, EDV-Dienstleister),
- in 8 Fällen Unternehmen des Groß- und Einzelhandels (Autos, Möbel, EDV-Bedarf),
- in 6 Fällen Unternehmen der Versandhandelsbranche,
- in 4 Fällen Kreditkartenunternehmen,
- in 3 Fällen Datenträgervernichter und Unternehmen der Abfallwirtschaft,
- in 3 Fällen kommerzielle Freizeiteinrichtungen und Sportstätten,
- in 34 Fällen sonstige Stellen (Vermögensberater, Zeitungsverlage, Markt- und Meinungsforschungsunternehmen, Inkassodienste sowie Detektive und Sicherheitsunternehmen).

In insgesamt 59 Fällen waren die Beschwerden begründet. Sämtliche bei diesen Nachforschungen der Aufsichtsbehörden festgestellten unzulässigen Verarbeitungen personenbezogener Daten und anderer Verstöße gegen Vorschriften des Rechts der Tele- und Mediendienste führten zu Beanstandungen der jeweiligen Verarbeitungsverfahren bei den betroffenen Stellen.

Die bei den Überprüfungen beanstandeten 59 Verstöße gegen Datenschutzbestimmungen konnten festgestellt werden:

- in 12 Fällen bei Kreditinstituten und Banken,
- in 8 Fällen bei Unternehmen der Werbewirtschaft
- in 5 Fällen bei Anbieter von Tele- und Mediendiensten (Internet),
- in 4 Fällen bei eingetragene Vereinen und Dachverbänden,
- in 4 Fällen bei Adresshändlern und Listbrokern
- in 3 Fällen bei Stellen, die Personal- und Bewerberdaten verarbeiten,
- in 3 Fällen bei Wohnungs- und Immobilienverwaltungen
- in 3 Fällen bei Wirtschaftsauskunfteien
- in jeweils 2 Fällen bei Versicherungsgesellschaften, bei Akteneinlagebetrieben, im Gesundheitssektor, im Einzelhandel, bei Inkassounternehmen, und bei kommerziellen Sport- und Freizeiteinrichtungen,
- in jeweils 1 Fall bei einer Kapitalanlagegesellschaft, einem Kreditkartenunternehmen, der SCHUFA, einem Detektiv und einem Markt- und Meinungsforschungsunternehmen.

Bei 42 Eingaben an die Datenschutzaufsichtsbehörden konnte der den Überprüfungen zugrunde liegende Sachverhalt nicht vollständig aufgeklärt werden, sodass eine abschließende Beurteilung, ob die Datenverarbeitung in zulässiger oder in unzulässiger Weise erfolgt war, nicht sicher getroffen werden konnte. Die Aufsichtsbehörden haben hier zwar keine formalen Beanstandungen ausgesprochen. Der Kontakt mit den Unternehmen wurde in diesen Fällen aber immer zu Beratungsangeboten genutzt, mit denen auch viele Unternehmensleitungen für datenschutzrechtliche Problemstellungen sensibilisiert werden konnten.

In 65 Fällen waren die Ermittlungen der Aufsichtsbehörden zum Ende des Berichtsjahres noch nicht abgeschlossen.

Von den noch aus den Vorjahren anhängigen Beschwerden wurden 63 Fälle abgeschlossen. Die Beurteilung dieser teilweise hochkomplexen und in der Regel nur mit hohem Ermittlungsaufwand aufklärbaren Fälle durch die Aufsichtsbehörden ergab, dass davon 15 Eingaben begründet waren.

Die beanstandeten 15 Verstöße gegen Datenschutzbestimmungen konnten festgestellt werden:

- in 3 Fällen bei Versandhandelsunternehmen
- in 2 Fällen bei Banken,
- in 2 Fällen bei einem Verein und einem Dachverband
- in 2 Fällen bei einem Kreditkartenunternehmen,
- sowie in jeweils 1 Fall bei einem Vermögensberater, einer Versicherung, einem Arzt, einem Arbeitgeber, einem Marktforschungsunternehmen und einem Großhändler, die personenbezogene Daten unzulässig gespeichert, genutzt oder übermittelt hatten.

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

### **2.1 Melderegister**

Die Aufsichtsbehörden führen nach § 38 Abs. 2 BDSG das Register der Stellen, die personenbezogene Daten geschäftsmäßig zum Zweck der personenbezogenen oder der anonymisierten Übermittlung speichern oder im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen. Diese Stellen unterliegen nach § 32 BDSG der Meldepflicht bei den Datenschutzaufsichtsbehörden.

Am 1. Februar 2001 waren 847 meldepflichtige Unternehmen im Register der Aufsichtsbehörden eingetragen. Damit war eine Steigerung gegenüber dem Vorjahr von ca. 5 v.H. zu verzeichnen.

Den größten Anteil hieran haben mit 707 Meldungen die nach § 32 Abs. 1 Ziff. 3 BDSG gemeldeten Unternehmen, die im Auftrag 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 78 Meldungen haben die nach § 32 Abs. 1 Ziff. 2 BDSG meldepflichtigen Unternehmen der Markt- und Meinungsforschung, die personenbezogene Daten zum Zwecke der anonymisierten Übermittlung speichern, den zweitgrößten Anteil am Melderegisterbestand.

Den geringsten Anteil haben mit 62 Registereinträgen die nach § 32 Abs. 1 Ziff. 1 BDSG gemeldeten Unternehmen, die, wie z.B. Adresshändler oder auch Wirtschaftsauskunfteien, personenbezogene Daten zum Zwecke der Übermittlung speichern.

## 2.2 Prüfungsübersicht

Im Berichtsjahr wurden 44 Prüfungen nach § 38 Abs. 2 BDSG durchgeführt. Diese betrafen folgende Unternehmen:

- Servicerechenzentren	13
- Konzerndatenverarbeiter/verbundene Unternehmen	4
- Datenvernichter	7
- Adresshändler	8
- Telemarketingunternehmen/Call-Center	1
- Markt- und Meinungsforschung	3
- Vereine/Verbände	2
- Mikroverfilmer/Datenarchive	4
- Auskunfteien	2

Die Prüfungen führten zu folgendem Ergebnis:

- Beanstandungen	23
- Empfehlungen (z.T. zusätzlich zu Beanstandungen in andern Punkten ausgesprochen)	32
- ohne Beanstandungen/Empfehlungen	6

Folgende wesentliche Mängel wurden am häufigsten festgestellt:

1. völlig unzureichende oder keine Schulung der Mitarbeiter,
2. mangelhafte Vorgaben zur Nutzung von Passwörtern; leichtsinniger Umgang mit Passwörtern,
3. desolate Organisation von Benutzer-/Zugriffsrechten (ohne Konzept),
4. unvollständige bzw. fehlende Dokumentation der Informationstechnik,
5. keine Weisungen der Auftraggeber nach § 11 BDSG,
6. während der Prüfung festgestellte Veränderung zu den Meldungen nach § 32 BDSG (somit verspätete Meldung),
7. Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten nicht erfüllt oder keine sichtbare Tätigkeit des betrieblichen Datenschutzbeauftragten,
8. unzulängliche Regelung der Zugangskontrolle (offene Türen zum Server-Raum).

## 3. Bearbeitung von Anfragen zu datenschutzrechtlichen Problemstellungen

Die Beratungstätigkeit der Aufsichtsbehörden wurde im Berichtsjahr weiter ausgebaut, da sich die Zahl der Bitten um datenschutzrechtliche Stellungnahmen zu laufenden Verarbeitungsverfahren oder geplanten - auch internationalen - EDV-Projekten im Vergleich zum Vorjahr fast verdoppelt hat.

Die bei den Datenschutzaufsichtsbehörden immer häufiger anzutreffenden Kooperationswünsche datenverarbeitender Stellen sind häufig die Folge betriebswirtschaftlicher Kalkulationen, die das Ziel haben, kostspielige Fehlinvestitionen in die Entwicklung und Implementierung datenschutzrechtlich letztlich unzulässiger Datenverarbeitungsverfahren zu vermeiden. Die Aufsichtsbehörden kommen solchen Beratungsersuchen gerne nach. Es ist ohne Zweifel sinnvoll und effektiv, Problemfelder bereits im Projektvorfeld zu identifizieren und datenschutzrechtliche Bedenken bei der DV-technischen Umsetzung zu berücksichtigen, statt abzuwarten, bis sich problematische oder unzulässige Verfahren etabliert haben, die dann nach einer Beanstandung durch die Aufsichtsbehörden abzuändern sind. Die Ausweitung dieser prophylaktischen Beratungstätigkeit entspricht auch voll und ganz dem Selbstverständnis der Dienststellen.

Der steigende Beratungsbedarf kann aber auch als Indiz dafür gewertet werden, dass durch die im Berichtsjahr 2000 noch nicht vollzogene Novellierung des Bundesdatenschutzgesetzes bestehende Unsicherheiten in der Bevölkerung und in den Betrieben weiter zugenommen haben.

Erfreulicherweise ist das novellierte BDSG endlich am 23. Mai 2001 in Kraft getreten. Der Novellierungsentwurf und die Stellungnahme des Bundesrates konnten von den Aufsichtsbehörden bereits vor dem Inkrafttreten bei Beratungsanfragen berücksichtigt werden.

Das Datenschutzrecht spielt als Querschnittsmaterie heute in nahezu allen Bereichen unseres von Technik durchdrungenen Lebens eine wichtige Rolle. Dies ist unter anderem schon an dem breiten Spektrum der unter Nr. 1 dieses Berichtes aufgeführten Branchen und Sektoren zu erkennen.

Dementsprechend breitgefächert waren die Beratungsanfragen.

Wie schon im letzten Jahr hat die Beantwortung von Datenschutzfragen zur betrieblichen und privaten Internet-Nutzung erneut einen breiten Raum eingenommen (vgl. Nr. 8 des Berichtes). Unabhängig von den unter Nr. 8 dieses Berichtes dargestellten Einzelfällen musste die Datenschutzaufsicht besonders im privaten Bereich oftmals feststellen, dass es vielen Nutzerinnen und Nutzern von Internetdiensten an elementarsten Grundkenntnissen über die Funktionsweisen der genutzten Dienste (meistens WWW und E-Mail) und der datenschutzrechtlichen Aspekte ihrer Inanspruchnahme mangelte. Die kostenlosen Telefon-Hotlines der Internet-Provider konnten bei datenschutzrelevanten Fragen in den seltensten Fällen weiterhelfen. Im Gegenteil: Schlecht ausgebildete Mitarbeiter ("Ihre Daten kann man nicht mehr löschen") in kurzfristig angemieteten Call-Centern ("Keine Ahnung, wir machen das erst seit gestern") mit hoher Personalfuktuation ("Ich bin erst kurz hier und kenne niemanden") in Verbindung mit einer schon fast dauerbesetzten Servicenummer fördern eher die Unsicherheit und das Misstrauen der Kunden, die dann bei der Datenschutzaufsichtsbehörde mit der Bitte um Aufklärung oder Unterstützung wegen des Umganges mit ihren Bestands- oder Nutzungsdaten nachfragen. An dieser Stelle sind besonders die betrieblichen Datenschutzbeauftragten der Internet-Provider gefordert, neue Call-Center-Vertragspartner und deren Mitarbeiter umgehend intensiv datenschutzrechtlich zu schulen, um einen angemessenen Qualitätsstandard erreichen zu können.

Als weiterer Arbeitsschwerpunkt hat sich im Jahr 2000 das Thema "Videoüberwachung und -aufzeichnung" herauskristallisiert. Das Interesse am Verhalten von Mitmenschen ist in unserer Gesellschaft aus unterschiedlichsten Gründen gewachsen und die Marktverfügbarkeit kostengünstiger Videoüberwachungsanlagen auch für den Privatbereich (Wohnung, Grundstück) ist deutlich gestiegen. Da moderne Videokameras bei geschickter Installation kaum noch erkennbar sind und die Begehrlichkeiten, Informationen über Nachbarn, Besucher, Gäste, Personal oder auch Mieter zu erhalten, ebenfalls groß sind, ist zu befürchten, dass die Medien, Betroffene und die Datenschutzaufsichtsbehörden nur von der so genannten Spitze des Eisberges (vgl. Nr. 7 dieses Berichtes) Kenntnis erhalten.

Ein weiterer inhaltlicher Schwerpunkt lag wie schon im Vorjahr bei den Anfragen zur Position und Funktion des betrieblichen Datenschutzbeauftragten nach §§ 36, 37 BDSG (vgl. Nr. 15 des Berichtes).

Nicht nur in kleinen und mittleren Unternehmen gibt es immer noch große Defizite bei der Wahrnehmung der gesetzlich vorgesehenen Selbstkontrolle durch betriebliche Datenschutzbeauftragte. Umfang und Bedeutung dieser Selbstkontrolle werden durch die Novellierung des BDSG weiter zunehmen. Das Regierungspräsidium Darmstadt wird daher im laufenden Jahr zur Vorbereitung der Betriebe auf die neuen Regelungen des BDSG und insbesondere auf die neuen Aufgaben für die betrieblichen Datenschutzbeauftragten zusammen mit südhessischen Industrie- und Handelskammern entsprechende Informations- und Schulungsveranstaltungen zur BDSG-Novelle anbieten. Das vorhandene Internet-Angebot der Datenschutzaufsichtsbehörden im WWW wird ebenfalls umfassend überarbeitet und neugestaltet werden.

#### **4. 6. Workshop der Datenschutzaufsichtsbehörden am 14./15. September 2000 beim Regierungspräsidium Darmstadt**

Das Regierungspräsidium Darmstadt lud im Berichtsjahr alle Aufsichtsbehörden des Bundesgebietes zu einem Erfahrungs- und Meinungsaustausch über praktische Vollzugsfragen ein. Es war der 6. Workshop; zu den vorangegangenen Workshops hatten der Hamburgische Datenschutzbeauftragte (1995), der Niedersächsische Datenschutzbeauftragte (1996), das Innenministerium Brandenburg (1997), das Regierungspräsidium Dresden (1998) und das Thüringer Landesverwaltungsamt (1999) eingeladen.

Auf der Tagesordnung stand dieses Mal unter anderem ein Erfahrungsaustausch zum Thema Videoüberwachung. Die Ergebnisse der Erörterungen sind in die nachstehenden Ausführungen unter Nr. 7 eingeflossen.

Auch die unter Nr. 13 aufgeführten Datenschutzprobleme beim Direktmarketing wurden auf dem Workshop behandelt.

Einen breiten Rahmen nahm die geplante Änderung der Meldepflicht nach dem neuen BDSG und die künftige Registerführung bei den Datenschutzaufsichtsbehörden ein. Hierzu hatte eine kleine Arbeitsgruppe am 13. September 2000 Vorüberlegungen angestellt und ein neues Meldeformular mit Merkblatt zur Meldepflicht nebst Anlagen (Entscheidungsbäume) dazu erarbeitet. Diese Materialien wurden beim Workshop ausführlich erörtert und mit kleinen Änderungen als erste Arbeitsgrundlage für die Datenschutzaufsichtsbehörden akzeptiert. Die erarbeiteten Unterlagen sind diesem Tätigkeitsbericht als Anlagen 1 bis 4 beigelegt. Es ist beabsichtigt, diese Unterlagen auch über das virtuelle Datenschutzbüro im Internet verfügbar zu machen (<http://www.datenschutz.de>).

Weitere Themen des Workshops waren die Verarbeitung von Daten aus den ärztlichen Arzneimittelverordnungen, ein Erfahrungsaustausch zum Recht der neuen Medien, Datenverarbeitungsprobleme im Zusammenhang mit dem Wirtschaftsschutz im High-Tech-Bereich, die Kooperation zwischen Datenschutzaufsichtsbehörden und wissenschaftlichen Einrichtungen sowie ein Informations- und Erfahrungsaustausch zur Durchführung von Bußgeldverfahren und der Bearbeitung von Eingaben.

Da die Datenschutzmaterie und damit die Aufgaben der Aufsichtsbehörden immer komplexer werden, wurde der Erfahrungsaustausch von allen Teilnehmern als hilfreich für eine möglichst effiziente Bewältigung der Aufgaben bewertet.

Der nächste Workshop wird vom Berliner Beauftragten für Datenschutz und Akteneinsicht organisiert werden.

#### **5. Datenverarbeitung bei Banken**

##### **5.1 Einholung von Auskunft-Daten zu anderen als den angegebenen Zwecken**

Die Möglichkeit, Bonitätsauskünfte über Dritte einholen zu können, scheint auch zu Missbrauch zu verleiten, obwohl die gesetzliche Verpflichtung besteht, bei einer Auskunftseinholung das berechtigte Interesse hieran zu dokumentieren (§ 29 Abs. 2 Satz 2 und 3 BDSG).

Ein Mitarbeiter eines Kreditinstitutes forderte von einer Wirtschaftsauskunftei Bonitätsauskünfte über ein einzelkaufmännisch geführtes Immobilienunternehmen an. Im Rahmen der Nachforschungen durch die Aufsichtsbehörde

konnte nicht abschließend geklärt werden, ob dem ein eigenes berechtigtes Interesse des Kreditinstitutes zugrunde lag, oder ob der Mitarbeiter diesen Zugang lediglich für seine privaten Interessen nutzte. Er stand nämlich zuvor schon wegen eines privaten Immobiliengeschäfts mit dem betroffenen Unternehmen in Verhandlungen.

Dabei spielte eine Rolle, dass das von dem Mitarbeiter geltend gemachte Anfrageinteresse "Anbahnung einer Geschäftsverbindung" dem Sachverhalt nach eher fraglich war und das Vorliegen dieses Interesses beim Kreditinstitut nicht eindeutig belegt werden konnte.

Das Kreditinstitut stellte sich jedoch auf den Standpunkt, dass die Einholung einer Auskunft durch den Mitarbeiter selbst dann rechtmäßig gewesen wäre, wenn er diese nur für seine privaten Kaufinteressen hätte nutzen wollen.

Dem war entgegen zu halten, dass Bonitätsauskünfte in der Tat von jedermann eingeholt werden können, es dafür jedoch erforderlich bleibt, dass die tatsächlichen Interessen benannt und keine unzutreffenden Gründe vorgeschoben werden. Die Einholung einer Bonitätsauskunft unter Ausnutzung eines Arbeitgeberanschlusses, bei der Arbeitgeberinteressen vorgeschoben werden, jedoch ein privater Anlass zugrunde liegt, ist als datenschutzrechtlich unzulässig anzusehen.

Möchte ein Arbeitgeber seinen Mitarbeitern die günstigen Konditionen für solche Auskünfte zugänglich machen, bedarf es entsprechender Vereinbarungen mit der Auskunftgeberin und detaillierter Regelungen gegenüber den Mitarbeitern, die auch die Nennung des tatsächlichen privaten Anfrageinteresses beinhalten.

Soweit der Arbeitgeber keine solche Regelung trifft, ist es seine Pflicht, verdeckte Anfragen für private Zwecke zu untersagen und für die Einhaltung dieses Verbots Sorge zu tragen.

## **5.2 Unzulässige Speicherung des Warnhinweises "arbeitslos"**

Der Kontosachbearbeiter einer Großbank hatte bei einem Kunden in ein freies Feld für Bemerkungen zum Girokonto den Hinweis "arbeitslos" eingegeben. Diese Bemerkung wurde dann bei einer anderen Filiale mehr oder weniger zwangsläufig als quasi Kontosperrung (trotz Guthabens) interpretiert. Die Organisationsrichtlinien der Bank sahen aber einen derartigen Hinweis überhaupt nicht vor.

Der Vermerk war offensichtlich nur für die Kontoführung bei der für den Kunden zuständigen Geschäftsstelle gedacht und konnte deshalb an anderer Stelle innerhalb der Bank nicht zutreffend interpretiert werden. Der Vermerk war nach einem Kundengespräch entstanden und könnte durchaus wohlmeinend gewesen sein. Beispielsweise könnte der Kontoführer hieraus eine besondere Rücksichtnahme bei finanziellen Schwierigkeiten ableiten.

Von finanziellen Schwierigkeiten war bei dem betroffenen Kunden aber nicht die Rede. Ohne eine besondere Einwilligung konnte eine derartige negativ interpretierbare Datenspeicherung nur als unzulässig bewertet werden.

Es bleibt einer Bank unbenommen, bei sich verringernden laufenden Zahlungseingängen - auch ohne Negativmerkmale - die Kreditlinie zu reduzieren.

Eine Rechtfertigung zur Speicherung des Negativmerkmals "arbeitslos" besteht somit in keinem Fall.

## **5.3 Datenweitergabe an einen freigestellten Mitarbeiter**

Für Banken ist es teilweise vorteilhaft, ausscheidende Mitarbeiter vorzeitig von ihrer Tätigkeit zu entbinden, obwohl das Beschäftigungsverhältnis noch andauert. Mit dieser Übergangsphase wird versucht, den Mitarbeiter noch einer Loyalitätspflicht gegenüber seinem Arbeitgeber zu unterwerfen und gleichzeitig die neuesten geschäftlichen Entwicklungen von dem Mitarbeiter fern zu halten.

Im Beschwerdefall handelte es sich offensichtlich um eine gütliche Trennung, denn es wurden in der Übergangsphase auch noch geschäftliche Probleme - hier weitere Kundenbetreuung - gemeinsam besprochen. Im Rahmen dieser Besprechungen wurden dem Mitarbeiter auch Kunden genannt, die für eine

externe Betreuung durch ein Unternehmen der Ehefrau des ausscheidenden Mitarbeiters in Frage kamen.

Generell wurden die betroffenen Kunden von der Bank angeschrieben bzw. angerufen und um Zustimmung für eine externe Betreuung gebeten. In einem Fall erreichte die Bank über einen längeren Zeitraum ihre Kundin nicht telefonisch. Deshalb beschaffte sich der ausscheidende Mitarbeiter die Telefonnummer der Kundin und rief sie von seinem Wohnsitz aus an. Die Kundin beschwerte sich darüber, dass ihre Daten an einen Mitarbeiter übermittelt wurden, der nicht mehr der Bank angehöre. Es konnte aber datenschutzrechtlich nicht von einer Datenübermittlung ausgegangen werden, da der Mitarbeiter immer noch (freigestellter) Beschäftigter der Bank war.

Allerdings war die Nutzung der Daten durch den freigestellten Mitarbeiter - quasi im Interesse seiner Ehefrau für deren Unternehmen - datenschutzrechtlich zu beanstanden. Selbst wenn man zugesteht, dass die Bank für ihre Kundin eine externe Betreuung suchte, gehörte es nicht mehr zu den Aufgaben des freigestellten Bankmitarbeiters, Bankkundenkontakte herzustellen.

#### **5.4 Keine Datenlöschung bei Geschlechtsumwandlung**

Eine Betroffene beschwerte sich darüber, dass nach einer Geschlechtsumwandlung noch Informationen über ihre frühere Identität als Mann bei der Bank gespeichert seien.

Soweit es die Kundenakte betraf, konnten keine Forderungen nach dem Bundesdatenschutzgesetz erhoben werden, es sei denn, die Akte enthielte Auszüge aus Dateien, die dem BDSG unterfallen (§§ 1 Abs. 2 Nr. 3, 27 Abs. 2 BDSG).

Bei den Konten des Betroffenen - hier ein Giro- und ein Sparkonto - war die Angelegenheit problematisch, da die Konten mit der männlichen Identität verbunden waren und gegebenenfalls auch gegenüber Aufsichtsbehörden - Bundesaufsichtsamt für das Kreditwesen, Steuerprüfung - Nachweise geführt werden müssen. Die Löschungswünsche der Betroffenen konnten deshalb nur mit einer Sperrung der Daten gemäß § 35 Abs. 3 Nr. 1 BDSG berücksichtigt werden. Die Integrität des Rechnungswesens einer Bank muss bestehen bleiben.

Damit eine weitere Sachbearbeitung völlig losgelöst von der alten (männlichen) Identität vonstatten gehen konnte, wurden die alten Konten aufgelöst und Konten mit der neuen (weiblichen) Identität eröffnet. Ein weiteres Entgegenkommen war nicht möglich und aus Sicht der Aufsichtsbehörde auch nicht notwendig. Mit den neu eröffneten Konten unter der weiblichen Identität hatte die Betroffene einen von ihrer Vergangenheit unbelasteten Neuanfang. Dem Offenbarungsverbot von § 5 Transsexuellengesetz wurde damit auch organisatorisch Rechnung getragen.

## **6. SCHUFA**

### **6.1 Keine Einwilligung und falscher Eintrag**

Systembedingt kann die Datenspeicherung bei der SCHUFA immer nur so gut sein, wie die weitgehend automatisiert erfolgenden Einmeldungen der angeschlossenen SCHUFA-Partner.

Im Beschwerdefall hatte ein Kreditnehmer zwar eingewilligt, dass über ihn bei der SCHUFA angefragt wird, aber er hatte nicht zugestimmt, seine Vertragsdaten an die SCHUFA zu übermitteln.

Solange Kreditvertragsdaten noch positiv sind - d.h. der Schuldner kommt regelmäßig seinen Verpflichtungen nach -, darf die Bank ohne eine gesonderte Einwilligung nach § 4 BDSG keine Vertragsdaten an die SCHUFA übermitteln. Die Datenübermittlung war damit schon aus diesem Grunde unzulässig. Darüber hinaus war die Meldung an die SCHUFA auch noch sachlich falsch, weil überhaupt kein Ratenkredit bestand, sondern stattdessen ein Aktienkauf finanziert wurde und später die Summe in einem Betrag fällig war.

Leider hatte die Bank - nach Reklamation des Kunden - den Falscheintrag bei der SCHUFA nur mit einem Erledigungsvermerk versehen lassen. Das sogenannte Qualitätsmanagement der Bank verdiente offensichtlich seinen Namen

nicht. Erst nach Intervention des Regierungspräsidiums Darmstadt wurde der unzulässige Krediteintrag gelöscht. Der betroffene Kunde hatte als Folge des falsch eingetragenen Kredites Schwierigkeiten bei der Kreditaufnahme für eine Eigentumswohnung. Er erhielt dann trotzdem seine Hypothek; bei den Zinsverhandlungen dürften die falschen SCHUFA-Eintragungen aber eine negative Rolle gespielt haben. Für die Durchsetzung eventueller Schadensersatzansprüche konnte nur auf § 8 BDSG (Umkehr der Beweislast) verwiesen werden.

## **6.2 SCHUFA-Eintrag über beantragte Zwangsvollstreckung**

Ein ausgehandelter Vergleichsentwurf über die Rückzahlung einer Geldforderung wurde von dem betroffenen Schuldner einseitig abgeändert, indem er die Ratenhöhe reduzierte. Dieses neue Vergleichsangebot hat die Gläubigerin nicht angenommen. Erst nach Beantragung der Zwangsvollstreckung durch die Gläubigerin wurde einvernehmlich ein (neuer) Vergleich erzielt - mit nunmehr reduzierten Raten. Der Betroffene forderte eine Löschung der an die SCHUFA gemeldeten Zwangsvollstreckung.

Dies war jedoch nicht gerechtfertigt, da die Forderung in der Hauptsache unstrittig war und die im Vergleich eingeräumte Ratenzahlung ein Zugeständnis der Gläubigerin an die Zahlungsschwierigkeiten des Schuldners war. Der gesamte Ablauf der Schuldenrückführung offenbarte nachhaltige Zahlungsschwierigkeiten.

Das Interesse des Betroffenen an einer Löschung des Zwangsvollstreckungseintrages musste deshalb gegenüber dem berechtigten Interesse der Gläubigerin an einer geregelten Rückzahlung zurückstehen. Vor allem galt es, potenzielle weitere Gläubiger auf die Zahlungsschwierigkeiten hinzuweisen und den Betroffenen vor weiterer (selbst verursachter) Verschuldung zu schützen. Konkret musste bei der SCHUFA lediglich die Vergleichssumme und die monatliche Ratenhöhe aufgenommen werden. Mit diesen zusätzlichen Daten relativierte sich der Zwangsvollstreckungseintrag, wodurch ein angemessener Interessenausgleich stattfand.

## **6.3 Personenverwechslung und trotzdem Entgeltzahlung für Eigenauskunft**

Fehler haben gelegentlich eine längere Vorgeschichte. Die Rechnung eines Versandhandelsunternehmens wurde nicht bezahlt und daraufhin ein Inkassodienst beauftragt. Der Inkassodienst fand keine zustellfähige Adresse und holte deshalb eine Auskunft beim Einwohnermeldeamt ein. Dieses gab jedoch wegen Namensgleichheit eine Auskunft über eine andere Person, sodass der Inkassodienst eine Mahnung an die vermeintliche Schuldnerin sowie eine Negativmeldung (Forderungsverkauf) an die SCHUFA sandte. Diese Negativmeldung erhielt auch die Hausbank der Betroffenen als Nachmeldung. In der Folge wurde der Betroffenen der Dispositionskredit gekündigt und die Eurocard zurückgefordert.

Da die Betroffene überhaupt nicht die Schuldnerin war und die geschilderten Vorgänge erst von zwei jeweils regional zuständigen Aufsichtsbehörden aufgeklärt werden mussten, entstand ein erheblicher Arbeitsaufwand für alle Beteiligten.

Die Negativmeldung hätte frühestens nach einer erfolglosen Mahnung an die SCHUFA übermittelt werden dürfen. Verwechslungen aber können leider immer wieder passieren. Betroffenen ist zu empfehlen, sich möglichst frühzeitig an die zuständige Aufsichtsbehörde zu wenden, damit Schaden begrenzt bzw. verhindert werden kann.

Im konkreten Fall war besonders ärgerlich, dass die Betroffene - trotz zweimaliger Aufforderung - von der SCHUFA das Auskunftsentgelt von 15 DM zunächst nicht zurückerhielt. Erst nach Aufforderung durch die Aufsichtsbehörde wurde auch dies erledigt. Die Betroffene wollte weiterhin über die sachlichen Korrekturen hinaus, dass die SCHUFA die "Anfrage des Versandhandels" im Datenbestand löscht. Die Anfrage bestand aber (wenn auch zur falschen Person), und aufgrund dessen wurde auch eine Auskunft erteilt. Diese Anfrage war zehn Tage lang allen zur Person anfragenden SCHUFA-Partnern ersichtlich; sie wird dann noch ein Jahr lang ausschließlich für Auskunftszwecke an die persönlich Betroffene vorgehalten. Das Auskunftsanfragedatum ist damit nach zehn Tagen gesperrt. Dem Löschungsbegehren nach

§ 35 BDSG konnte nicht entsprochen werden, weil eine Kontrolle der Aktivitäten der SCHUFA nach der Löschung des Anfragedatums nicht mehr möglich gewesen wäre. Die Aufsichtsbehörde muss ein Interesse daran haben, dass Auskünfte bei einer Auskunftstelle vollständig dokumentiert sind. Lediglich die Sperre des Anfragedatums kann auch sofort und nicht erst nach zehn Tagen erfolgen, wenn der Betroffene sich sofort bei der SCHUFA meldet und auf eine Personenverwechslung hinweist. Dies hat allerdings keine praktische Bedeutung, da der Betroffene in der Regel nicht zeitnah erfährt, wer wann über ihn angefragt hat.

#### 6.4 SCHUFA-Anfrage in jedem Fall?

Ein Kunde eines Baustoffhändlers wollte ursprünglich gegen Barzahlung beliefert werden, der beauftragte Baustoffhändler lieferte aber grundsätzlich nur gegen Rechnung. Wegen des angeblich bestehenden Lieferantenrisikos holte der Baustoffhändler bei der SCHUFA, ohne Kenntnis des Betroffenen, eine Auskunft ein. Weil der Betroffene bereits eine Barzahlung angeboten hatte, konnte eine Berechtigung für die SCHUFA-Abfrage nicht festgestellt werden. Die Abfrage hätte unterbleiben müssen.

Die Aufsichtsbehörde musste auch ein Kreditinstitut darauf hinweisen, dass bei Kontoeröffnungsanträgen nicht in jedem Fall SCHUFA-Anfragen gestartet werden dürfen, auch wenn dies in den Antragsbedingungen vorgesehen sein sollte. Bei Konten, die ausschließlich auf Guthabenbasis geführt werden, bedarf es einer solchen Auskunft nicht. Es obliegt den Kreditinstituten, ihre Mitarbeiter so zu instruieren, dass die erforderlichen Differenzierungen im Alltagsgeschäft getroffen werden.

### 7. Videoüberwachung

#### 7.1 Auslegung der geplanten Regelung in § 6 b BDSG n.F.

Wie bereits unter Nr. 3 ausgeführt wurde, informierten die Aufsichtsbehörden bei Beratungsanfragen zur Videoüberwachung auch über die geplante Neuregelung in § 6 b BDSG in der Fassung des Kabinettschlusses vom 14. Juni 2000. Auch bei Beschwerden versuchen sie, Lösungen herbeizuführen, die mit § 6 b BDSG n.F. zu vereinbaren sind.

Im Folgenden wird auf Auslegungsfragen eingegangen, die sich hierbei ergeben haben.

a) Zunächst war stets der Anwendungsbereich des § 6 b BDSG n.F. zu klären. § 6 b BDSG n.F. setzt voraus, dass es sich um "öffentlich zugängliche Räume" handelt. Ein öffentlich zugänglicher Raum ist jeder Bereich, der ohne besondere Voraussetzungen betreten werden kann. Er kann innerhalb oder außerhalb von Gebäuden liegen. Der Begriff stellt nicht auf die Eigentumsverhältnisse ab; es ist also unerheblich, ob es sich um ein öffentliches oder ein privates Grundstück handelt (vgl. Hinweise des Innenministeriums Baden-Württemberg zum Datenschutz für private Unternehmen und Organisationen [Nr. 39] vom 25. Januar 2001).

Zweifellos fallen daher Bahnsteige, Ausstellungsräume eines Museums, Verkaufsräume oder Schalterhallen darunter (BT-Drs. 14/4329, S. 38), ebenso Restaurants, Bowlingcenter oder Diskotheken.

Schwieriger ist die Anwendbarkeit hingegen bei Wohnanlagen. Der Treppen- und Eingangsbereich eines Zweifamilienwohnhauses ist sicher kein öffentlich zugänglicher Raum. Bei großen Wohnanlagen hingegen, die durch eine gewisse Anonymität gekennzeichnet sind, können die Eingangsbereiche, Treppenhäuser, Fahrstühle und Tiefgaragen als öffentlich zugängliche Bereiche bewertet werden, jedenfalls wenn die Bereiche auch von Externen ohne besondere Schwierigkeiten betreten werden können.

Nicht öffentlich zugängliche Bereiche wie Aufenthalts- und Sozialräume für Personal oder Produktionsbereiche von Unternehmen etc., zu denen nur die Arbeitnehmer Zugang haben, sind nicht Gegenstand der Regelung des § 6 b BDSG n.F. Bezüglich des Arbeitnehmerbereiches sollen im Rahmen eines Arbeitnehmerdatenschutzgesetzes besondere Regelungen getroffen werden. Solange ein solches noch nicht in Kraft getreten ist, bleibt nur die Orientierung an der arbeitsrechtlichen Rechtsprechung sowie an § 28 BDSG n.F.,

denn für die von § 6 b BDSG n.F. nicht erfassten Videoüberwachungen soll § 28 BDSG n.F. einschlägig bleiben (Christians, RDV-Sonderdruck 4/2000, S. 15). Im Übrigen ist die zivilrechtliche Rechtsprechung zur Zulässigkeit von Videoüberwachungsanlagen zu berücksichtigen. Danach ist nach umfassender Abwägung unter Heranziehung grundrechtlicher Positionen und unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes zu bewerten, ob die Videoüberwachung einen unzulässigen Eingriff in das allgemeine Persönlichkeitsrecht darstellt und einen Schadensersatzanspruch nach § 823 BGB und/oder einen Unterlassungs- und Beseitigungsanspruch nach § 1004 BGB begründet. Soweit die Aufnahmen verbreitet werden, ist stets auch das Kunsturhebergesetz zu beachten.

b) Unter § 6 b BDSG n.F. fällt bereits die Videobeobachtung, d.h. für die datenschutzrechtliche Relevanz der Videoüberwachung kommt es nicht darauf an, ob das Bildmaterial auch anschließend gespeichert wird (BT-Drs. 14/4329, S. 38).

Unerheblich ist auch, ob eine analoge oder digitale Kameratechnik eingesetzt wird, denn die Vorschrift greift - wie in der Begründung der Bundestagsentscheidung vom 6. April 2001 klargestellt wurde - insoweit über den Anwendungsbereich des BDSG n.F., wie er in § 1 Abs. 2 Nr. 3 BDSG n.F. definiert ist, hinaus, als sie nicht voraussetzt, dass die durch eine Beobachtungsmaßnahme gewonnenen Daten unter Einsatz von oder für Datenverarbeitungsanlagen erhoben wurden.

c) Die Videobeobachtung ist nach § 6 b BDSG n.F. nur zulässig, soweit sie zur Aufgabenerfüllung öffentlicher Stellen oder zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Unter dem "Hausrecht" ist die Gesamtheit der rechtlich geschützten Befugnisse, über Haus und Hof frei zu verfügen, zu verstehen. Hierunter fällt auch das Recht, Maßnahmen gegen Diebstahl oder Beschädigungen des Eigentums zu ergreifen und Hausverbote gegen Personen auszusprechen, welche entsprechende Verhaltensregeln nicht einhalten oder die Bewohner oder andere Besucher verletzen, gefährden oder bedrohen. Die zu solchen Zwecken vorgenommene Videobeobachtung muss jedoch erforderlich und nach Abwägung mit den Belangen der Betroffenen auch verhältnismäßig sein.

Das Motiv einer allgemeinen abstrakten Gefahrenvorsorge reicht nicht. Vielmehr müssen belegbare Tatsachen die Annahme rechtfertigen, dass schwerwiegende Beeinträchtigungen der durch das Hausrecht geschützte Interessen drohen. Bei der Abwägung, ob die schutzwürdigen Interessen der Betroffenen überwiegen, kommt es darauf an, wer überhaupt zum Kreis der Betroffenen gehört (Arbeitnehmer, Besucher etc.) und inwieweit diese Personen in zeitlicher und räumlicher Hinsicht einem Überwachungsdruck ausgesetzt sind.

Je umfassender und unausweichlicher der Überwachungsdruck ist, desto höheres Gewicht müssen die Interessen haben, die mittels der Videoüberwachung geschützt werden sollen bzw. desto stärker muss deren Bedrohung sein.

Bei der Abwägung ist auch relevant, inwieweit der Kreis derjenigen Personen, welche die Bilder sehen, begrenzt ist.

Die Erforderlichkeit zur Erfüllung "berechtigter Interessen" ist restriktiv auszulegen. Sie liegt regelmäßig nicht vor, wenn die Beobachtung der Hauptzweck oder ein wesentlicher Nebenzweck der Geschäftstätigkeit ist. Webcams sind besonders kritisch zu bewerten, (s. hierzu Nr. 7.9).

d) Die Videoüberwachung ist nach § 6 b Abs. 2 BDSG n.F. nur zulässig, wenn der Vorgang für die Betroffenen transparent ist. Sowohl der Umstand der Beobachtung als auch die verantwortliche Stelle sind daher durch geeignete Maßnahmen erkennbar zu machen. Dies kann durch deutlich wahrnehmbare Hinweisschilder geschehen. Im Hinblick auf etwaige Sprachprobleme bietet sich die Verwendung von Piktogrammen an - verbunden mit schriftlichen Hinweisen über die verantwortliche Stelle, falls nicht aus den sonstigen Umständen ersichtlich ist, wer diese Stelle ist. Nur wenn die Kameras so groß und an so deutlich sichtbarer Stelle angebracht sind, dass die Betroffenen sie nicht übersehen können, und wenn offensichtlich ist, wer

verantwortliche Stelle ist, könnte auf entsprechende Hinweisschilder oder sonstige schriftliche Informationen verzichtet werden.

Gleichwohl empfiehlt sich u.U. eine entsprechende Beschilderung, damit die Betroffenen sich der Videoüberwachung bewusst sind, bevor sie sich in das Blickfeld der Kameras begeben.

Welche Maßnahmen konkret zu treffen sind, um die Transparenz sicherzustellen, richtet sich auch nach den schutzwürdigen Interessen der Betroffenen.

Im Arbeitnehmerbereich ist daher grundsätzlich eine vorherige schriftliche Information geboten.

e) Nach § 6 b Abs. 3 BDSG n.F. ist die Verarbeitung oder Nutzung der im Einklang mit § 6 b Abs. 1 BDSG n.F. erhobenen Daten nur zulässig, wenn dies zum Erreichen des verfolgten Zwecks erforderlich ist.

Der Entwurf vom 14. Juni 2000 sah in Abs. 3 - im Gegensatz zu Abs. 1 - nicht explizit eine Abwägung mit den schutzwürdigen Interessen vor. Die Aufsichtsbehörden waren jedoch der Auffassung, dass sich dieses Erfordernis bereits daraus ergibt, dass Abs. 3 an Abs. 1 anknüpft, und außerdem aus dem Umkehrschluss aus § 6 b Abs. 4 BDSG n.F., wonach die Daten unverzüglich zu löschen sind, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen des Betroffenen einer weiteren Speicherung entgegenstehen. In der am 23. Mai 2001 in Kraft getretenen Fassung ist nun klargestellt, dass eine weitere Verarbeitung oder Nutzung der Daten nur zulässig ist, wenn keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Außerdem wurde explizit geregelt, dass Zweckänderungen nur zulässig sind, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit, sowie zur Verfolgung von Straftaten erforderlich ist.

Im Folgenden werden zur Vertiefung einige Einzelfälle dargestellt, mit denen sich die Aufsichtsbehörden befasst haben.

## 7.2 Wohnhaus-Videoüberwachung auf TV-Sonderkanal

Im Eingangsbereich einer Wohnanlage, die einer gemeinnützigen Wohnungsbau-gesellschaft gehört, war auf Wunsch einiger Mieter eine Videoüberwachung installiert worden.

Die Kamerabilder wurden in das hauseigene Fernseekabelnetz eingespeist und konnten so von jedem Bewohner über sein Fernsehgerät eingesehen werden. Da jedoch ein Streit über die Zulässigkeit dieser Videoüberwachung entbrannte, bat ein Aufsichtsratsmitglied (Vertreterin einer Stadt) die Aufsichtsbehörde um eine datenschutzrechtliche Bewertung. Leider wurde das konkrete Objekt nicht benannt. Daher übersandte die Aufsichtsbehörde zunächst nur Informationen über die einschlägige zivilrechtliche Rechtsprechung und die Novelle des BDSG und verwies darauf, dass danach eine umfassende Abwägung zu treffen sei.

Dabei kommt es unter anderem darauf an, ob konkrete Anhaltspunkte für einen starken Vandalismus oder eine Gefährdung der Bewohner oder Besucher bestehen oder ob es sich dabei um überwiegend alte oder behinderte Menschen handelt, die besonders schutzbedürftig gegenüber etwaigen Belästigungen oder tätlichen Übergriffen sind. Selbst wenn man nach einer entsprechenden Abwägung zu dem Ergebnis käme, dass eine Videobeobachtung des Eingangsbereiches zulässig wäre, so ist jedoch die Einspeisung sämtlicher Bilder in einen Haus-Fernsehkabelkanal besonders kritisch zu sehen und letztlich unverhältnismäßig. Jeder Hausbewohner könnte jederzeit beobachten, wann die Nachbarn das Haus betreten oder verlassen, in welchem Zustand sie sich befinden (betrunken?, streitend?), von wem sie begleitet werden und von wem sie wie lange Besuch erhalten. Durch Aufzeichnung auf einen Videorekorder könnte die Beobachtung auch nachts erfolgen und die Videobänder könnten über Jahre aufbewahrt werden.

Grundsätzlich ist nicht ausgeschlossen, dass eine Videokamera nebst Fernsehgerät als eine Art "verlängerter Türspion" genutzt wird. Es muss jedoch grundsätzlich sichergestellt sein, dass der jeweilige Mieter/Bewohner nur seine Besucher sehen kann. (Ebenso LfD Nds., TB 1999/2000, S. 28).

Damit die Einhaltung des Lösungsgebotes des § 6 b Abs. 4 BDSG n.F. gewährleistet ist und kontrolliert werden kann, wäre eine zentrale Lösung, bei der beispielsweise nur der Pförtner oder der Hausmeister die Bilder sieht, sinnvoll.

Der Aufsichtsrat der Wohnungsbaugesellschaft entschied sich schließlich für den Abbau der Videoanlagen. Statt dessen sollte für eine verstärkte Präsenz der Hausmeister mit entsprechenden Kontrollgängen gesorgt werden. Außerdem sollte ein nebenamtlicher Hauswart bestellt werden, um den Sicherheitsbedürfnissen aller Mieter gerecht zu werden.

### **7.3 Videoüberwachung im Fahrstuhl**

Ein weiterer Fall betraf ebenfalls eine Videoüberwachung in einer großen Wohnanlage. Ein betroffener Mieter beschwerte sich darüber, dass selbst im Fahrstuhl eine Videokamera installiert sei.

Bei einer Ortsbesichtigung stellte das zuständige Regierungspräsidium Darmstadt fest, dass es sich bei der Wohnanlage um einen extremen sozialen Brennpunkt handelte, der durch eine hohe Kriminalität gekennzeichnet war. Spuren der Verwüstung und Sachbeschädigung waren überall zu sehen. Die Videoüberwachung war eine von vielen Maßnahmen, um die Sachbeschädigung einzudämmen und zu mehr Sicherheit, auch für die Bewohner, zu gelangen - unter anderem wurden auch abends verstärkt Kontrollgänge durch das Wachpersonal durchgeführt. Die Videoaufzeichnungen konnten nur vom Hausmeister eingesehen werden und wurden nach kurzer Zeit gelöscht bzw. überspielt.

Die Videobeobachtung war somit ein erforderliches und verhältnismäßiges Mittel zur Wahrnehmung des Hausrechts. Schutzwürdige Interessen der Bewohner und Besucher überwogen demgegenüber nicht. Auch die kurzzeitige Speicherung war zur Beweissicherung erforderlich, zumal der Hausmeister das Videobild nicht pausenlos betrachten konnte.

Fraglich war jedoch, ob für ausreichende Transparenz gesorgt war.

Einige Kameras im Eingangsbereich waren sehr groß und deutlich sichtbar angebracht. Im Fahrstuhl konnte die Aufsichtsbehörde jedoch keine Kamera entdecken. Erst auf entsprechenden Hinweis des Hausmeisters wurde festgestellt, dass eine Miniaturkamera von der Größe eines Stecknadelkopfes in einem Buchstaben eines Rauch-Verbots-Schildes versteckt war. Die gelieferten Bilder waren relativ unscharf. Jedoch konnte durchaus beobachtet werden, wer sich in dem Fahrstuhl befindet.

Ein Hinweisschild im Eingangsbereich machte auf die Videoüberwachung aufmerksam. Zwar war der Fahrstuhl nicht explizit genannt, doch war der überwachte Bereich hinreichend klar eingegrenzt umschrieben.

Wenngleich ein Fahrstuhl von den Benutzern als Bereich relativer Privatheit empfunden werden kann und somit grundsätzlich hohe Anforderungen an die Erkennbarkeit der Videoüberwachung zu stellen sind, so wurde das Hinweisschild im konkreten Fall doch als ausreichend bewertet, weil der angestrebte Zweck anders nicht hätte erreicht werden können. Gerade auch der Fahrstuhl zeigte deutliche Spuren des Vandalismus. Wäre die Kamera sichtbar gewesen, so wäre sie mit ziemlicher Sicherheit - unbemerkt - als erstes zerstört worden.

Der Beschwerdeführer war übrigens - wie sich herausstellte - mittels der Videoüberwachung der Beschädigung des Fahrstuhls überführt worden.

### **7.4 Löschung der Videoaufzeichnung und Zugriffsschutz nicht gewährleistet**

Auch in einem dritten Fall beschwerte sich ein Mieter über die Videoüberwachung in einer großen Wohnanlage. Diese bestand aus fünf Hochhäusern und - wie im vorgenannten Fall - war offensichtlich, dass eine hohe Kriminalitätsrate bestand. Zum Zeitpunkt der Ortsbesichtigung hob die Polizei ein Waffenlager in einer der Wohnungen aus. Die Videobeobachtung war auf die Hauseingänge begrenzt und im Grundsatz gerechtfertigt.

Wenngleich die Kameras relativ leicht zu entdecken waren, hielt die Aufsichtsbehörde gleichwohl die Anbringung von Hinweisschildern für geboten.

Die von insgesamt 16 Videokameras in digitaler Technik aufgenommenen Bilder liefen auf mehreren Bildschirmen zusammen, die in einem Raum im Erdgeschoss eines der Hochhäuser aufgestellt waren. Dieser Raum dient auch den Mietparteien dazu, mit ihren Anliegen an die Hausverwaltung heranzutreten. Daher war der Raum ständig geöffnet und in der Regel mit zwei Mitarbeitern besetzt. Die Möglichkeit, die Bildschirme einzusehen, bestand letztendlich für jeden Mieter, aber auch für Fremde, wie bei der Besichtigung der Anlage festgestellt werden konnte. Es existierten keinerlei Regelungen über die Aufbewahrungsdauer der Aufzeichnungen bzw. die Löschung der Daten und auch keine Regelung bzgl. der Zugriffsrechte für diese Daten.

Daher wurde das Unternehmen aufgefordert, entsprechende Zutritts- und Zugriffsregelungen zu erstellen, sowie für die unverzügliche Löschung der Aufzeichnungen (nach spätestens 72 Stunden) zu sorgen. Außerdem wurde die nach § 36 Abs. 1 Satz 1 BDSG erforderliche Bestellung eines Datenschutzbeauftragten angemahnt.

### **7.5 Überwachung von Schuhreparatur-Filialen in Kaufhäusern**

Auf eine Videoüberwachung am Arbeitsplatz wurde die Aufsichtsbehörde durch den Hinweis eines Pressevertreters aufmerksam. An diesen hatte sich ein betroffener Mitarbeiter gewandt. Er war von seinem Arbeitgeber, einem auf Schuh-Reparaturen spezialisierten Unternehmen mit zahlreichen Filialen in Einkaufszentren und Kaufhäusern, darüber informiert worden, dass in allen Filialen Videokameras installiert würden.

Auf Nachfragen bestätigte das Unternehmen gegenüber der Aufsichtsbehörde, dass zwar alle Filialen mit Videokameras bzw. Attrappen ausgestattet werden sollten, jedoch nur in wenigen Filialen, in denen sich ein konkreter Diebstahls- bzw. Unterschlagungsverdacht ergeben habe, tatsächlich eine Videobeobachtung erfolgen solle. Zur Ermittlung eines solchen konkreten Verdachts war ein gestuftes Vorgehen vorgesehen. Dieses war in der Tat zur Eingrenzung und Erhärtung eines Diebstahls- und Unterschlagungsverdachts geeignet. Da in den einzelnen Filialen nur eine sehr geringe Zahl an Mitarbeitern beschäftigt waren, war damit auch eine klare personelle Begrenzung der Maßnahme gegeben.

Die Videobeobachtung sollte auf den Theken- und Kassenbereich ausgerichtet und damit zugleich räumlich begrenzt werden.

Insgesamt konnte die Videobeobachtung daher bezüglich der Mitarbeiter in den betroffenen Filialen als erforderlich und verhältnismäßig bewertet werden.

Die Aufsichtsbehörde forderte jedoch, dass technisch sichergestellt werden müsse, dass tatsächlich nur diejenigen Filialen, welche aufgrund konkreter Verdachtsmomente in den "Fokus" genommen wurden, videoüberwacht werden. Deshalb sollte die Software so ausgelegt sein, dass die Verbindung ausschließlich zu den Kameras in den entsprechenden Filialen hergestellt wird. Es müsste also eine Programmeingabe erforderlich sein, um die Verbindung herzustellen.

Hierzu sollte das "Vier-Augen-Prinzip" beachtet werden, indem nicht nur der mit der Videobeobachtung betraute Mitarbeiter (im konkreten Fall wollte der Geschäftsführer die Beobachtung zunächst selbst vornehmen), sondern ein weiterer Mitarbeiter, möglichst der betriebliche Datenschutzbeauftragte, jeweils ein Passwort eingeben.

Welche Filiale in den Fokus genommen wird, ist jedenfalls mit dem betrieblichen Datenschutzbeauftragten abzustimmen und von diesem zu dokumentieren.

Dass nicht nur eine Videobeobachtung, sondern auch eine Aufzeichnung erfolgen sollte, erschien akzeptabel, da die Aufzeichnung durch automatisches Überspielen gelöscht werden sollte, es sei denn, es hatte sich ein konkreter Vorfall (Straftat) ergeben.

Problematisch war jedoch, dass das Unternehmen nicht bereit war, die Mitarbeiter konkret darüber zu informieren, welche Filiale jeweils unter Videoüberwachung steht.

Bezüglich der im "Fokus" befindlichen Filialen war dies hinnehmbar, da die betroffenen Mitarbeiter aufgrund des gestuften Verfahrens damit rechnen mussten, denn dieses sieht unter anderem vor, dass der Mitarbeiter in einem Gespräch auf die Unregelmäßigkeiten hingewiesen wird und eine Verwarnung erhält. Im übrigen lässt die arbeitsgerichtliche Rechtsprechung als ultima ratio sogar eine verdeckte Videoüberwachung zu, d.h. wenn sich ein konkreter Diebstahlsverdacht nicht anders aufklären lässt. Angesichts der vorgesehenen präzisen Ermittlungen in dem gestuften Verfahren wären diese Voraussetzungen wohl sogar gegeben gewesen. Jedenfalls aber war die allgemeine Information insoweit ausreichend.

Bezüglich der Mitarbeiter in den anderen Filialen bedeutete die Ankündigung der Videoüberwachung und die Installation der Kameras jedoch, dass sie sich einem ständigen Überwachungsdruck ausgesetzt fühlen, obwohl gegen sie möglicherweise keinerlei Diebstahls-/Unterschlagungsverdacht vorliegt.

Nach eingehender Diskussion erklärte sich das Unternehmen daher wenigstens bereit, alle Mitarbeiter über das gestufte Verfahren zu unterrichten. Darüber hinaus haben alle Mitarbeiter die Möglichkeit, sich beim betrieblichen Datenschutzbeauftragten anhand der bei ihm geführten Dokumentationen im Nachhinein zu informieren, ob ihre Filiale unter Videoüberwachung stand. Hierfür werden die Dokumentationen ein viertel Jahr lang aufbewahrt, danach vernichtet.

Wenn bei der Videoüberwachung eine Straftat festgestellt wurde, wird dies dem betroffenen Mitarbeiter sofort vorgehalten.

Da auch Kunden in dem Aufnahmebereich der Kameras gelangen können, erklärte sich das Unternehmen bereit, durch ein Piktogramm hierauf hinzuweisen.

Die weitere Umsetzung des Vorhabens bleibt abzuwarten und zu beobachten, wobei wegen der Verlagerung der Unternehmenszentrale aus dem Rhein/Main-Gebiet nach Nordrhein-Westfalen nun die dortige Landesdatenschutzbeauftragte zuständig ist.

## 7.6 Überwachung von Freizeitanlagen

Der Aufsichtsbehörde wurde bekannt, dass eine Bowling-Center-Kette, deren Muttergesellschaft sich in den USA befindet, ihre Betriebsstätten durch Videoaufzeichnungen überwachen lassen würde.

Überprüfungen vor Ort in zwei Betriebsstätten ergaben, dass die grundsätzliche Entscheidung für die nicht digitale Videoüberwachung in der Unternehmenszentrale getroffen worden war, da es häufig zu Tötlichkeiten der Kunden bzw. Beschädigungen gekommen war und auch Raubüberfälle stattgefunden hatten. Diese Entscheidung der Zentrale wurde jedoch von der Leitung vor Ort in den einzelnen Betriebsstätten unterschiedlich umgesetzt.

Eine Betriebsstätte wurde mit zwei Kameras für den Empfangsbereich und den Thekenbereich der Gastronomie überwacht. Das Aufzeichnungsgerät befand sich im Büroraum des Betriebsleiters, der nach Bekunden der Mitarbeiter die 24-Stunden-Aufzeichnungen häufiger beobachtete. Darüber hinaus waren jedoch auch Installationen vorhanden, wodurch das gesprochene Wort abgehört und aufgezeichnet wurde. Im Empfangsbereich wies ein kaum wahrnehmbares Schild in Englisch auf die Videoinstallation hin.

In der zweiten Betriebsstätte erfolgte die Überwachung durch vier Kameras mit 24-Stunden-Aufzeichnungen, allerdings ohne Tonüberwachung, gerichtet auf Empfangsbereich, Spielbereich und Außenbereich. Hinweisschilder auf die Überwachung waren nicht vorhanden, jedoch konnten hier auch die Besucher die Bildschirme im Empfangsbereich einsehen.

Die Aufsichtsbehörde wies die zentrale Geschäftsleitung zunächst darauf hin, dass sie die Tonüberwachung im Hinblick auf § 201 StGB für unzulässig halte.

Bezüglich der Videoüberwachung von Besuchern und Arbeitnehmern verwies sie auf die zivilrechtliche Rechtsprechung und die BDSG-Novelle.

Danach ist die unzureichende Kenntlichmachung der Videoüberwachung zu bemängeln.

Wenngleich die konkrete Aufzeichnungsdauer nicht zu beanstanden war, sollten die Aufzeichnungen nur im Bedarfsfall und nur von den dafür verantwortlichen Personen angesehen werden. Soweit die Geschäftsleitung sich dies vorbehalten hat, muss sie ihrerseits Sorge dafür tragen, dass unbefugte Dritte keinen Zugang zu den Aufnahmen haben.

Die Überprüfungen ergaben jedoch auch, dass das Unternehmen aufgrund der umfangreichen Verarbeitung personenbezogener Daten durch Buchungen, Dauerkartenvergabe, Wettbewerbsorganisation, Erstellung von Mitarbeiterplänen, sowie die Bearbeitung der Personalverwaltung und Abrechnung eines betrieblichen Datenschutzbeauftragten bedurfte, der unverzüglich bestellt werden musste.

Es bleibt abzuwarten, ob durch dessen Tätigkeit auch einheitliche Regelungen für alle Betriebsstätten und deren Videoüberwachung realisiert werden.

### 7.7 Webcam

Ein Marketingunternehmen installierte an seinem Bürogebäude eine digitale Kamera, um die gegenüberliegende Straßenseite und den Eingang in das dort befindliche Rathaus aufzunehmen. Die Aufnahmen sollten auf einen ans Internet angeschlossenen Rechner zum Abruf aus dem Internet bzw. genauer aus dem World Wide Web (WWW) bereitgestellt werden.

Damit wollte das Unternehmen für sich werben. Ferner war beabsichtigt, im Rathaus einen Bildschirm aufzustellen, um die Besucher des Rathauses mit den Aufnahmen zu unterhalten. Ein Bediensteter der Stadtverwaltung fragte jedoch zuvor die Aufsichtsbehörde nach der grundsätzlichen Zulässigkeit - auch im Hinblick auf die BDSG-Novelle.

Im Hinblick auf § 6 b BDSG n.F. stellt sich zunächst die Frage nach der Erforderlichkeit.

Die Beobachtung mittels der so genannten Webcam dient weder der Aufgabenerfüllung einer öffentlichen Stelle noch der Wahrnehmung des Hausrechts. Auch wenn man das Werbeinteresse des Unternehmens möglicherweise als berechtigtes Interesse i.S.d. § 6 b Abs. 1 Nr. 3 BDSG n.F. anerkennen kann, überwiegen jedoch nach Ansicht der Aufsichtsbehörde die Interessen der betroffenen Passanten und Rathausbesucher deutlich das Werbeinteresse des Unternehmens - vorausgesetzt, die Aufnahmen sind so scharf, dass Personen erkennbar sind und damit eine Personenbeziehbarkeit besteht.

Das Problem bei den Webcams liegt vor allem in der weltweiten Verbreitung der Bilder und der nahezu unbegrenzten Verfügbarkeit und Weiterverwendung durch jeden Internet-Nutzer: Die Bilder können heruntergeladen und gespiegelt, d.h. im Internet vervielfältigt werden. Darüber hinaus können Internet-Nutzer durch spezielle Software Vergrößerungen vornehmen. Es besteht also keinerlei Kontrollmöglichkeit mehr über die weitere Verwendung der Bilder. Dass das Lösungsgebot des § 6 b BDSG n.F. nicht erfüllt werden kann, ist offensichtlich.

Ob man bei sehr deutlichen Hinweisschildern (und guter Erkennbarkeit und Abgrenzung des Aufnahmebereiches) eine Einwilligung "in anderer Form" i.S.d. § 4 Abs. 2 Satz 2 BDSG annehmen könnte, wenn Betroffene den Bereich trotz Kenntnis der Webcam betreten, erscheint äußerst fraglich. Jedenfalls wenn es sich - wie im konkreten Fall - um eine öffentliche Straße handelt und außerdem kein anderer Zugang zu dem Rathaus besteht, fehlt es bereits an der für eine wirksame Einwilligung grundsätzlich erforderlichen Freiwilligkeit (vgl. auch Hinweise des Innenministeriums Baden-Württemberg Nr. 39, C. vom 25. Januar 2001).

Bei einer anderen Anfrage wäre dies schon eher diskutabel gewesen, aber letztlich auch zu verneinen: Ein Diskothekenbesitzer wollte Bilder seiner Diskothek, insbesondere der Tanzfläche, zu Werbezwecken ins WWW stel-

len. Im Eingangsbereich der Diskothek sollten entsprechende Hinweisschilder aufgestellt werden.

Man mag zwar argumentieren, dass der Besuch einer Diskothek nicht ebenso notwendig ist wie die Nutzung einer öffentlichen Straße oder der Besuch eines Rathauses. Gleichwohl kann das Betreten der Diskothek trotz Hinweises auf die Webcam nicht als besondere Form der Einwilligung gewertet werden. Abgesehen davon, dass konkludente Einwilligungen problematisch sind, ist die Erkennbarkeit der Videobeobachtung nach § 6 b Abs. 2 BDSG n.F. nur eine zusätzliche bzw. eine Mindestvoraussetzung für die Zulässigkeit der Videobeobachtung, sodass daraus noch kein Erlaubnistatbestand abgeleitet werden kann.

Eine andere Bewertung würde sich nur ergeben, wenn der Diskothekenbesitzer ein Wahlrecht einräumen würde, beispielsweise in dem nur in einem von mehreren Tanzräumen eine Webcam installiert wäre. Besucher könnten sich dann - nach entsprechender klarer Information - entscheiden, ob sie sich im WWW zur Schau stellen wollen oder nicht. Dann wäre die Datenverarbeitung und Nutzung bereits aufgrund der Interessenabwägung nach § 6 b Abs. 1 Nr. 3 und Abs. 3 BDSG n.F. zulässig (sodass es nicht der "Konstruktion" einer Einwilligung bedarf).

## **8. Neue Medien, Internet-Provider**

### **8.1 Unzulässig lange Speicherung von Nutzungsdaten**

Durch den Hinweis eines Journalisten wurde die Aufsichtsbehörde auf folgenden Fall aufmerksam.

Ein in Berlin ansässiges Unternehmen bietet im Internet aktuelle Börseninformationen (so genannte Realtime-Kursinformationen) an. Wer diese Dienstleistung in Anspruch nehmen will, muss sich bei dem Unternehmen unter Angabe seines Namens und seiner Adresse registrieren. Das Unternehmen unterrichtete auf der Anmeldeliste darüber, dass die Daten an die Deutsche Börse AG weitergeleitet würden und berief sich auf seine vertragliche Verpflichtung gegenüber der Deutschen Börse AG.

Da das Regierungspräsidium Darmstadt für die Deutsche Börse AG zuständig ist, bearbeitete es die Eingabe in Abstimmung mit dem für das Berliner Unternehmen zuständigen Berliner Beauftragten für Datenschutz und Akteneinsicht (BBDA). Gegenüber dem BBDA gab das Unternehmen an, die Zugriffe der Nutzer auf Kursinformationen zu protokollieren und zehn Jahre lang personenbezogen zu speichern und darüber hinaus der Deutschen Börse AG auf Verlangen Einsicht in diese Protokolldateien zu gewähren. Auch insoweit berief sich das Unternehmen auf vertragliche Vorgaben durch die Deutsche Börse AG.

Das Angebot, Börsenkurse im Internet abzufragen, stellt einen Teledienst i.S.d. § 2 Abs. 2 Nr. 2 TDG dar. Sowohl die Erhebung, Speicherung und Übermittlung der Registrierungsdaten als auch die Verarbeitung der Daten über die Kursabfragen sind der Teledienstebene zuzuordnen.

Die Erhebung von personenbezogenen Daten im Rahmen eines Registrierungserfordernisses steht grundsätzlich im Widerspruch zu dem Gebot des § 4 Abs. 1 TDDSG. Danach hat der Diensteanbieter dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist.

Registrierungsdaten dürfen als Bestandsdaten nach § 5 Abs. 1 TDDSG nur erhoben, verarbeitet und genutzt werden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses mit dem Anbieter über die Nutzung von Telediensten erforderlich sind.

Im konkreten Fall bestand keine Vertragsbeziehung zwischen den Nutzern und der Deutschen Börse AG, sondern nur zwischen den Nutzern und dem Berliner Unternehmen. Da der Dienst für die Nutzer kostenlos war und durch Werbeeinblendungen finanziert wurde, war an sich überhaupt keine Notwendigkeit ersichtlich, Bestandsdaten zu erheben.

Folgender Hintergrund war jedoch zu beachten:

Die Deutsche Börse AG bietet urheberrechtlich geschützte Kursinformationen zu börsenmäßig gehandelten Finanzinstrumenten (Aktien, Anleihen, Optionen etc.) an. Bei diesen Kursinformationen handelt es sich um aufbereitete Informationen zu Börsengeschäften sowie um abgeleitete Kursinformationen, wie insbesondere Indizes, die von der Deutschen Börse AG fortlaufend berechnet werden und zu deren Gunsten auch markenrechtlich geschützt sind (z.B. DAX, REX, NEMAX 50). Diese Kursinformationen werden von der Deutschen Börse AG stets aktuell in Echtzeit (realtime) angeboten und haben einen erheblichen kommerziellen Wert. Bei den Nutzern der Daten wird zwischen zwei Kategorien unterschieden, nämlich "Informationsanbietern" und "Endnutzern". Bei Informationsanbietern (so genannten Vendoren) handelt es sich um Unternehmen, die ihrerseits die Kursinformationen in eigene Dienstleistungen einbinden und weiterverteilen.

Mit sämtlichen Vendoren bestehen Kursvermarktungsverträge, die insbesondere Art und Umfang der Weiterleitung der Kursinformationen und die hierfür an die Deutsche Börse AG zu zahlende Vergütung regeln. Die Vendoren generieren aus den Kursinformationen unterschiedliche Informationsprodukte, die sich in der Art der Informationen und der Aktualität der Daten unterscheiden. Zeitverzögerte Kursinformationen (mindestens 15 Minuten alt) sind für professionelle Nutzer nicht mehr interessant und können daher von den Vendoren frei über das Internet (ohne Registrierungsanforderungen) zur Verfügung gestellt werden. Da bei den wesentlich wertvolleren Realtime-Informationen die Gefahr besteht, dass Endnutzer diese unautorisiert weiterleiten und in unlauteren Wettbewerb zu anderen Vendoren treten, verlangt die Deutsche Börse AG von den Vendoren, diese Realtime-Informationen nur innerhalb von geschlossenen Benutzergruppen weiterzuleiten, d.h. jeder Endnutzer muss sich namentlich unter Angabe seiner Adresse beim jeweiligen Vendor registrieren lassen.

Die Deutsche Börsenaufsicht sprach sich gegenüber der Aufsichtsbehörde gegen anonyme Online-Abfragen von Realtime-Kursen aus - wegen der Gefahr des manipulativen Eingriffs in das Börsengeschehen.

Vor diesem Hintergrund hielt die Aufsichtsbehörde es für vertretbar, dass die namentliche Registrierung gefordert wurde.

Entgegen der missverständlichen Information auf der Registrierungsseite des Berliner Unternehmens wurden die Registrierungsdaten nicht routinemäßig an die Deutsche Börse AG übermittelt, sondern nur in den Fällen, in denen der konkrete Verdacht besteht, dass der Nutzer entgegen seiner vertraglichen Vereinbarung mit dem Unternehmen die Kursinformationen kommerziell verwertet, d.h. an andere weiterverkauft. Der Nutzer kann dann mit der Deutschen Börse AG selbst einen Vendor-Vertrag (mit entsprechender Gebührenvereinbarung!) schließen oder er erhält keine Daten mehr. Diese Übermittlung an die Deutsche Börse AG war nicht zu beanstanden.

Die Verarbeitung der Nutzungsdaten war jedoch unverhältnismäßig und mit § 6 TDDSG nicht zu vereinbaren.

In der Tat hatte die Deutsche Börse AG den Vendor vertraglich verpflichtet, alle Einzelkursabfragen zehn Jahre lang aufzubewahren und auf Anforderung der Deutschen Börse AG aufgeschlüsselt auf Endnutzer-Basis nebst den entsprechenden Personalien zur Verfügung zu stellen. Zum Zwecke der Abrechnung war dies nicht erforderlich. Wie oben ausgeführt, bestand für den Nutzer selbst keine Gebührenpflicht und die vom Vendor an die Deutsche Börse AG zu zahlenden Gebühren richteten sich nach der Gesamtzahl der Kursabfragen. Daher ist insoweit eine anonymisierte/pseudonyme aggregierte Speicherung der Nutzungsdaten ausreichend.

Die Deutsche Börse AG verwies jedoch auf die erforderliche Missbrauchs-kontrolle:

Ab einer bestimmten Anzahl an Einzelkursabfragen am Tag sei es zum einen möglich, einen kommerziell interessanten Kursinformationsdienst für Dritte anzubieten. Zum anderen sei es kaum möglich, die betreffende Anzahl an Abfragen pro Tag noch manuell am PC einzugeben, sodass eine große Wahrscheinlichkeit bestehe, dass elektronische Abfrageroutinen geschaltet seien. Die konkrete Gefahr einer unerlaubten Einrichtung eines eigenen Informationsdienstes werde freilich erst angenommen, wenn regelmäßig und fortlaufende entsprechende Abfrage-Überschreitungen vorlägen.

Auch das Interesse einer Missbrauchskontrolle rechtfertigt jedoch nicht die Speicherung sämtlicher Abfragen für zehn Jahre. Die Deutsche Börse AG war daher letztlich bereit, den Vertrag mit dem Berliner Vendor (und auch die Verträge mit anderen Vendors) folgendermaßen abzuändern:

Die für einen Kalendertag gespeicherten Einzelkursabfragen von sämtlichen Endnutzern, die noch nie die kritische Grenze der Einzelkursabfragen pro Tag und Marktsegment überschritten haben, sind 24 Stunden nach Ende des betreffenden Kalendertages zu löschen. Die Einzelkursabfragen von Endnutzern, die bereits einmal oder mehrfach die kritische Grenze überschritten haben, sind für einen Zeitraum von drei Monaten seit der letzten Überschreitung, längstens jedoch für drei Jahre, zu speichern.

Das Kontrollinteresse der Deutschen Börse AG gegenüber dem Vendor kann grundsätzlich durch eine bloße Systemprüfung erfüllt werden.

Lediglich bei den Überschreitungsfällen forderte die Deutsche Börse AG weiterhin, dass ihr auf Anforderung personenbezogene Informationen zu geben seien.

Obwohl nach § 6 Abs. 3 TDDSG die Übermittlung personenbezogener Nutzungsdaten an Dritte an sich nur zulässig ist, soweit dies zum Zwecke der Einziehung einer Forderung erforderlich ist, konnte diese reduzierte Übermittlung zu Kontrollzwecken akzeptiert werden, da dies im Vertrag zwischen Nutzer und Vendor geregelt war. Bei einem Anfangsverdacht auf einen Missbrauch musste der Vertrag zudem in Schriftform (per Post) abgeschlossen werden (zur Bestätigung der Online-Vereinbarung).

## **8.2 Angebliche Sicherheitslücke beim Homebanking trotz HBCI**

Eine Pressemitteilung, in der behauptet wurde, der Bankensicherheitsstandard HBCI (Homebanking Computer Interface) sei nicht sicher, sorgte für Aufregung. Auf die Sicherheit von HBCI an sich wurde jedoch gar nicht eingegangen, sondern es wurde darauf hingewiesen, dass Viren HBCI gefährden könnten. Es handelt sich hierbei um die banale Weisheit, dass, wenn ein Rechner und das darauf befindliche Betriebssystem sich nicht in einer sicheren Systemumgebung befinden, alle möglichen Gefahren drohen können. Wenn beispielsweise ein Spionageprogramm (z.B. so genannte "Trojaner") Tastatureingaben speichert und unbemerkt an einen unbekanntem Dritten übermittelt, ist natürlich nichts mehr sicher.

Nicht umsonst hat sich eine ganze Industrie mit Virensuchprogrammen etabliert. Als Konsequenz hieraus sollte auch der private Anwender Virensuchprogramme ständig einsetzen und vor allem auch durch die Nutzung der Update-Funktion fortlaufend den aktuellen Erfordernissen anpassen.

Dies ist leider nicht überflüssig und, wenn Homebanking genutzt wird, in jedem Fall zu empfehlen. Darüber hinaus sollte sich die Chipkarte, die beim HBCI Standard zur Identifizierung genutzt wird, nur beim Anmeldevorgang und vor jeder einzelnen Transaktion im Lesegerät befinden. Es wäre sinnvoll, wenn die Banken auf diese Problematik detailliert hinweisen würden. Wenn zukünftig - wider Erwarten - doch noch Mängel des HBCI-Standards offengelegt werden sollten, bleibt dem Anwender immer noch der Rückgriff auf das bereits unter Btx bewährte Verfahren mit Verwendung von PIN und TAN (Transaktionsnummer).

## **8.3 Daten anderer Kunden beim Online-Banking übermittelt**

Bei einer Bank war durch eine Programmänderung die Indizierung der Datenbank durcheinander geraten. Dem Kunden wurden zwar die richtigen Beträge verbucht, die Verwendungszwecke stammten jedoch von völlig anderen Kunden.

Der gleiche Qualitätskontrolleur, dessen Wirken schon unter Nr. 6.1 beanstandet werden musste, schrieb dem Kunden, dass es sich um einen bedauerlichen Fehler handle, da aber keine personenbezogenen Daten betroffen seien, sei der Schaden begrenzt. Der Kunde war berechtigterweise empört, gingen doch aus den Verwendungszwecken die unterschiedlichsten personenbezogenen Daten - unter anderem detaillierte Daten über Kreditrückzahlungen, Versicherungszahlungen - hervor.

Jedenfalls sind bei Kredit- und Versicherungsverträgen über die Vertragsnummern die Personen bestimmbar, sodass von personenbezogenen Daten

ausgegangen werden muss. Noch klarer ist dieser Sachverhalt, wenn - wie im Beschwerdefall - neben der Lebensversicherungsnummer auch noch der Name des Versicherungsnehmers steht.

Nachträglich konnte nur noch gefordert werden, dass Programmendkontrolle und Mitarbeiterschulung verbessert werden. Insbesondere das Erfordernis der Mitarbeiterschulung - dazu bei der Qualitätskontrolle - wurde hierbei besonders deutlich. Die Mitarbeiter müssen mindestens wissen, was unter personenbezogenen Daten zu verstehen ist.

#### **8.4 SMS-Nachrichten mit unverlangter Werbung auf dem Handy**

Dass bei der Akquirierung neuer Kunden oftmals mit viel Kreativität und dem Einsatz modernster Technologien gearbeitet wird, konnte die Datenschutzaufsichtsbehörde im Berichtsjahr bei einem Unternehmen feststellen, gegen dessen aggressive Werbemethoden sich mehrere Petenten mit ihren Beschwerden wandten.

Alle Beschwerdeführer hatten zu Ihrer Überraschung auf dem Display Ihres Handys eine SMS-Werbebotschaft (Short Message Service) vorgefunden, in der sie aufgefordert wurden, bei Interesse an dem beworbenen Produkt unter einer im Text angegebenen 0180-Servicenummer (Call-Center zur Auftragsannahme) eine Bestellung aufzugeben. Als Absenderkennung am Ende der SMS war eine Telefonnummer mit Darmstädter Vorwahl angegeben. Alle Beschwerdeführer waren insbesondere deswegen beunruhigt, weil ihre jeweilige Handynummer nicht im Telefonbuch oder anderen Verzeichnissen veröffentlicht war. Zusätzlich hatten sie gegenüber dem Handy-Anbieter bei Vertragsabschluß der Weitergabe ihrer Handynummer zu Werbezwecken widersprochen. Die betroffenen Bürgerinnen und Bürger mussten nun befürchten, dass ihre Handynummer unbefugt und entgegen ihrem Willen weitergegeben wurde, um sie zu Werbezwecken zu nutzen. Die als Absenderkennung angegebene Telefonnummer war 24 Stunden dauerbesetzt, was die Betroffenen nur noch misstrauischer werden ließ.

Die Aufsichtsbehörde konnte Namen und Anschrift des Absenders der unverlangten Werbe-SMS anhand der angegebenen Telefonnummer ermitteln, aber nur dadurch, dass die Telefonnummer zufällig aus der Korrespondenz in ganz anderen Beschwerdefällen bekannt war. Bei der sodann durchgeführten unangemeldeten Prüfung in den Geschäftsräumen stellte sich allerdings heraus, dass dem Unternehmen keine Verzeichnisse von Handy-Kunden oder ähnliche personenbezogene Daten mit den Handynummern der Beschwerdeführer zur werblichen Nutzung vorlagen. Das Unternehmen setzte zur Versendung der Werbe-SMS ein entsprechendes frei erhältliches Programm ein, mit dem über einen ISDN-Anschluss aus dem PC vorbereitete SMS-Texte an ganze Gruppen von Pager- oder Handy-Nummern versandt werden können. Mittels einer speziell für die Bedürfnisse des Unternehmens programmierten Eingaberoutine wurden Schritt für Schritt alle logisch möglichen siebenstelligen Nummern eines Handy-Netzes automatisch generiert und dann zur Versendung der SMS-Webetextes genutzt, ohne dass für das Unternehmen zu diesem Zeitpunkt ein Bezug zur Person des Handy-Besitzers herstellbar gewesen wäre. Die am Ende der SMS angegebene Absenderkennung war die Anschlussnummer über die - auch während der Überprüfung vor Ort - eine ganze Reihe von PCs mit der Generierung und Versendung von SMS-Werbung befasst waren. Ein (wohl vom Versender unerwünschter) Rückruf unter dieser Nummer war den Beschwerdeführern daher schon aus technischen Gründen nicht möglich.

Der Versender kann bei dieser Werbevariante nicht feststellen, ob eine SMS-Botschaft angekommen ist oder nicht (z.B. weil das empfangende Handy längere Zeit abgeschaltet war oder weil die Nummer noch gar nicht vergeben wurde), da es bei diesem (Blind)Versand von SMS-Texten keine Empfangsbestätigungen oder andere Rückmeldung gibt. SMS-Nachrichten, die aus irgendwelchen Gründen nicht ankommen, werden von dem Betreiber des jeweiligen Handy-Netzes nach einiger Zeit verworfen. Dennoch gab das Unternehmen an, dass sich der Einsatz dieser neuen Werbestrategie lohnt, da der Aufwand für eine SMS gering sei und in den großen Handy-Netzen mit hoher Anschlussdichte mindestens jede vierte SMS auf ein existierendes Handy trifft und auch dort ankommt und gelesen wird.

Die Aufsichtsbehörde kam bei der datenschutzrechtlichen Bewertung des Verfahrens zu dem Ergebnis, dass keine unzulässige Datenverarbeitung oder -nutzung vorliege, da es bei der Versendung von SMS-Texten an automatisch generierte Handynummern an der erforderlichen Personenbeziehbarkeit der generierten Telefonnummern mangelt. Für den Versender der SMS-Werbung sind die erzeugten Handynummern ohne Zweifel anonyme Daten, zu denen ihm keinerlei weitere Informationen über die Besitzerin oder den Besitzer vorliegen, und zwar nicht einmal die Information, ob es eine solche Person überhaupt gibt.

Die Behörde wies jedoch daraufhin, dass die unverlangte Zusendung von SMS-Werbung, wenn schon nicht aus Datenschutzgründen, dann zumindest wettbewerbsrechtlich unzulässig sein dürfte, wenn man die Argumentation der Rechtsprechung zu unverlangter Telefon-, Telefax- und E-Mail-Werbung zugrunde legt.

Darüber hinaus wies die Aufsichtsbehörde darauf hin, dass das Unternehmen als Versender von Massen-SMS aber jedenfalls als Telediensteanbieter nach § 2 Abs. 2 Nr. 2 Teledienstegesetz (TDG) eingestuft werden kann, mit der Folge, dass es in seinen SMS-Nachrichten eine gültige Anbieterkennzeichnung im Sinne des § 6 TDG (Name und Anschrift, auch der vertretungsberechtigten Person) anzubringen hat. Bei einer auf 160 Zeichen begrenzten SMS ist daher zumindest ein Name, ein Ort und eine Telefonnummer anzugeben, mit der die Empfänger auch etwas anfangen können. Die Angabe einer Absender-Telefonnummer, die immer besetzt und damit letztlich unerreichbar ist, kann vor diesem rechtlichen Hintergrund nicht hingenommen werden.

Wäre der Aufsichtsbehörde nicht der Zufall zu Hilfe gekommen, hätte sie ihre Prüfpflichten kaum erfüllen können. Dies belegt die Bedeutung der Anbieterkennzeichnungspflicht.

### **8.5 Personenverwechslung im Call-Center eines Internet-Providers**

Ein Internet-Nutzer hatte festgestellt, dass er sich mit der neuen Zugangskennung, die er von seinem Internet-Service-Provider nach einem Wohnungswechsel erhalten hatte, nicht mehr ins Internet einwählen konnte. Nach einer telefonischen Beschwerde beim Call-Center des Internet-Service-Providers (Service-Hotline) erhielt er neue Zugangsdaten, mit denen er sich zu seiner Überraschung aber nur wenige Tage in das Internet einwählen konnte. Danach war sein Zugang erneut gesperrt. Nach aufwendigen eigenen Nachforschungen des Users stellte sich heraus, dass noch ein weiterer Kunde existierte, der den gleichen Vor- und Nachnamen trägt und der, wie sich bei einem ersten Kontakt herausstellte, seit dem ersten Umzug seines Namensvetters ebenfalls erhebliche Unregelmäßigkeiten bei seinem Internetzugang verzeichnen musste. Beide Kunden vermuteten nun, dass es ihre Namensgleichheit war, die zu den aufgetretenen Problemen führte und wandten sich nun beide gleichzeitig an die vom Call-Center betreute Service-Hotline ihres Providers mit der Bitte, in der Angelegenheit nachzuforschen, die Kundendatenbank zu berichtigen und ihre beiden betroffenen Internet-Zugänge wieder funktionsfähig zu konfigurieren.

Trotz mehrerer Telefonate, Telefaxe und Briefe mit genauen Schilderungen und Sachverhaltsdarstellungen war die Service-Hotline des Providers mehrere Monate lang nicht in der Lage, den Fehler zu finden und zu beheben. Daraufhin kündigte einer der Kunden seinen Vertrag, verlangte vom Provider die Rückzahlung der bereits entrichteten Gebühren für seinen funktionsunfähigen Internetzugang und bat gleichzeitig die Datenschutzaufsichtsbehörde, sich der Sache anzunehmen, da er befürchten musste, dass seine personenbezogenen Daten in der Kundendatenbank des Providers weiterhin falsch gespeichert und verarbeitet werden.

Die Aufsichtsbehörde wandte sich zunächst an den betrieblichen Datenschutzbeauftragten des Providers und forderte diesen auf, nun endlich Licht ins Dunkel seiner Kundendatenbank zu bringen. Erst durch dessen intensive Nachforschungen bei der Kundenverwaltung und einem der Call-Center, die die Service-Hotline betreiben, konnte der bereits bei der ersten Adressänderung entstandene Fehler identifiziert und die weitere unglückliche und durch menschliche Fehlleistungen gekennzeichnete Verkettung von Umständen nachvollzogen werden.

Die Verwechslung beruhte darauf, dass aufgrund eines Bearbeitungsfehlers die vom Petenten mitgeteilte Adressänderung bei dem verkehrten Datensatz, nämlich dem seines Namensvetters ausgeführt wurde. Alle weiteren Versuche der beiden betroffenen Kunden über die Service-Hotline eine Berichtigung der Daten zu erreichen, schlugen letztlich fehl, da die Mitarbeiter des Call-Centers alle Datenänderungen immer wieder am jeweils falschen Datensatz vornahmen und alle Änderungsmitteilungen mit den unter diesen Voraussetzungen größtenteils falschen Zugangsdaten immer wieder an den jeweils falschen Kunden abgesandt wurden. Sogar die nach der Vertragskündigung durch den Petenten erfolgte Rückzahlung der zuviel erhobenen Gebühren erfolgte auf das (falsche) Konto des Namensvetters! Sämtliche Korrekturversuche der Beschwerdeführer führten so zu einer weiteren Verschlechterung und Verfälschung der ohnehin schon undurchsichtigen Datenlage, die nur mit Unterstützung durch die Datenschutzaufsichtsbehörde und durch den betrieblichen Datenschutzbeauftragten des Providers geklärt und berichtigt werden konnte.

Wo Menschen arbeiten, können menschliche Fehler natürlich nie vollkommen ausgeschlossen werden. Die im vorliegenden Fall in erheblichem Maße aufgetretenen Mitarbeiterfehler führten dennoch zu einer Beanstandung durch die Aufsichtsbehörde. Immerhin hatte der Provider trotz der massiven Kundenbeschwerden mehrere Monate verstreichen lassen, ohne den in seiner Kundendatenbank offensichtlich vorliegenden Fehler zu finden. Das Unternehmen wurde aufgefordert, die Mitarbeiterinnen und Mitarbeiter der Kundenverwaltung und vor allem der externen Call-Center intensiver zu schulen und nachhaltig zur Sorgfalt - insbesondere bei Fällen mit übereinstimmenden Namen - anzuhalten. Gerade in Anbetracht der hohen Personalfuktuation bei den externen Call-Centern ist es nach Auffassung der Aufsichtsbehörde unerlässlich, diese Mitarbeiterinnen und Mitarbeiter mit regelmäßigen Schulungen für ihre Tätigkeit angemessen zu qualifizieren. Bei Eingaben und Beschwerden von Kunden mit datenschutzrechtlicher Relevanz ist die Beteiligung des betrieblichen Datenschutzbeauftragten sinnvoll und - wie der vorliegende Fall eindrucksvoll gezeigt hat - unumgänglich.

## 9. Auslandsdatenverarbeitung

In den vorangegangenen Tätigkeitsberichten wurde bereits mehrfach über die Zulässigkeit von Datenübermittlungen in Staaten außerhalb der Europäischen Union berichtet (s. jeweils Nr. 10 des 12. und 13. Tätigkeitsberichtes).

Wenn in dem Empfängerland kein angemessenes Datenschutzniveau besteht, ist die Übermittlung grundsätzlich nur zulässig, wenn der Betroffene eingewilligt hat oder wenn die Übermittlung zur Erfüllung eines Vertrages mit dem Betroffenen oder eines im Interesse des Betroffenen geschlossenen Vertrages erforderlich ist. § 4 c Abs. 1 BDSG n.F. enthält eine genaue Auflistung der gesetzlichen Ausnahmetatbestände von dem grundsätzlichen Verbot der Datenübermittlung in so genannten Drittstaaten, d.h. Staaten außerhalb der EU, in denen kein angemessenes Datenschutzniveau besteht.

Wenn diese Voraussetzungen nicht gegeben sind, kann die Übermittlung gleichwohl zulässig sein, wenn das übermittelnde Unternehmen durch eine vertragliche Regelung mit dem Empfänger ausreichende Garantien für den Schutz des Persönlichkeitsrechts der Betroffenen schafft. Wenn übermittelndes Unternehmen und Empfänger demselben Konzern angehören, können sich solche Garantien auch aus verbindlichen Unternehmensregeln ergeben. Für die USA wird davon ausgegangen, dass ein angemessenes Datenschutzniveau besteht, sofern sich der dort ansässige Datenempfänger den so genannten "Safe Harbor Principles" unterwirft.

Im Berichtsjahr erhielten die Aufsichtsbehörden mehrere Anfragen von Unternehmen und Organisationen, welche die Vertragslösung oder die Unterwerfung unter die Safe Harbor Principles zunächst scheuten - aus welchen Gründen auch immer (Aufwand etc.).

Da die Übermittlung in den Drittstaat ohne angemessenes Datenschutzniveau nicht zur Erfüllung eines Vertrages mit den Betroffenen erforderlich war, sollten Einwilligungen der Betroffenen eingeholt werden.

Die erforderliche "informierte" Einwilligung setzt voraus, dass der Zweck der Datenverarbeitung angegeben wird (§ 4 Abs. 2 Satz 1 BDSG). Dies impliziert auch die Angabe des Empfängers und Zielortes der Übermittlung. Ferner muss auf die dort geltenden Verarbeitungsvoraussetzungen und die damit möglicherweise verbundenen Risiken hingewiesen werden (Simitis, BDSG, § 4 Rn. 62). Konkret sollte daher die Angabe erfolgen, dass in dem Empfängerland kein der EG vergleichbares Datenschutzniveau gewährleistet ist - eventuell relativiert durch Angaben zur konkreten Verarbeitungssituation beim Empfänger.

Besonders wichtig ist die Freiwilligkeit der Einwilligung. § 4 a Abs. 1 Satz 1 BDSG n.F. hebt hervor, dass sie auf "der freien Entscheidung des Betroffenen" beruhen muss.

Bei einer beabsichtigten Übermittlung von Daten der Teilnehmer von Yoga-Kongressen konnte von der Freiwilligkeit ausgegangen werden (bei entsprechendem Hinweis), denn sie sollte nur innerhalb des weltweiten Yoga-Verbandes erfolgen und der Informationsversendung und Organisation weiterer Kongresse dienen.

Problematischer ist die Beurteilung bei Arbeitsverhältnissen. Aufgrund der typischen Abhängigkeitssituation kann eine Einwilligung grundsätzlich keine Grundlage für die Übermittlung von Personaldaten in Drittstaaten ohne angemessenes Datenschutzniveau sein. (Unproblematisch ist die Datenübermittlung im Zusammenhang von Auslandseinsätzen, da diese zur Vertragserfüllung erforderlich ist und somit - im erforderlichen Umfang - ohne weitere Voraussetzungen zulässig ist.)

Ein Grenzfall war folgender:

Die deutsche Tochtergesellschaft eines US-amerikanischen Unternehmens wollte Daten ihrer Mitarbeiter an die Muttergesellschaft übermitteln, damit diesen Konzernaktien (stock options) zugeteilt werden konnten. Die Zuteilung und Verwaltung der Aktien sollte also in den USA erfolgen, und zwar im wesentlichen über ein von der Muttergesellschaft eingeschaltetes Dienstleistungsunternehmen.

Da die Aktienzuteilung einen zusätzlichen finanziellen Vorteil für die Betroffenen bedeutete, sprach dies dafür, die beabsichtigte Einholung entsprechender Einwilligungen als wirksam zu bewerten. Unerlässlich war jedoch zumindest eine Reduzierung des Datenumfangs, denn es war nicht ersichtlich, inwieweit gewisse Personaldaten für die Aktienverwaltung relevant waren.

Darüber hinaus kann aber auch bei solchen Übermittlungen die Freiwilligkeit der Einwilligung fraglich sein: Je höher die finanzielle Vergünstigung ist (und quasi einen wesentlichen Gehaltsbestandteil darstellt), desto eher kann auch insoweit von einer gewissen Abhängigkeit die Rede sein.

Erfreulicherweise war das Unternehmen letztlich bereit, zusätzlich einen Vertrag mit der Muttergesellschaft zugunsten der Mitarbeiter abzuschließen. Durch diesen wurde ein angemessenes Datenschutzniveau gewährleistet und insbesondere die Zweckbindung festgelegt. In der Vereinbarung wurde festgehalten, dass das deutsche Unternehmen im Verhältnis zu seinen Mitarbeitern voll verantwortlich bleibt (hinsichtlich der Rechte auf Auskunft, Löschung, Berichtigung, Schadensersatz etc.), d.h. auch bzgl. der im Ausland erfolgenden Datenverarbeitung.

## **10. Arbeitnehmerdatenschutz**

### **10.1 Werbemaßnahmen von Zeitarbeitsunternehmen**

Ein Wirtschaftsunternehmen übermittelte der Aufsichtsbehörde eine Faxwerbung, die ihm selbst unverlangt zugesandt worden war.

Darin bot ein Zeitarbeitsunternehmen seinen Service zur Vermittlung von Mitarbeitern an, indem die Dienste von namentlich genannten Mitarbeitern und deren Stundensätze offeriert wurden. Darüber hinaus wurden Mitarbeiterprofile aller angebotenen Zeitarbeitnehmer mit übersandt, die wiederum die Namen der Betroffenen, deren Geburtsdaten, Schulabschlüsse, Berufserfahrungen sowie spezielle Kenntnisse beinhalteten und mit einer Bemerkung zur Person des Zeitarbeitnehmers endeten.

Das Zeitarbeitsunternehmen berief sich gegenüber der Aufsichtsbehörde darauf, dass Profile erstellt werden müssten, um den Interessenten die Leistungsfähigkeit der Angebote zu verdeutlichen. Darüber hinaus hätten die Betroffenen in ihren Personalbögen in die Verarbeitung ihrer personenbezogenen Daten, insbesondere in die Übermittlung ihrer Daten an Unternehmen, die mit dem Zeitarbeitsunternehmen verbunden seien, eingewilligt.

Dem Zeitarbeitsunternehmen wurde mitgeteilt, dass die unverlangte Werbung durch Übermittlung von Mitarbeiterprofilen unter expliziter Nennung von Namen und Geburtsdaten als unzulässig anzusehen ist. Zum einen war sie nicht durch die im Personalbogen enthaltene Einwilligungserklärung der Mitarbeiter gedeckt. Diese war zu pauschal abgefasst. Es wurde den Mitarbeitern nämlich nicht mitgeteilt, welche Daten zu welchen Zwecken an welche Unternehmen übermittelt würden. Zum anderen war zu berücksichtigen, dass der Umfang der Datenübermittlung nicht das für den konkreten Zweck erforderliche Maß überschreiten darf.

So dürften selbst konkreten Vertragspartnern nicht alle Daten, die im Personalfragebogen aufgeführt sind, übermittelt werden.

Umso mehr gilt dies für die Fälle der unverlangt übermittelten Werbung, die Mitarbeiterprofile enthält.

Daher forderte die Aufsichtsbehörde das Zeitarbeitsunternehmen auf, künftig nur noch anonymisierte Mitarbeiterprofile (ohne Namen und Geburtsdatum) für Werbemaßnahmen zu verwenden. Darüber hinaus wurde darauf hingewiesen, dass die Einwilligungserklärung im Personalfragebogen im Hinblick auf die konkreten Übermittlungsvoraussetzungen bei der personenbezogenen Übermittlung an konkrete Vertragspartner überarbeitet werden muss.

## 10.2 Datenübermittlung an Gewerkschaften

Die Nutzung und Übermittlung von Arbeitnehmerdaten, die beim Arbeitgeber im Rahmen eines Arbeitsvertrages gespeichert sind, ist nach § 28 Abs. 1 Nr. 1 BDSG nur im Rahmen der Zweckbestimmung dieses Vertragsverhältnisses zulässig. Nutzungen und Übermittlungen zu anderen Zwecken bedürfen in aller Regel der Legitimation durch die informierte Einwilligung (§ 4 Abs. 2 BDSG) des betroffenen Personals. Diese restriktiven Bedingungen sind zur Vermeidung der Beeinträchtigung schutzwürdiger Belange von Arbeitnehmerinnen und Arbeitnehmern sowohl von Arbeitgebern und ihren Verbänden als auch von Betriebsräten und Gewerkschaften zu beachten, worauf die hessischen Datenschutzaufsichtsbehörden in einzelnen Fällen jedes Jahr erneut hinweisen müssen.

Als unzulässig sah die Aufsichtsbehörde daher auch die Übermittlung der Privatanschriften von Mitarbeitern an eine Gewerkschaft: Diese wurde vorgenommen durch den örtlichen Betriebsrat einer südhessischen Niederlassung eines großen deutschen Unternehmens. Die Mitarbeiteranschriften wurden von der Gewerkschaft zur postalischen Mitgliederwerbung genutzt, wogegen sich einer der umworbenen Betroffenen, der bereits einer konkurrierenden Berufsorganisation angehörte, bei der Aufsichtsbehörde beschwerte.

Dem Betriebsrat wurde deutlich gemacht, dass sich aus seinem umfassenden mitbestimmungsrechtlichen Unterrichtsanspruch im Betrieb zwangsläufig auch das Gebot der Schweigepflicht ergibt. Wenn Personaldaten, die dem Betriebsrat aus seiner Funktion als Mitarbeitervertretung zur Verfügung stehen, an Dritte übermittelt werden, steht das im krassen Gegensatz zu seiner Verpflichtung gemäß Betriebsverfassungsgesetz, über persönliche Verhältnisse der Beschäftigten, die ihm im Rahmen der Amtstätigkeit bekannt geworden sind, zu schweigen. Dies gilt auch gegenüber den Gewerkschaften, die datenschutzrechtlich als "Dritte" im Sinne des Gesetzes zu betrachten sind. Die Mitarbeitervertreter unterliegen zusätzlich der Schweigepflicht nach § 5 Abs. 1 BDSG, nach der jede unbefugte Verarbeitung und Nutzung der Daten untersagt und gegebenenfalls mit Strafe (§ 43 BDSG) bedroht ist.

Die §§ 28 Abs. 1 Nr. 2 und 28 Abs. 2 Nr. 1 b BDSG scheiden als Erlaubnistatbestand aus.

Daher wurde die Datenübermittlung an die Gewerkschaft bei dem betroffenen Betriebsrat gerügt, die anschließende unzulässige werbliche Nutzung der Daten wurde gegenüber der Gewerkschaft beanstandet. Arbeitnehmer können

auch auf andere Weise von Betriebsräten und Gewerkschaftern angesprochen werden. Hier bieten sich als datenschutzfreundliche Werbevarianten vor allem die persönliche Ansprache im Betrieb sowie das Verteilen von Flugblättern und Mitarbeiterzeitungen an, mit denen ohne irgendeine Datenerhebung oder -nutzung der gleiche Zweck erreicht werden kann.

Der von dem örtlichen Betriebsrat und der gewerkschaftlichen Betriebsverwaltung zu Rate gezogene Datenschutzbeauftragte des gewerkschaftlichen Hauptvorstandes bestätigte die Rechtsauffassung der Datenschutzaufsichtsbehörde. Neben wortreichen Entschuldigungen haben der Betriebsrat und die Gewerkschaft mitgeteilt, dass die unzulässig erhaltenen Adressdaten bei der Gewerkschaft nach der Einschaltung der Aufsichtsbehörde umgehend gelöscht und zwischenzeitlich auch nicht an weitere Stellen weitergegeben wurden. Weiterhin wurden alle Beteiligten auf die rechtliche Problematik solcher Werbeaktionen hingewiesen. Mitarbeiterschulungen und andere organisatorische Maßnahmen sollen künftig die Einhaltung datenschutzrechtlicher Bestimmungen sicherstellen.

### **10.3 Veröffentlichung der Arbeitszeitabrechnung**

Der Mitarbeiter eines Unternehmens fragte bei der Aufsichtsbehörde an, inwieweit es zulässig sei, dass die Daten der Arbeitszeitabrechnung offen ausgedruckt und dann den Mitarbeitern am Arbeitsplatz verteilt würden. Wenn ein Arbeitsplatz nicht besetzt ist, würden die Ausdrucke auf dem jeweiligen Schreibtisch abgelegt, sodass sie allen anderen Mitarbeitern zugänglich seien. Bisher sei die Zeitabrechnung auf verdeckten Unterlagen ausgedruckt worden.

Es stellte sich heraus, dass das Unternehmen ein neues Verfahren im Druckbereich installiert hatte. Der bis dahin genutzte Drucker ist durch einen neuen Drucker abgelöst worden. Dieser ist technisch nicht mehr in der Lage, ein zugeschlossenes und an den Seiten perforiertes Papier zu bedrucken. Aus diesem Grunde habe man ganz einfach normales Papier bedrucken lassen und die Unterlagen entsprechend verteilt. Das Unternehmen sagte sofortige Änderung des Verfahrens zu und wollte zukünftig die Zeitabrechnung in verschlossenen Umschlägen verteilen.

## **11. Medizinischer Bereich**

### **11.1 Verwertung der Rezeptdaten von Kassenpatienten**

Apotheken bedienen sich i.d.R. spezieller Rechenzentren, um die Rezepte der Kassenpatienten bei den gesetzlichen Krankenkassen einzureichen und somit abzurechnen. Neben einigen rein privaten Rechenzentren führen die Abrechnungen vor allem die fünf standeseigenen Apotheken-Rechenzentren (ARZ) in Darmstadt, München, Berlin, Haan (Nordrhein-Westfalen) und Bremen (Norddeutsches Apothekenrechenzentrum) durch.

Die Bundesvereinigung Deutscher Apothekerverbände (= Arbeitsgemeinschaft der Berufsverbände deutscher Apotheker - ABDA) mit Sitz in Eschborn wollte nun Daten aus den ARZ für die berufs- und verbandspolitische Interessenvertretung der Apotheker nutzen und bat die Aufsichtsbehörde um datenschutzrechtliche Bewertung. Die Daten sollen statistisch ausgewertet werden.

Nach § 300 SGB V dürfen die ARZ die Rezeptdaten (nur) für im Sozialgesetzbuch bestimmte Zwecke verarbeiten und nutzen, soweit sie dazu von einer berechtigten Stelle beauftragt worden sind (insbesondere von einer Apotheke für die Abrechnung mit den gesetzlichen Krankenkassen). Anonymisierte Daten dürfen sie nach § 300 SGB V auch für andere Zwecke verarbeiten und nutzen. Daher stellte sich die Frage, ob die für die statistischen Auswertungen benötigten Datenübermittlungen nach § 300 SGB V zulässig sind.

Die ABDA legte dar, dass die Auswertungen eine starke Konnexität zu den SGB-Zwecken aufweisen, sie stützte sich aber letztlich auf die zweite Alternative von § 300 SGB V, denn es würden nur anonyme Daten übermittelt werden.

Für die Auswertungen in Phase I war dies offensichtlich. Hier sollen ökonomische Auswertungen zum Verordnungsgeschehen durchgeführt werden. Die benötigten Datensätze lassen keinerlei Rückschlüsse auf Patienten oder verschreibende Ärzte zu.

In Phase II sollen zu spezifisch pharmazeutisch-pharmakologischen Fragestellungen Zeitreihenanalysen durchgeführt werden, bei denen die Datensätze "Versichertenanonymen" zugeordnet werden sollten. Beispielsweise sollen Intervallimpfungen untersucht werden: In vielen Fällen wird der beabsichtigte Impfschutz nur erreicht, wenn über einen bestimmten Zeitraum mehrere Impfungen durchgeführt werden. Werden Impfindervalle ausgelassen, wird der Impfschutz nicht planmäßig erreicht, was eine Vergeudung von Ressourcen bedeutet. Um Studien über regionale Unterschiede bezüglich der Einhaltung der Impfindervalle durchführen zu können, ist es notwendig zu wissen, ob einem Patienten, dem ein bestimmtes Impfpräparat verschrieben wurde, auch das entsprechende Präparat für die folgenden Impftermine verschrieben wurde.

Hierfür sollen die ARZ auf der Basis der Versichertennummer eine Einwegverschlüsselung der Verschreibungsdaten vornehmen. In einer GmbH, die sich im Eigentum der ABDA befindet, sollen die Daten aller ARZ zusammengeführt und erneut verschlüsselt werden. Sodann sollen die verschlüsselten Daten in einem neu zu gründenden Rechenzentrum statistisch ausgewertet werden. Für eine Übergangszeit solle das NARZ die Auswertungen vornehmen.

Angesichts des gewählten sehr starken Einweg-Verschlüsselungs-Verfahrens sah die Aufsichtsbehörde nach Abstimmung mit den für die anderen ARZ zuständigen Aufsichtsbehörden keine Bedenken, jedenfalls wenn die Auswertungen in dem neu zu gründenden Rechenzentrum durchgeführt werden. Bei Speicherungen und Auswertungen im NARZ wurde folgendes Problem gesehen:

Das NARZ könnte eventuell Rezepte mit besonderen Verschreibungsweisen aus dem eigenen Datenbestand in der Gesamtmenge der Daten - trotz der zweifachen Verschlüsselung - wiedererkennen und missbräuchlich (Versichertennummer und Krankenkassenkennzeichen im Klartext) dem verschlüsselten Versichertennummerwert zuordnen. Dies wäre möglich, weil Verschreibungsweisen und Diagnosen grundsätzlich unverschlüsselt bleiben. Diese Missbrauchsgefahr betrifft freilich nur Rezepte von Ärzten, deren Rezepte teils beim NARZ, teils bei anderen ARZ eingereicht werden.

Daher waren beim NARZ zusätzliche technisch-organisatorische Maßnahmen erforderlich, um die Missbrauchsgefahr einzudämmen. Der insoweit zuständige Landesbeauftragte für den Datenschutz in Bremen ordnete diese an.

## **11.2 Unzulässige Übermittlung von Patientendaten an ein externes Labor**

Ein Arzt darf Patientendaten gegenüber Dritten grundsätzlich nur offenbaren, wenn ein Gesetz dies erlaubt oder wenn der Patient den Arzt von der Schweigepflicht entbindet. So hat der Bundesgerichtshof bereits 1991 entschieden, dass eine zu Abrechnungszwecken vorgenommene Übermittlung von Patientendaten an eine private ärztliche Verrechnungsstelle nur dann zulässig ist, wenn der darüber informierte Patient ausdrücklich seine Einwilligung dazu erklärt hat. In der Praxis geschieht dies in der Regel mit formularmäßigen Schweigepflichtentbindungserklärungen.

Dass diese Verfahrensweise leider immer noch nicht überall praktiziert wird, zeigte sich anhand der Eingabe der Patientin eines Hautarztes, die sich beim Regierungspräsidium Darmstadt darüber beschwerte, dass sie von einer privatärztlichen Verrechnungsstelle eine Abrechnung erhalten habe, obwohl sie die auf der Rechnung angegebene Laborarztpraxis gar nicht kenne und dort nie zur Behandlung gewesen sei und die darum bat, herauszufinden, wie die Laborarztpraxis und infolge dann auch die beteiligte Verrechnungsstelle an ihre Daten gelangt waren.

Bei den Nachforschungen der Datenschutzaufsichtsbehörde stellte sich dann schnell heraus, dass der die Beschwerdeführerin behandelnde Hautarzt im Rahmen seiner Untersuchung den Laborarzt für eine Analyse in Anspruch genommen hatte, wovon die Patientin allerdings nichts wusste. Dieser Laborarzt rechnete seine Leistungen über eine private ärztliche Verrechnungsstelle ab, die der Patientin dann die Rechnung zukommen ließ. Da der Haut-

arzt seine eigenen Leistungen auch selbst abrechnet, benötigt er für Abrechnungszwecke keine Schweigepflichtentbindungserklärung. Dass allerdings auch die Beauftragung eines externen ärztlichen Labors der Zustimmung durch die betroffenen Patientinnen und Patienten bedarf, wenn die Proben dabei zusammen mit den Namen übermittelt werden, war ihm nicht bekannt.

Auch die Datenübermittlung durch den Laborarzt an eine private Abrechnungsstelle war unzulässig, da keine Schweigepflichtentbindungserklärung der Patientin vorlag.

Die von der Aufsichtsbehörde zunächst vorgeschlagene Lösungsmöglichkeit, mit anonymisierten Proben (Patientennummer u.Ä.) zu arbeiten, wurde von den beteiligten Ärzten als unzumutbar aufwändig abgelehnt. Insbesondere der Laborarzt war nicht bereit, seine Rechnungen an behandelnde Ärzte zu richten, was aber die zwingende Folge von anonymisierten Probeanalysen wäre. Er bestand darauf, seine Laborleistungen weiterhin direkt mit dem Patienten abzurechnen. Als Kompromisslösung konnte bei den beteiligten Ärzten durchgesetzt werden, dass der behandelnde Arzt in Zukunft in jedem Fall der Beteiligung eines externen Labors eine Einwilligungserklärung der Patienten einholt, die ihn ermächtigt, die für die Untersuchung benötigten Daten an das Arztlabor zu übermitteln. Aufgrund des mangelnden direkten Kontaktes zwischen Patient und Laborarzt muss diese Schweigepflichtentbindungserklärung des Hautarztes zusätzlich auch noch eine Einwilligung in die Übermittlung der rechnungsrelevanten Laborarzt-daten an eine ärztliche Verrechnungsstelle enthalten.

### **11.3 Datenübermittlung durch Sanitätshaus**

Die Zweigstelle eines Sanitätshauses wollte einer einzelnen Kundin eine Nachforderung belegen, indem sie ihr die Kopie einer Aufstellung übersandte, die alle mit der Krankenkasse abgerechneten Leistungen und deren Korrektur durch diese Krankenkasse enthielt. Es handelte sich dabei aber nicht nur um die Abrechnungen der Krankenkasse für die betroffene einzelne Kundin, sondern um die Aufstellung der Abrechnungen aller Kunden des Sanitätshauses in einem bestimmten Rechnungszeitraum.

Für die umfassende Übermittlung der Liste fehlte im Rahmen des § 28 BDSG die Erforderlichkeit. Das Sanitätshaus wurde aufgefordert, alle Zweigstellen darüber zu informieren, dass solche Übermittlungen zukünftig unterbleiben müssen.

## **12. Versicherungen: Datenübermittlungen im Zusammenhang mit Holocaust-Entschädigungen**

Eine im Aufsichtsbezirk Darmstadt ansässige Versicherung fragte an, ob die sich für ihre Geschäftstätigkeit in Kalifornien ergebenden Verpflichtungen aus dem dort erlassenen Holocaust Victim Insurance Relief Act von 1999 mit den Anforderungen des Datenschutzes vereinbar wären.

Dieses kalifornische Gesetz bestimmt, dass Versicherungen, die in Kalifornien tätig sind, innerhalb einer bestimmten Frist detaillierte Angaben zu allen in Europa abgeschlossenen Versicherungspolice in den Sparten Lebens-, Sach-, Haftpflicht-, Kranken-, Leibrenten-, Aussteuer-, Ausbildungs- und Unfall-Versicherungen aus den Jahren 1920 bis 1945 einem Beauftragten des Staates Kalifornien vorlegen sollten. Diese Angaben umfassten die Versicherungsnummern, den Versicherungsnehmer, den Begünstigten, den aktuellen Stand der Versicherungspolice sowie den Geburtsort, den Wohnort oder die Adresse jedes Versicherungsnehmers. Diese Informationen sollten in ein öffentlich zugängliches Register aufgenommen werden. Damit sollte den in Kalifornien lebenden Holocaust-Opfern und deren Angehörigen die Möglichkeit gegeben werden, sich über das Vorhandensein eventuell Forderungen aus den Versicherungsverträgen zu informieren.

Sollte eine in Kalifornien tätige Versicherung nicht bis zum Fristablauf der gesetzlich festgelegten Verpflichtung nachkommen, drohte der Entzug der Lizenz zum Betreiben von Versicherungsgeschäften im kalifornischen Bundesstaat.

Die Aufsichtsbehörde hielt diese Verpflichtung für sehr problematisch. Die Übermittlung der Daten von Personen, die nicht zum Kreis der zu entschädigenden Holocaust-Opfer zählen, war als nicht zulässig anzusehen,

denn sie hätte nicht mehr im Rahmen der Zweckbestimmung des Versicherungsvertrages gelegen. Auch eine Übermittlung aufgrund anderer Tatbestände des § 28 BDSG kam nicht in Betracht, da Grund zu der Annahme bestand, dass die nicht zum Kreis der Opfer bzw. Entschädigungsberechtigten gehörenden Personen ein überwiegendes schutzwürdiges Interesse an der Nichtübermittlung ihrer Daten haben würden.

Allerdings erschien auch die Übermittlung der Daten von Opfern des Holocaust als problematisch, weil der Zweck - die Aufnahme in ein für jedermann zugängliches Register - nicht nach § 28 Abs. 1 Nr. 1 BDSG vom Versicherungsverhältnis gedeckt wäre.

Im Rahmen des § 28 Abs. 1 Nr. 2 bzw. Abs. 2 Nr. 1 BDSG konnte auch nicht davon ausgegangen werden, dass zumindest alle Opfer i.S.d. Insurance Act mit der Übermittlung ihrer Daten an ein öffentliches Register einverstanden wären. Denn es war zu berücksichtigen, dass auch insoweit schutzwürdige Interessen am Ausschluss einer solchen Übermittlung vorliegen könnten (z.B. wenn ein Betroffener nicht öffentlich als Holocaust-Opfer bekannt werden will).

Hinzu kam der Aspekt der Datenübermittlung ins Ausland, bei der die Gewährleistung des angemessenen Schutzniveaus nicht geklärt war.

Zu berücksichtigen war auch, dass die Versichertendaten nach § 203 Abs. 1 Nr. 6, Abs. 4 StGB strafrechtlich vor unbefugter Offenbarung geschützt sind, was sowohl die lebenden als auch die bereits verstorbenen Versicherungsnehmer betroffen hätte.

Aus vorgenannten Gründen hätte man wohl nur dann von einer mutmaßlichen Einwilligung der Opfer in die Offenbarung ihrer Daten ausgehen können, wenn eine treuhänderisch tätige Stelle einen Abgleich der Versicherungsdaten mit den Daten der möglicherweise Betroffenen oder Begünstigten vorgenommen hätte.

Es wurde daher seitens der Aufsichtsbehörde angeregt, einen solchen Abgleich zu initiieren.

Die Vertreter der obersten Aufsichtsbehörden haben sich inzwischen gleichlautend zu der Problematik geäußert und werden gegenüber dem Bundesaufsichtsamt für das Versicherungswesen eine entsprechende Stellungnahme abgeben, damit diese in die Verhandlungen mit den amerikanischen Behörden einfließen und so eine datenschutzverträgliche Lösung gefunden werden kann.

## **13. Werbewirtschaft**

### **13.1 Auskunftserteilung beim Listbroking**

Wenn Unternehmen für ihre Werbeschreiben die Adressdatenbestände fremder Unternehmen im sogenannten Listbroking-Verfahren einsetzen, ist es für die beworbenen Bürger z.T. äußerst schwer, sich Kenntnis über die Quelle ihrer für Werbung genutzten Daten zu verschaffen. Diese ist jedoch erforderlich, um beim Adresssigner Widerspruch gegen die künftige Verwendung ihrer Daten für Werbezwecke einzulegen. Hierüber wurde bereits im 12. Tätigkeitsbericht unter Nr. 13.2 berichtet.

Die dort dargestellte Rechtsauffassung der Aufsichtsbehörde, wonach der Adresssigner vertraglich zu regeln hat, dass Betroffene ihr Auskunftsrecht durchsetzen können und dass das werbende Unternehmen sicherzustellen hat, dass Betroffene tatsächlich Auskunft erhalten, wurde 1999 auf dem Workshop der Aufsichtsbehörden in Dresden erörtert und von allen Anwesenden geteilt.

Trotz entsprechenden Hinweises war jedoch auch im Berichtsjahr ein werbendes Unternehmen nicht bereit, betroffenen Bürgern die erbetene Auskunft zu erteilen; noch nicht einmal der Listbroker/Werbedienstleister wurde mitgeteilt. Das Unternehmen berief sich darauf, dass es die Daten nicht speichere (und auch der Dienstleister die Daten nicht in seinem Auftrag i.S.d. § 11 BDSG verarbeite) und somit nach § 34 BDSG keine Auskunftspflicht bestünde. Der Gesetzgeber möge eine klare Regelung treffen. Letztlich war das Unternehmen aber bereit, gegenüber der Aufsichtsbehörde Auskunft zu geben - betonte jedoch zugleich, dass hieraus keine Zusage für künftige Fälle abgeleitet werden könne.

Eine derartige Haltung ist nicht gerade geeignet, das Vertrauen der Bürger in den Umgang mit ihren Daten zu fördern. Der Fall zeigte die Notwendigkeit unmissverständlicher gesetzgeberischer Vorgaben, um die Transparenz der Datenverarbeitung zu gewährleisten.

Ein Vorentwurf zur BDSG-Novelle hatte noch vorgesehen, dass der Bürger bei der Ansprache zum Zwecke der Werbung "über die Herkunft" seiner Adressdaten zu unterrichten ist.

Aufgrund der Einwände des Deutschen Direktmarketingverbandes (DDV) war diese Verpflichtung gestrichen bzw. in der Weise abgeändert worden, dass nur über die "verantwortliche Stelle" zu unterrichten sei.

Der Begriff der "verantwortlichen Stelle" ist in § 3 Abs. 7 BDSG n.F. definiert. Danach ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Im Sinne dieser Definition ist zunächst der Adresssigner verantwortliche Stelle, soweit er seine Kundendaten durch einen Dienstleister für fremde Werbezwecke verarbeiten lässt, und zwar in seinem Auftrag i.S.d. § 11 BDSG (und dass ein solches Auftragsverhältnis vorliegt, wurde von der Werbewirtschaft meines Erachtens zutreffenderweise vorgetragen, s. 12. Tätigkeitsbericht, Punkt 13.2).

Der DDV wies nun jedoch in einem Gespräch mit der Aufsichtsbehörde zu Recht darauf hin, dass es unverständlich sei, wenn man über den Begriff der verantwortlichen Stelle doch wieder eine Unterrichtungspflicht über die Adressenherkunft begründen würde. Die Unterrichtungspflicht in § 28 Abs. 4 Satz 2 BDSG n.F. sei also so auszulegen, dass sie sich nur auf die Angabe des werbenden Unternehmens beziehe. Auch dieses ist verantwortliche Stelle i.S.d. § 3 Abs. 7 BDSG n.F., da es die Daten nutzt.

Mit dem DDV bestand jedoch Einigkeit, dass das werbende Unternehmen auf Verlangen des betroffenen Bürgers sicherzustellen habe, dass dieser Auskunft über die Herkunft seiner Daten erhält. Der DDV hält seine Mitgliedsunternehmen an, in diesem Sinne mitzuwirken.

Wie die jüngsten Beschwerdefälle zeigten, stand jedoch zu befürchten, dass auch nach der vorgesehenen Neuregelung (verantwortliche Stelle statt speichernde Stelle) wieder Streitigkeiten über die Auslegung des Gesetzes entstehen. Möglicherweise würden sich werbende Unternehmen auf "Unmöglichkeit" berufen, weil sie die Daten nicht selbst speichern. Daher wandte sich die Aufsichtsbehörde an das Hessische Ministerium des Innern und für Sport. Dieses setzte sich dafür ein, dass der Bundesrat eine klarstellende Ergänzung des § 28 Abs. 4 Satz 2 BDSG N.F. forderte.

Der Vorschlag des Bundesrates wurde mit geringer sprachlicher Veränderung aufgenommen.

§ 28 Abs. 4 Satz 2 BDSG n.F. lautet daher nun wie folgt:

"Der Betroffene ist bei der Ansprache zum Zwecke der Werbung oder der Markt- oder Meinungsforschung über die verantwortliche Stelle sowie über das Widerspruchsrecht nach Satz 1 zu unterrichten; soweit der Ansprechende personenbezogene Daten des Betroffenen nutzt, die bei einer ihm nicht bekannten Stelle gespeichert sind, hat er auch sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann."

Die Bundesregierung erläuterte, dass es sich insoweit um eine Erleichterung handle, als (wie oben ausgeführt) unter den Begriff der verantwortlichen Stelle, über die künftig unmittelbar im Werbeschreiben zu unterrichten ist, an sich auch der Adresssigner falle. Zugunsten der Werbetreibenden, die selbst verantwortliche Stelle seien, werde eingeräumt, dass sie die Adresssigner i.d.R. nicht kennen, sondern nur den Adressmakler/Listbroker, welcher die Datenquelle als Geschäftsgeheimnis regelmäßig nicht offenbare.

Ob die Berufung auf ein Geschäftsgeheimnis hinzuzunehmen ist, ist fraglich. Dem Interesse der Betroffenen ist jedoch durch die Verpflichtung, die Auskunftserteilung sicherzustellen (z.B. durch Weiterleitung an den Adressmakler/Listbroker), genüge getan. Gegenüber dem Betroffenen darf dieser sich nicht auf ein Geschäftsgeheimnis berufen. Mit der vorgesehenen Regelung wird also erfreulicherweise Klarheit geschaffen sein.

## **14. Datenverarbeitung in Vereinen und Verbänden**

Im Berichtszeitraum befassten sich die Aufsichtsbehörden wiederholt mit der Frage, unter welchen Voraussetzungen Vereinsmitgliederdaten durch übergeordnete Verbände übermittelt werden dürfen, wenn damit finanzielle Vorteile für den Verband verbunden sind, die wiederum der Verbands- bzw. Vereinstätigkeit förderlich sein können. Es handelte sich dabei um vertragliche Vereinbarungen, die zwischen Dachverbänden und Wirtschaftsunternehmen ausgehandelt worden waren.

### **14.1 Bundeseinheitlicher elektronischer Mitgliedsausweis**

Ein Bundessportverband traf Vereinbarungen mit einem Provider, durch welche die Erstellung eines bundeseinheitlichen elektronischen Mitgliedsausweises für alle Sportler finanziert werden sollte. Voraussetzung sollte allerdings sein, dass mindestens 30 v.H. der Mitglieder der den Landesverbänden angehörigen Ortsvereine einen Internetanschluss über den Provider nutzten, der als kostenlos bezeichnet wurde. Nach einer Online-Registrierung sollte das Vereinsmitglied eine Einwahlnummer erhalten, um ins Internet zu gelangen, für die auch Nutzungsgebühren anfallen sollten.

Den elektronischen Mitgliedsausweis sollte das Vereinsmitglied dann erhalten, wenn es ihn im Internet anforderte und seinen Internetzugang über den Provider in einem bestimmten Quartal mindestens 30 Stunden lang genutzt hätte. Nach Auslieferung des elektronischen Mitgliedsausweises sollte jedes Mitglied 20 DM bezahlen, wovon die Hälfte als Registriergebühr und je ein Viertel für den Bundesverband bzw. als Aufwandpauschale für den Kartenversand verwandt werden sollten. Der Provider sollte die Erstellung des elektronischen Mitgliedsausweises veranlassen, der durch Platzierung von Werbung von weiteren Wirtschaftsunternehmen gesponsert werden sollte.

Von der Aktion waren 1,6 Mio. Vereinsmitglieder in 15.000 Ortsvereinen, die in 20 Landesverbänden organisiert sind, betroffen.

Die bei den Landesverbänden gespeicherten Daten der Ortsvereinsmitglieder waren von einem Landesverband bereits an den Provider übermittelt worden, der seinerseits die Mitgliederlisten nochmals zum Abgleich den Ortsvereinen vorgelegt hatte.

Das zuständige Regierungspräsidium Darmstadt wies darauf hin, dass eine derartige Verknüpfung vereins- bzw. verbandsbezogener Zwecke und wirtschaftlicher Ziele Dritter datenschutzrechtlich nicht zulässig ist. Die Übermittlung der Vereinsmitgliederdaten an den Provider ist nicht von § 28 Abs. 1 Nr. 1 BDSG gedeckt, da sie nicht im Rahmen der Zweckbestimmung des Vereins- bzw. Verbandsverhältnisses erfolgt. Sie ist auch im Rahmen der Abwägung nach § 28 Abs. 1 Nr. 2 BDSG bzw. § 28 Abs. 2 Nr. 1 b BDSG nur dann als zulässig anzusehen, wenn die Mitglieder vorab über die beabsichtigte Übermittlung ihrer Daten und alle damit verfolgten Zwecke angemessen informiert werden und die Möglichkeit zum Widerspruch dagegen erhalten.

Unabhängig davon war in Zweifel zu ziehen, ob der Zweck des Bundesverbandes, den bundeseinheitlichen Mitgliedsausweis einzuführen, durch diese Aktion erreicht werden könnte, wenn man davon ausgeht, dass nicht alle Vereinsmitglieder ihren Mitgliedsausweis über das Internet abrufen wollen oder können.

Der betreffende Bundesverband hat die Aktion gestoppt und wird nun über andere Möglichkeiten der Umsetzung des elektronischen Mitgliedsausweises nachdenken, die den Datenschutzanforderungen gerecht werden.

### **14.2 Verbandszwecke und Versicherungsgeschäfte**

Über einen anderen Bundesverband im Wassersportbereich bestand für ca. 70.000 Mitglieder in 70 Ortsvereinen eine Pflicht-Gruppenversicherung aller Sportler für Unfall, Haftpflicht und Rechtsschutz bei einem Versicherungskonzern, um spezifische Risiken dieser Sportler abzudecken. Einmal jährlich wurden dabei die Namen der Mitglieder, ihre Adresse und ihr Alter an die für die einzelnen Sparten zuständigen Tochterunternehmen des Konzerns gemeldet.

Der Bundesverband kam nach Beschlussfassung der stimmberechtigten Vereine mit dem Versicherungskonzern überein, dass dieses Versicherungspaket durch eine Auslandsreisekrankenversicherung bei einem weiteren Tochterunternehmen des Konzerns erweitert werden soll. Diese Gruppenversicherung soll jedoch nicht nur bei spezifischen wassersportbedingten Unfällen, sondern bei allen im Ausland auftretenden Erkrankungen eingreifen. Die Vereine tragen die Kosten der Maßnahme durch eine Erhöhung der abzuführenden Beiträge für ihre Mitglieder an den Bundesverband. Im Gegenzug dazu verpflichtete sich der Versicherungskonzern, eine Unfall-Hotline für wassersportspezifische Unfälle im Ausland einzurichten, die verunfallten Sportlern beim raschen Auffinden spezieller Behandlungseinrichtungen im Ausland behilflich sein soll. Die von den Vereinen zu bestreitenden Mehraufwendungen setzten sich aus 5/6 der Beitragserhöhung für die Auslandsreisekrankenversicherung und 1/6 für die Fortbildung der Mediziner der Unfall-Hotline zusammen.

Einzelne Mitglieder aus den örtlichen Vereinen wandten sich gegen die zwangsweise Erweiterung der Pflichtgruppenversicherung und untersagten dem Bundesverband die Übermittlung ihrer Daten an das für die Auslandsreisekrankenversicherung zuständige Tochterunternehmen. Doch die Übermittlungen hatten bereits stattgefunden und der Bundesverband machte geltend, dass es sich lediglich um ein sinnvoll erweitertes Versicherungspaket handele, dessen günstige Konditionen nur aufrecht erhalten werden könnten, wenn alle Sportler daran teilnehmen würden. Zudem sei Schwerpunkt des Ganzen die Unfall-Hotline, die dem verbandsspezifischen Zweck, nämlich Förderung der spezifischen Wassersportart, diene. Da die Auslandsreisekrankenversicherung auch bei wassersportspezifischen Unfällen gelte, sei die Maßnahme insgesamt als datenschutzrechtlich zulässig anzusehen.

Die Aufsichtsbehörde stellte jedoch klar, dass die für die Förderung eines Vereins- oder Verbandszwecks geeigneten Maßnahmen nicht unbedingt mit dem weitaus engeren Begriff der datenschutzrechtlichen Erforderlichkeit im Rahmen der Zweckbestimmung des vertragsähnlichen Vertrauensverhältnisses übereinstimmen und dass eine allgemein gültige Auslandsreisekrankenversicherung insoweit für die Zweckbestimmung des vertragsähnlichen Vertrauensverhältnisses zwischen Sportler und Verein bzw. Bundesverband nicht als erforderlich anzusehen ist.

Im Rahmen des § 28 Abs. 1 Nr. 1 BDSG wirkt nicht jeder Beschluss so auf das vertragsähnliche Vertrauensverhältnis der einzelnen Vereinsmitglieder zu ihrem Verein ein, dass damit automatisch eine ausreichende Rechtsgrundlage für die Verarbeitung der Daten der einzelnen Vereinsmitglieder gegeben ist.

Eine Übermittlung der personenbezogenen Daten an die Auslandsreisekrankenversicherung, ohne zumindest eine Widerspruchsmöglichkeit für die Betroffenen zu ermöglichen, war auch nicht nach § 28 Abs. 1 Nr. 2 bzw. Abs. 2 Nr. 1 b BDSG gerechtfertigt. Zumindest diejenigen Betroffenen, welche die Aufnahme in die Auslandsreisekrankenversicherung ablehnten, hatten ein überwiegendes schutzwürdiges Interesse daran, dass ihre Daten nicht an die dafür zuständige Tochtergesellschaft des Konzerns übermittelt wurden.

Der Bundesverband erklärte sich nach eingehenden Erörterungen bereit, den einzelnen Vereinsmitgliedern einen nachträglichen Widerspruch (und Löschungsanspruch) gegen die Speicherung und Nutzung ihrer Daten bei der betreffenden Tochtergesellschaft des Versicherungskonzerns zu ermöglichen. Diese Widerspruchsmöglichkeit wird über die Vereine publik gemacht und an eine Frist gebunden. Die Daten von Neumitgliedern sollen nur übermittelt werden, wenn diese (freiwillig) ihre Einwilligung hierzu gegeben haben.

Noch offen ist bislang, ob die der Übermittlung bzw. Nutzung widersprechenden Sportler weiterhin den Rest des Versicherungspakets in Anspruch nehmen können oder ob ihre Teilnahme an den Unfall-, Haftpflicht- und Rechtsschutzversicherungen nunmehr entfällt. Auf die vereinsrechtlich beschlossene Erhöhung der von den Vereinen abzuführenden Beiträge für alle ihre Mitglieder hat dies keinen Einfluss.

### 14.3 Übermittlung von Sammlerdaten

Ganz andere Aspekte der Verbandstätigkeit betraf die Anfrage eines Landesverbandes von Hobbysammlern, ob die Daten derjenigen Sammler, die ihre Sammelobjekte ausstellen, in einer elektronischen Datei erfasst und an den

Bundesverband bzw. an Vereine, die an den Ausstellungsthemen interessiert sind, übermittelt werden dürfen.

Bisher wurde bei dem Landesverband eine Kartei geführt, in die die Aussteller selbst ihre Daten eintrugen. Es handelte sich dabei um die Personalien der ausstellenden Sammler, sowie um Angaben zu ihren Sammlungen einschließlich der Bewertungen, die die Sammlungen auf Ausstellungen erlangt hatten.

Wenn keine ausdrücklichen Einwilligung der Betroffenen vorliegt, ist für die Zulässigkeit der Übermittlung an übergeordnete Verbände zunächst bedeutsam, ob die jeweiligen Satzungen Bestimmungen enthalten, nach denen eine Übermittlung zur Erfüllung von spezifischen Verbandszwecken erforderlich ist. Ist die Erforderlichkeit der Übermittlung für satzungsmäßige Zwecke des Vereins/Verbandes nicht zu bejahen, liegt kein Erlaubnistatbestand nach § 28 Abs. 1 Nr. 1 BDSG vor. Eine Erlaubnis nach § 28 Abs. 1 Nr. 2 BDSG scheidet häufig an den schutzwürdigen Interessen der Betroffenen am Abschluss der Verarbeitung oder Nutzung, die gegenüber den berechtigten Interessen der Vereine/Verbände überwiegen.

Im vorliegenden Fall bedingte die Werthaltigkeit der Sammlungen der betroffenen Aussteller ein gewisses Risiko bei einer Übermittlung an Dritte.

Aber auch eine mehrheitlich beschlossene vereins-/verbandsrechtliche Satzungsänderung muss das informationelle Selbstbestimmungsrecht der Vereins-/Verbandsmitglieder berücksichtigen. Dies ist in der Regel dadurch gewährleistet, dass die Mitglieder über geplante Übermittlungen vorab informiert werden und Gelegenheit zum Widerspruch erhalten. Die Daten widersprechender Mitglieder sind mit Sperrvermerken zu versehen, so dass eine Übermittlung unterbleibt.

#### **14.4 Persönliche Angaben über Jugendliche im Vorraum einer Turnhalle**

Eine Mutter beschwerte sich darüber, dass zu ihrer Tochter und anderen jugendlichen Mitgliedern eines Vereins Angaben wie Name, Anschrift, Geburtsdatum und Trainingszeiten in einem auch für Nichtmitglieder zugänglichen Flur zu einer Sporthalle ausgehängt waren. Stichhaltige Gründe für den Umfang dieser Liste, die aus der automatisiert verarbeiteten Mitgliederdatei herausgedruckt wurde, konnte der Vorstand des Vereins nicht vortragen. Er sicherte daraufhin der Aufsichtsbehörde zu, dass zukünftig nur noch die erforderlichen Daten wie Name und Bezeichnung der zugehörigen Gruppe aufgelistet würden, damit die Übungsleiter den entsprechenden Überblick hätten. Diesem Verfahren konnte zugestimmt werden.

#### **15. Der betriebliche Datenschutzbeauftragte**

Betriebliche Datenschutzbeauftragte haben bekanntlich keine leichte Aufgabe - sie ist konfliktträchtig und stellt hohe persönliche und fachliche Anforderungen, die durch die neuen gesetzlichen Regelungen und die Zunahme der Datenverarbeitung und die Globalisierung der Wirtschaft ständig steigen.

Die deutliche Zunahme von Anfragen bei den Aufsichtsbehörden, welche die Stellung, Funktion und Aufgaben von betrieblichen Datenschutzbeauftragten betreffen, belegt, dass sich die Problematik verschärft hat.

Nur wenn Unternehmen engagierte und fachkundige Datenschutzbeauftragte bestellen und diesen vor allem auch die gesetzlich geforderte Unterstützung zukommen lassen, hat der Datenschutz eine Chance. Häufig fehlt es jedoch gerade an dieser Unterstützung. So werden betriebliche Umstrukturierungen häufig zum Anlass genommen, nebenamtlichen Datenschutzbeauftragten eine Fülle weiterer Aufgaben aufzubürden, sodass der Datenschutz zwangsläufig zu kurz kommt.

### 15.1 Kündigung eines internen Datenschutzbeauftragten, unklare Unternehmensstrukturen

Im Berichtszeitraum wandte sich ein Datenschutzbeauftragter an die Aufsichtsbehörde, weil er von seinem Arbeitgeber fristlos gekündigt worden war.

Der Datenschutzbeauftragte war interner Datenschutzbeauftragter bei der Holdinggesellschaft und externer Datenschutzbeauftragter bei einer Vielzahl konzernangehöriger Unternehmen. Bei diesen waren zu seiner Unterstützung interne Datenschutz-Koordinatoren bestellt worden.

Eines Tages ordnete die Holding die räumliche Umsetzung des Datenschutzbeauftragten zu einer der Tochtergesellschaften an. Diese Maßnahme wurde damit begründet, dass bei der Tochtergesellschaft der gewünschte größere Arbeitsraum zur Verfügung stünde, dass die Entfernung zur Holdinggesellschaft gering sei (ca. 2 km) und dass die Tochtergesellschaft umfangreiche Personaldatenverarbeitung betreibe, für die der Datenschutzbeauftragte als insoweit externer Datenschutzbeauftragter ebenfalls zuständig sei.

Der Datenschutzbeauftragte betrachtete die Umsetzung jedoch als ungerechtfertigte Benachteiligung, da er vom betrieblichen Informationsfluss abgeschnitten werde und damit eine wesentliche Voraussetzung für eine effektive Arbeit fehle. Da keine Einigung erzielt werden konnte, setzte sich der Datenschutzbeauftragte durch einen Antrag auf Erlass einer einstweiligen Verfügung gegen die Umsetzung zur Wehr.

Dies bewertete das Unternehmen als vorwerfbare Zerstörung des Vertrauensverhältnisses und sprach daher die fristlose Kündigung aus.

Die um Stellungnahme gebetene Aufsichtsbehörde wies darauf hin, dass die Kündigung eines betrieblichen Datenschutzbeauftragten einen Verstoß gegen § 36 Abs. 3 Satz 4 BDSG darstellen kann. Nach dieser Bestimmung kann die Bestellung zum Beauftragten für den Datenschutz nur auf Verlangen der Aufsichtsbehörde oder in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches widerrufen werden.

Wenn die Tätigkeit als Datenschutzbeauftragter auf der Basis eines Arbeitsvertrages erfolgt und damit Bestellung und Vertrag insoweit unlösbar miteinander verknüpft sind, dass bei Beendigung des Vertrages auch die Bestellung als Datenschutzbeauftragter endet, so können Abberufung und Kündigung nicht (völlig) getrennt betrachtet werden (Gola, Jaspers, RDV 1998, 47). Jede andere Betrachtung würde den Abberufungsschutz des § 36 Abs. 3 Satz 4 BDSG völlig ins Leere laufen lassen.

Daraus folgt: Jedenfalls dann, wenn die Kündigung zumindest in einem gewissen Zusammenhang mit der Tätigkeit des Arbeitnehmers als Datenschutzbeauftragter steht oder ein solcher Zusammenhang nicht auszuschließen ist, kann eine Kündigung nur erfolgen, wenn ein wichtiger Kündigungsgrund i.S.d. § 626 Abs. 1 BGB vorliegt.

Im konkreten Fall bestand unzweifelhaft ein solcher Zusammenhang, denn der Antrag auf Erlass einer einstweiligen Verfügung und die in diesem Zusammenhang erfolgten Äußerungen des Datenschutzbeauftragten, auf welche die Kündigung gestützt wurde, bezog sich unmittelbar auf die Tätigkeit als betrieblicher Datenschutzbeauftragter. Eine ordentliche Kündigung kam daher nicht in Betracht. Insoweit bestand auch Übereinstimmung mit dem Unternehmen, denn dieses hatte ja eine fristlose, d.h. eine außerordentliche Kündigung ausgesprochen.

Der für eine fristlose Kündigung vorausgesetzte wichtige Grund i.S.d. § 626 BGB war jedoch nach Auffassung der Aufsichtsbehörde nicht ersichtlich.

Die räumliche Umsetzung eines Datenschutzbeauftragten kann durchaus gegen das Benachteiligungsverbot bzw. die Unterstützungspflicht verstoßen. Das Benachteiligungsverbot des § 36 Abs. 3 Satz 3 BDSG erstreckt sich auch auf indirekte Benachteiligungen, wie z.B. die räumliche Auslagerung des Datenschutzbeauftragten, verbunden mit einer Isolierung von unternehmensinternen Informationsabläufen (Schlemann, Recht des betrieblichen Datenschutzbeauftragten, Rn. 4.3). Die Verpflichtung des Unternehmens gemäß § 36 Abs. 5 BDSG zur aktiven Unterstützung des Datenschutzbeauftragten

gebietet es grundsätzlich, dass dem Datenschutzbeauftragten zentral gelegene Räumlichkeiten zugewiesen werden sollten, um es den Mitarbeitern zu erleichtern, sich an ihn zu wenden (Schlemann, a.a.O., Rn. 4.5.2). Es ist dabei freilich immer eine Einzelfallbewertung erforderlich.

Der Vergleich mit externen Datenschutzbeauftragten ist dabei nicht ohne weiteres gerechtfertigt, denn die Entscheidung für einen internen Datenschutzbeauftragten bedeutet grundsätzlich auch, dass man sich für eine stärkere Präsenz und Einbindung entschieden hat, die dann auch gegeben sein muss.

Soweit jedoch durch moderne Bürokommunikationsmittel einerseits gewährleistet ist, dass Betroffene sich jederzeit vertraulich an den Datenschutzbeauftragten wenden können, z.B. durch verschlüsselte private E-Mails, und dieser andererseits von seinem Arbeitsplatz elektronischen Zugriff auf die von ihm zu kontrollierende Datenverarbeitung hat, ist eine räumliche Umsetzung relativ unkritisch.

Im konkreten Fall waren - wie sich bei späterer genauer Prüfung durch die Aufsichtsbehörde herausstellte - aber gerade die Zugriffsmöglichkeiten und sonstigen Informationen nicht gewährleistet.

Im Hinblick auf die Kündigung war die Aufsichtsbehörde der Auffassung, dass der Antrag auf Erlass einer einstweiligen Verfügung jedenfalls nicht als böswillige Schädigungshandlung bewertet werden konnte, da Indizien für eine Rechtsverletzung durch den Arbeitgeber vorlagen oder die Rechtslage zumindest unklar war.

Die Aufsichtsbehörde vermochte auch nicht zu erkennen, dass der Datenschutzbeauftragte - wie vom Unternehmen behauptet - Tatsachen offensichtlich verdreht oder falsch dargelegt hatte.

Obwohl sich der betriebliche Datenschutzbeauftragte und das Unternehmen in einem Vergleich auf eine Weiterbeschäftigung bis zum Eintritt in den Vorruhestand (und die Beibehaltung des alten Büros) einigten, sah sich die Aufsichtsbehörde zu einer umfassenden Datenschutzüberprüfung in dem Unternehmen veranlasst.

Der Datenschutzbeauftragte war dem Vorstand des Bereiches "Recht" unterstellt, während der EDV-Bereich einem anderen Vorstand zugeordnet war. Die Zuständigkeiten im EDV-Bereich waren jedoch unklar geregelt, insbesondere die Abgrenzung zwischen den Aufgaben der Informationstechnik (IT) Stelle in der Konzernmutter zu einem rechtlich ausgegliederten IT-Dienstleistungsunternehmen (das im selben Haus untergebracht war) und zu den Konzerntöchtern waren schwer nachzuvollziehen. Dies galt teilweise auch für die Abgrenzung des EDV-Bereiches zu den anderen Fachbereichen.

Der wesentliche Grund für diese Organisationsmängel ist der Datenverarbeitung zuzuordnen. Zwar befindet sich die Informationstechnik (also Geräte wie auch die Programme) auf einem sehr hohen modernen Niveau, doch die Organisation und die leitenden Mitarbeiter haben die Veränderung von der zentralen bestimmenden Datenverarbeitung zur heterogenen geöffneten, dezentralen Informationstechnik mit Auslagerung wesentlicher Teile dieser Informationstechnik nicht begleitet. Selbst die Fachabteilungen stöhnten unter Problemen, die sich für ihre tägliche Arbeit daraus ergaben.

Dabei wurde offensichtlich, dass es für den Datenschutzbeauftragten aufgrund der Organisationsstrukturen sehr schwer war, seine gesetzliche Aufgabe zu erfüllen. Es stand dem Datenschutzbeauftragten oftmals kein kompetenter Ansprechpartner zur Verfügung, der zuständig war bzw. sich zu seiner Zuständigkeit bekannte. Dies führte auch dazu, dass der Datenschutzbeauftragte sich teilweise vergeblich um die Gewährung von Zugriffsrechten bemühte.

Sowohl bezüglich der Erstellung des Dateienregisters erhielt er nicht die nötige Unterstützung als auch zur übrigen Erfüllung der Anforderungen nach § 37 Abs. 2 BDSG.

Diese Situation führte - möglicherweise verstärkt durch menschliche "Inkompatibilitäten" - bei den Akteuren dazu, dass der Datenschutzbeauftragte

bei seinen Forderungen zur Vorlage von Unterlagen oder zur Regelung der Zugriffsrechte für externe Mitarbeiter und den Einsatz von Verschlüsselungsverfahren häufig von einer Stelle zur anderen verwiesen oder ignoriert wurde. Oftmals mussten daher selbst einfache Dinge auf Vorstandsebene erörtert werden. Die Vorstandsebene hatte sich nicht hinreichend darüber verständigt, welcher Vorstand denn für die Umsetzung erforderlicher Maßnahmen zum Datenschutz und zur Datensicherheit verantwortlich war.

Wenngleich der DSB nicht selbst für die Umsetzung seiner datenschutzrechtlichen Forderungen verantwortlich ist, so muss es ihm doch einmal möglich sein, entsprechende Informationen zu erhalten, um überhaupt eine umfassende Bewertung abgeben zu können.

Darüber hinaus muss das Unternehmen selbstverständlich auch für eine effiziente Umsetzung sorgen.

Im konkreten Fall konnte die Aufsichtsbehörde erfreulicherweise im laufenden Jahr Einigkeit mit dem Unternehmen bzw. insbesondere mit dem betroffenen Vorstandsbereich EDV erzielen, dass die Zuständigkeitsregelungen etc. präzisiert werden.

## **15.2 Untätigkeit des externen Datenschutzbeauftragten**

Leider gibt es auch Fälle, bei denen die Defizite dem betrieblichen Datenschutzbeauftragten anzulasten sind.

Ein Unternehmen wandte sich an die Aufsichtsbehörde mit der Bitte um Unterstützung, weil der bestellte externe Datenschutzbeauftragte seine Aufgabe nicht ordnungsgemäß erfüllte.

Der Vertrag mit dem externen Datenschutzbeauftragten war unbefristet und die Kündigung und damit Abberufung des Datenschutzbeauftragten war laut Vertrag und Betriebsvereinbarung an die Zustimmung des Betriebsrates geknüpft, der diese jedoch zunächst nicht geben wollte; erst durch die spätere Einigungsstellenentscheidung wurde sie erteilt.

Bei der Überprüfung vor Ort durch die Aufsichtsbehörde wurde festgestellt, dass noch nicht einmal eine Verpflichtung der Mitarbeiter der Datenverarbeitungsabteilung nach § 5 BDSG vorlag und es hatte auch keine Schulung dieser Mitarbeiter stattgefunden.

Der Datenschutzbeauftragte hatte dem Unternehmen Schulungstermine in seinen eigenen Geschäftsräumen - weit entfernt von der Hauptverwaltung des Unternehmens - angeboten mit dem Hinweis, das Datenschutzgesetz gebiete eine externe Schulung. Abgesehen davon, dass das BDSG eher eine arbeitsplatzbezogene Unterrichtung verlangt, waren die Schulungsaktivitäten des Datenschutzbeauftragten jedenfalls insgesamt (ob extern oder intern) ungenügend.

Obwohl der Datenschutzbeauftragte zugleich nach § 80 Abs. 3 Betriebsverfassungsgesetz als EDV-Gutachter des Betriebsrates bestellt war, was grundsätzlich nicht zu beanstanden ist, hat nach den Feststellungen der Aufsichtsbehörde eine datenschutzrechtliche Begutachtung neuer Datenverarbeitungsverfahren zum großen Teil nicht stattgefunden. Auch eine Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme ist - nach den vor Ort gewonnenen Erkenntnissen der Aufsichtsbehörde - nicht erfolgt. Gleiches gilt für die Kontrolle von Maßnahmen zur Datensicherheit.

Die vom Unternehmen ausgesprochene Kündigung aus wichtigem Grund war daher nicht zu beanstanden.

Da noch Gerichtsverhandlungen anstehen, ist der Fall noch nicht abgeschlossen.

## **16. Datensicherheit**

### **16.1 Die günstige Flohmarkt-CD: Betriebsgeheimnisse für 3 DM!**

Durch eine Pressemeldung wurde die Datenschutzaufsichtsbehörde auf einen Fall aufmerksam, an dem leicht deutlich wird, welche drastischen Folgen der unsachgemäße Umgang mit Daten nach sich ziehen kann:

Auf einem der vielen Samstags-Flohmärkte in Hessen erstand ein Bürger für 3 DM eine selbstgebrannte CD. An seinem heimischen PC angelangt, traute er seinen Augen kaum. Die CD enthielt mehrere hundert MB vertraulicher interner Informationen aus dem EDV-System eines deutschen Großkonzerns! Mit dieser CD wandte sich der Käufer an die Presse, die ausführlich darüber berichtete.

Die Aufsichtsbehörde traf bei ihrer Überprüfung in dem Unternehmen vor Ort auf ein vorbildliches, aber auch kostenintensives Firmen-Notfallprogramm. Alle betroffenen Unternehmensbereiche waren schon mit der Analyse des Vorfalles und der Schadensbegrenzung befasst. Im vorliegenden Fall hatte trotz gegenteiliger Organisationsanweisungen zur Datensicherheit ein leitender Mitarbeiter zu Testzwecken Teile seines lokalen Datenbestandes mit seinem neuen CD-Brenner auf einen beschreibbaren Rohling kopiert und diese CD später mit nach Hause genommen. Dort geriet der brisante Datenträger versehentlich beim Hausputz auf einen Stapel Wegwerf-CDs, die dann auf dem Flohmarkt angeboten wurden.

Der Aufsichtsbehörde wurde vom betrieblichen Datenschutzbeauftragten vor Ort ein bereits existierendes und nahezu perfektes hierarchisches Sicherheitssystem präsentiert, das mit der Zuweisung fester Sicherheitsverantwortlichkeiten, internen jährlichen Datenschutz-Reviews, Kontrollen, Revisionen und Selbstprüfungs-Checklisten arbeitet. Das System wird durch ein ausgeklügeltes Werk an Regeln und Richtlinien in Handbuchform ergänzt, das ständig überprüft und aktualisiert wird. Das interne schriftliche Vorschriftenwerk für den Umgang mit unternehmensrelevanten Daten ist praktisch nicht mehr zu verbessern.

Dennoch zeigte der Vorfall, dass Datensicherheit nur angemessen verwirklicht werden kann, wenn dieses Regelsystem von den Beschäftigten vor Ort wirklich gelebt wird. Mit dem Bekanntwerden des Vorfalles durch die Veröffentlichung in den Medien sind dem Unternehmen neben der damit einhergehenden Rufschädigung auch hohe Kosten entstanden. Der betroffene Mitarbeiter, der im Unternehmen bis zu diesem Zeitpunkt auch für die Informationssicherheit und die Mitarbeiterschulungen in seiner Organisationseinheit zuständig war, und der den Vorfall wider besseres Wissen durch mangelnde Sorgfalt beim Umgang mit Firmendaten verursacht hatte, musste mit arbeitsrechtlichen Konsequenzen rechnen.

## **16.2 Die ärztliche Schweigepflicht - Ein Fall fürs Altpapier?**

Mit großer Verblüffung fand eine Bürgerin, die sich die Müllbehälter ihrer Wohnanlage mit der benachbarten ärztlichen Praxis teilte, Unterlagen mit Patientendaten in ihrer offenen Altpapierbox. Da sich der Vorfall nochmals wiederholte, schickte sie die gefundenen Unterlagen (z.B. EKG-Ausdrucke mit aufgedrucktem Namen der Patienten) an die Aufsichtsbehörde, mit der Bitte, die Vorfälle datenschutzrechtlich zu überprüfen.

Die Beamten der Aufsichtsbehörde konnten bei der unangemeldeten Überprüfung der Ärzte zwar einen Aktenschredder im Kellerarchiv finden, mussten bei der weiteren Überprüfung der Arztpraxis aber feststellen, dass in dem Betrieb keinerlei Regelungen zum Umgang mit anfallenden Unterlagen, die nicht auf Dauer aufbewahrt werden müssen, existierten. Der betroffene Arzt begründete diesen Zustand zunächst sogar damit, in seiner Praxis würde nichts ausgedruckt, was nicht auch im Kellerarchiv aufbewahrt würde. Diese Angabe musste er zurücknehmen, als ihm seine in der Altpapierbox gefundenen EKG-Ausdrucke überreicht wurden. Die Entsorgung von Patientenunterlagen blieb in dieser Arztpraxis offensichtlich dem Gutdünken der jeweiligen Arzthelferin oder sogar der Putzfrau überlassen. Dieser Zustand wurde unter Hinweis auf § 203 StGB ausdrücklich beanstandet.

Die ärztliche Schweigepflicht schützt Patientendaten in jeder Form (Akte, Karteikarte, Computerausdruck, Röntgenbild). Unterlagen mit Patientendaten sind, falls sie nicht aufbewahrt werden müssen, aufgrund ihrer Sensibilität grundsätzlich selbst mit einem Schredder zu zerkleinern.

Der Arzt wurde aufgefordert, verbindliche interne Anweisungen in seiner Praxis zu erlassen, die regeln, wie mit Patientenunterlagen umgegangen wird und wer in welcher Form für die datenschutzgerechte Vernichtung von Unterlagen zuständig ist.

### 16.3 Keinerlei Sicherheitskonzept bei Auftragsdatenverarbeiter

Der Betriebsrat eines Dienstleistungs-Unternehmens, das in erheblichem Umfang personenbezogene Daten für seine Auftraggeber verarbeitet, wandte sich mit der Bitte um Unterstützung an die Aufsichtsbehörde.

In der Regel sind derartige Dienstleister auch im Hinblick auf die Kontrollen, die die Auftraggeber durchführen, sehr sensibilisiert und achten sehr auf entsprechend abgesicherte Datenverarbeitungsverfahren. Nicht so in diesem Unternehmen. Der Betriebsrat konnte dem Vertreter der Aufsichtsbehörde vorführen, dass jeder Mitarbeiter über einen frei zugänglichen Rechner, der auch noch die Möglichkeit der privaten Nutzung von Internetdiensten bietet, Zugriff auf Personaldaten und auf Vertragsdaten zwischen Dienstleister und seinen Auftraggebern haben konnte. Erschwerend kommt im vorliegenden Fall auch hinzu, dass das Unternehmen aufgrund seiner Tätigkeit sehr viel mit Aushilfskräften und gering bezahlten Arbeitskräften zu tun hat. Bei der Befragung des Datenschutzbeauftragten musste bedauerlicherweise festgestellt werden, dass dieser zwar einmal - auch bereits auf Anforderung der Aufsichtsbehörde hin - vor Jahren ein Fachseminar besucht hatte, aber ansonsten keinerlei Tätigkeit im Unternehmen entwickelt hatte. Weder Schulungen von Mitarbeitern noch Kontrollen waren vom Datenschutzbeauftragten durchgeführt worden. Auch nach der Überprüfung zeigte die Geschäftsführung nur wenig Einsicht. Eine weitere Überprüfung ergab dann allerdings, dass zumindest die offene Zugriffsmöglichkeit auf die oben erwähnten Daten nicht mehr gegeben ist. Es fehlt nach wie vor an einem Sicherheitskonzept und an Vorgaben zu Maßnahmen zur Datensicherheit, wie z.B. Regelungen der Zugriffsberechtigungen, entsprechenden Maßnahmen zur Eingabekontrolle usw. Unglaublich, aber wahr ist auch, dass als Passwort in der Regel die Personalnummern der Mitarbeiter genutzt wurden. Es bleibt abzuwarten, wie das Sicherheitskonzept aussehen wird.

### 16.4 Aktionärsdaten ungeschützt im Internet abrufbar

Im Zusammenhang mit der Neuemission von Aktien waren Dateien mit Avis-Listen über zugeteilte Aktien auf einen falschen Rechner übertragen worden.

Die entsprechende URL (Internet-Adresse) war zwar nicht "verlinkt", aber für jedermann über das Internet erreichbar. So konnten Internetnutzer, die die URL in Newsgroups und Diskussionsforen erfahren hatten, lesen, wer Aktien in welchem Umfang und zu welchen Konditionen zugeteilt erhalten hatte.

Diese Avis-Listen wurden von dem Unternehmen in der Regel ausgedruckt und zur Beschleunigung der Gutschrift der Aktien den einzelnen Banken per Telefax zugesandt. Der Telefaxversand war hierbei ein zusätzlicher Schwachpunkt, wünschenswert wäre eine verschlüsselte direkte Übermittlung an die Banken ohne Medienbruch. Diese Verfahrensweise ist im übrigen rationeller.

Das betroffene Unternehmen teilte hierzu mit, dass es den Übertragungsweg so abgeändert habe, dass ein gleicher oder ähnlicher Fehler zukünftig ausgeschlossen sei. Die Daten werden verschlüsselt per E-Mail übertragen.

### 17. Die nicht alltägliche Geschäftsidee

Die Aufsichtsbehörde erreichte eine Anfrage zu einer eher ungewöhnlichen Geschäftsidee. Nach amerikanischem Vorbild wollte der Anfragende eine Agentur eröffnen, die im Auftrag genervter Mitmenschen anderen Personen Hinweise zukommen lassen wollte, dass sie Probleme mit Mund-, Körper- und/oder Fußgeruch oder Ähnlichem hätten.

Zu diesem Zweck sollten die personenbezogenen Daten der Betroffenen automatisiert gespeichert werden. Der Informant sollte dabei anonym bleiben. Die Aufsichtsbehörde verneinte die Zulässigkeit einer solchen Datenverarbeitung, da schutzwürdige Belange der Betroffenen am Ausschluss der Verarbeitung gegenüber den Geschäftsinteressen des Anfragenden überwiegen würden. Neben den Adressdaten der Betroffenen würden nämlich negative, überdies nicht verifizierte, körperliche Befindlichkeitsmerkmale gespeichert, die ähnlich den Gesundheitsdaten zu bewerten und mit besonderer Vorsicht

zu behandeln wären. Der anonym bleibende Informant würde diese vermeintlichen Probleme über Dritte (die Agentur) mitteilen, was einen demütigenden und nötigenden Charakter für den Betroffenen haben könnte. Zudem wären Missbrauchsmöglichkeiten nicht auszuschließen, durch die der Betroffene schikaniert werden könnte.

Letztlich ist zu bedenken, dass der sittliche, personale und soziale Geltungswert und der daraus folgende Achtungsanspruch eines Menschen durch strafrechtliche Bestimmungen geschützt ist, die durch die möglicherweise nicht verifizierbaren negativen Tatsachenbehauptungen bzw. die Art und Weise der Kundgabe verletzt werden könnten (Beleidigung, üble Nachrede, §§ 185, 186, 192 StGB).

## **18. Aus dem Alltag einer Datenschutzbehörde**

Oft sind es immer wieder die gleichen Verstöße und Fragestellungen, mit denen sich die Aufsichtsbehörde befassen muss. Dies zeigt, dass es bei vielen Unternehmen an grundlegenden Datenschutzkenntnissen fehlt.

### **18.1 Marktforscher nicht zum Register gemeldet**

Zu den "Standardverstößen" gehört die Missachtung der Meldepflicht nach § 32 BDSG. Leider muss immer wieder festgestellt werden, dass selbst Unternehmen, bei denen aufgrund ihres Geschäftsgegenstandes an sich besondere Kenntnisse des Datenschutzrechts zu erwarten wären, die Meldung unterlassen. So wurde der Aufsichtsbehörde bekannt, dass ein Marktforscher, der schon seit Jahren aktiv ist, unter anderem für einen großen Automobilkonzern, keine Meldung vorgenommen hatte.

Die Dauer des Verstoßes wird sich auf das anstehende Bußgeldverfahren negativ auswirken.

Der Automobilkonzern hätte aber auch das Marktforschungsunternehmen befragen sollen, ob es bei der zuständigen Aufsichtsbehörde gemeldet ist und ob u.U. auch schon eine Überprüfung (mit welchem Ergebnis?) stattgefunden hat. Da sowohl die Kunden als auch der Marktforscher das Erfordernis der Meldepflicht nicht in ihre Überlegungen einbezogen, konnte das Unternehmen bisher von der Datenschutzaufsicht unbehelligt tätig werden. Nach den bisherigen Erfahrungen prüfen lediglich Banken und Versicherungen vor Auftragsvergabe die Einhaltung der Meldepflicht durch den Auftragnehmer.

### **18.2 Name und Anschrift einer Kundin in Fahrplanheft**

In Zeiten, in denen Menschen ihre Privatsphäre in den Medien, insbesondere in Nachmittags-Talkshows und in Fernsehsendungen wie "Big Brother", völlig preisgeben, wird oft vergessen, dass auch bei weniger intensiven Offenbarungen der Privatsphäre eines Menschen das Recht auf informationelle Selbstbestimmung beachtet werden muss.

Ein Unternehmen, das für Verkehrsunternehmen Fahrpläne herausgibt, hatte in einem Fahrplanheft Werbung für ein vergünstigtes Schülerticket abgedruckt. Zu diesem Zweck wurde eine Schülerfahrkarte mit Namen und Anschrift einer Schülerin, an die tatsächlich eine solche Fahrkarte verkauft worden war, in dem Fahrplanheft abgedruckt.

Als die überraschte Schülerin, die nicht um ihr Einverständnis gebeten worden war, dies entdeckte, verlangte sie mit anwaltlichem Schreiben, dass das Unternehmen die Verbreitung des Fahrplanheftes unterlasse. Außerdem verlangte sie Abgabe einer entsprechenden Unterlassungserklärung und Zahlung des Anwaltshonorars.

Die daraufhin von dem Unternehmen um datenschutzrechtliche Bewertung gebetene Aufsichtsbehörde bestätigte, dass hier eindeutig ein Verstoß gegen das Bundesdatenschutzgesetz vorliegt. Weder § 28 noch § 29 BDSG enthalten einen Erlaubnistatbestand für die Veröffentlichung der Daten der Schülerin, sodass nach § 4 Abs. 1 BDSG deren schriftliche Einwilligung hätte eingeholt werden müssen.

Bereits im letzten Tätigkeitsbericht wurde unter Nr. 11.3 zu einem vergleichbaren Fall, in dem Daten einer Arbeitnehmerin zu Demonstrations- und Werbezwecken auf einer Chipkarte abgedruckt wurden, berichtet.

Die dort gegebene Empfehlung, fiktive Daten unter der Bezeichnung "Musterfrau" oder "Mustermann" zu verwenden, wird nochmals bekräftigt.

Im aktuellen Fall hat das Unternehmen den Fehler bedauert und alle Maßnahmen ergriffen, um eine Verbreitung des Fahrplanheftes zu verhindern.

### **18.3 Offenlegung der Putzfrauenabrechnung gegenüber Mietern**

Zu den immer wiederkehrenden Fragestellungen gehört die Frage, inwieweit es zulässig ist, dass ein Vermieter im Rahmen einer Nebenkostenabrechnung gegenüber dem jeweiligen Mieter Daten Dritter offenbart.

Wenn Nebenkosten nach Verbrauchsanteilen abgerechnet werden, haben Mieter ein berechtigtes Interesse i.S.d. § 28 Abs. 2 Nr. 1a BDSG an der Übermittlung der Abrechnungsdaten der übrigen Hausbewohner (Simitis in Simitis/Dammann/Geiger/Mallmann/Walz, Kommentar zum BDSG, § 28, Rn. 194, unter Hinweis auf AG Flensburg, Dok. § 24 BDSG 77 E 9). Schutzwürdige Belange der übrigen Hausbewohner stehen der Übermittlung nicht entgegen.

Werden Nebenkosten nach den tatsächlich entstandenen Kosten abgerechnet, so haben die Mieter auch ein berechtigtes Interesse an der Offenlegung der entsprechenden Belege. Werden etwa Reinigungskosten umgelegt, so hat der Vermieter die Reinigungskostenbelege vorzulegen.

In einem konkreten Fall wandte der Vermieter jedoch ein, dass schutzwürdige Belange der Putzkraft entgegenstehen könnten, denn diese sei selbst Mieterin. Durch die Offenlegung der Belege erhielten die anderen Mieter Einblick in die Einkommenssituation der als Putzkraft beschäftigten Mieterin.

Die Aufsichtsbehörde war jedoch der Auffassung, dass die Putzkraft kein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Als Mieterin weiß sie bzw. muss sie wissen, dass die Nebenkosten dargelegt und nachgewiesen werden müssen. Die Vorlage anonymisierter Kopien der Reinigungskostenbelege wäre nicht ausreichend, denn die Mieter müssen die Möglichkeit haben, nachzuprüfen, ob die Kosten tatsächlich entstanden sind. Im übrigen dürfte die Tatsache, dass die betreffende Mieterin als Putzkraft beschäftigt ist, ohnehin bekannt sein. Dem Vermieter ging es - wie sich letztlich herausstellte - auch nicht um die Schwärzung des Namens, sondern darum, die Belege überhaupt nicht vorzulegen. Ohne Nachweis der gezahlten Beträge ist jedoch eine entsprechende Umlegung der Kosten nicht möglich.

## **19. Ordnungswidrigkeitenverfahren**

Im Berichtsjahr 2000 wurden von den Aufsichtsbehörden fünf Verfahren nach dem Gesetz über Ordnungswidrigkeiten nach § 44 Abs. 1 BDSG gegen die Geschäftsführer datenverarbeitender Gewerbebetriebe mit einer Gesamtbußgeldsumme von 10.500 DM eingeleitet.

Zwei dieser Verfahren betrafen Unternehmen, die als Dienstleistungsdatenverarbeiter der Meldepflicht zum bei den Aufsichtsbehörden geführten Register nach § 32 Abs. 1 BDSG und damit der Regelaufsicht der Behörden unterliegen. Beide Unternehmen hatten sich nicht rechtzeitig innerhalb von vier Wochen nach Aufnahme der meldepflichtigen Tätigkeit ordnungsgemäß zum Register der meldepflichtigen Stellen angemeldet.

Wenngleich die Meldepflicht für Datenverarbeitungsdienstleister nach der Novelle des BDSG voraussichtlich entfallen wird, so entschieden sich die Aufsichtsbehörden in den konkreten Fällen gleichwohl für die Einleitung von Bußgeldverfahren, denn die Verletzung der Meldepflicht war - wie so oft - symptomatisch für eine generelle Nachlässigkeit in der Beachtung der datenschutzrechtlichen Vorschriften. Unter Berücksichtigung der jeweiligen Umstände wurde in dem einen Fall ein Bußgeld in Höhe von 2.000 DM und im anderen Fall in Höhe von 1.000 DM verhängt. Beide Bußgeldbescheide haben noch im Berichtsjahr Rechtskraft erlangt.

Zwei Ordnungswidrigkeitenverfahren nach § 44 Abs. 1 Ziff. 6 BDSG wegen der trotz mehrfacher Erinnerung nicht erfolgten Erteilung von Auskünften an die Aufsichtsbehörden entgegen § 38 Abs. 3 Satz 1 BDSG richteten sich gegen die Geschäftsführer eines Möbelhauses und eines Unternehmens der Werbe- und Direktmarketingbranche.

Der Geschäftsführer des Möbelhauses war bis zum Zeitpunkt der Erstellung dieses Berichtes nicht bereit, der Aufforderungen der Datenschutzaufsichtsbehörde zur Auskunftserteilung nachzukommen. Obwohl das Unternehmen sowohl schriftlich als auch persönlich vor Ort auf seine gesetzlichen Auskunftspflichten hingewiesen wurde, gingen lediglich ausweichende Antworten in Verbindung mit unsachlichen Drohungen und Unterstellungen des Geschäftsführers bei der Datenschutzaufsicht ein. Daher musste dem Anspruch der Behörde auf rechtzeitige, vollständige und korrekte Auskünfte mit dem Erlass eines Bußgeldbescheides über 3.000 DM der erforderliche Nachdruck verliehen werden. Über den Einspruch gegen diesen Bußgeldbescheid wird das zuständige Amtsgericht noch entscheiden.

Die Geschäftsführerin des Unternehmens aus der Werbewirtschaft hatte es versäumt, dafür zu sorgen, dass der Aufsichtsbehörde auf Fragen, die sich aus einer Datenschutzüberprüfung vor Ort ergaben, unverzüglich vollständige und korrekte Antworten erteilt wurden. Erst nachdem ihr ein Bußgeldbescheid über 2.000 DM wegen der unvollständigen Erteilung von Auskünften zugestellt wurde, konnte die Aufsichtsbehörde registrieren, dass datenschutzrechtliche Fragestellungen nun auch ernst genommen wurden. Der von den Anwälten der Werbefirma zwischenzeitlich eingelegte Einspruch gegen den Bußgeldbescheid wurde zurückgezogen, nachdem die Aufsichtsbehörde das Verfahren dem zuständigen Amtsgericht zur Entscheidung vorgelegt hatte.

In einem weiteren Verfahren wurde gegen den Verantwortlichen einer Lottereeinnahmestelle wegen nicht rechtzeitig erfolgter Bestellung eines Datenschutzbeauftragten nach § 36 BDSG eine Geldbuße in Höhe von 1.800 DM und wegen einer nicht vollständig erteilten Auskunft eine Geldbuße in Höhe von 700 DM erlassen. Der Bußgeldbescheid ist unmittelbar rechtskräftig geworden.

Immer wieder müssen die Bediensteten der Regierungspräsidien bei der Bearbeitung der Beschwerden betroffener Bürgerinnen und Bürger feststellen, dass vielen Unternehmen datenschutzrechtliche Regelungen und vor allem auch ihre Pflichten gegenüber den von der Verarbeitung ihrer Daten betroffenen Personen und den Aufsichtsbehörden nicht bekannt sind. Fast alle betroffenen Unternehmen sind allerdings nach entsprechenden Hinweisen und Informationen durch die Datenschutzaufsichtsbehörden jedenfalls bemüht, ihre Datenverarbeitung transparenter, datenschutzfreundlicher und gesetzeskonform zu gestalten. Die Einleitungen von Verfahren nach dem Gesetz über Ordnungswidrigkeiten mit dem Ziel, Bußgelder zu erlassen, bleiben glücklicherweise Ausnahmen im Alltagsgeschäft der Datenschutzaufsichtsbehörden, das ansonsten immer nachhaltiger von konstruktiv-beratenden Tätigkeiten geprägt wird.

Wiesbaden, 21. August 2001

Der Hessische Ministerpräsident  
**Koch**

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

#### Anlagen

1. Meldeformular
2. Merkblatt zur Meldepflicht
3. Entscheidungsbaum DSB
4. Entscheidungsbaum Meldepflicht

Hauptblatt

**Anmeldung**

gemäß § 4d Bundesdatenschutzgesetz (BDSG) zum Register nach § 38 Abs. 2 BDSG  
gegenüber der Datenschutzaufsichtsbehörde

beim .....

**1. Name / Firma der verantwortlichen Stelle**

**2. Verantwortungsträger**

**2.1 Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzlich oder nach der  
Verfassung des Unternehmens berufene Leiter der verantwortlichen Stelle**

**2.2 Mit der Leitung der Datenverarbeitung beauftragte Person(en)**

**2.3 Bei verantwortlicher Stelle mit Sitz außerhalb der EU:  
Im Inland ansässiger Vertreter (§ 1 Abs. 5 Satz 3 BDSG)**

**2.4 Name des Datenschutzbeauftragten der verantwortlichen Stelle \*)**

\*) s. Begründung im Merkblatt unter III

**3. Verantwortliche Stelle**

**3.1 Anschrift, ggfs. Telekommunikationsverbindungen (Telefon, Fax, eMail, etc.) der verantwortlichen Stelle**

**3.2 Bei verantwortlicher Stelle mit Sitz außerhalb der EU:  
Anschrift, ggfs. Telefon- und/oder Faxnummer des im Inland ansässigen Vertreters  
(§ 1 Abs. 5 Satz 3 BDSG)**

.....  
Ort, Datum und Unterschrift

Wird von der Aufsichtsbehörde ausgefüllt!

Aktenzeichen:

Meldeschlüssel:

**Anlage Nr. \_\_\_\_\_ \*)**

\*) für jedes automatisierte Verfahren ist eine separate Anlage auszufüllen

**Name der verantwortlichen Stelle**

**4. Zweckbestimmung der Datenerhebung, Datenverarbeitung oder Datennutzung  
(verfahrensbezogen)**

**5. Personengruppen und Datenkategorien**

**5.1 Beschreibung der betroffenen Personengruppen (je nach Anwendung bzw. Verfahren)**

**5.2 Beschreibung der Art der gespeicherten personenbezogenen Daten oder  
Datenkategorien**

**6. Empfänger oder Kategorien von Empfängern, denen Daten mitgeteilt/übermittelt werden können (bei Datentransfers in Drittstaaten [das sind Nicht-EU-Länder] siehe Nr. 8)**

**7. Regelfristen für die Löschung der Daten (verfahrensbezogen)**

**8. Datenübermittlung in Drittstaaten (Nicht EU-Länder)**

**Empfänger/Kategorien von Empfängern (mit Angabe des Drittstaates) und Art der Daten oder Datenkategorien (getrennt nach Empfänger/Drittstaat)**

## Nicht-öffentlicher Teil

### 9. Angaben zur Beurteilung der Angemessenheit getroffener Sicherheitsmaßnahmen

#### 9.1 Art der eingesetzten DV-Anlagen (Konfigurationsübersicht, Netzwerkstruktur), Betriebs- und Anwendungssoftware, spezielle Sicherheitssoftware

#### 9.2 Technisch-organisatorische Maßnahmen nach § 9 BDSG (einschließlich Anlage)

### 10. Zeitpunkt der Aufnahme der meldepflichtigen Tätigkeit:

Die Angaben unter Nr. 1 - 8 u. Nr. 10 können nach § 38 Abs. 2 Satz 2 BDSG von jedem eingesehen werden.

Die unter Nr. 9 mitzuteilenden Angaben werden gemäß § 38 Abs. 2 Satz 3 BDSG nicht in das öffentlich zugängliche Register aufgenommen.

Wird von der Aufsichtsbehörde ausgefüllt!

Aktenzeichen:

Meldeschlüssel:

.....  
Ort, Datum und Unterschrift

**Merkblatt zur Meldepflicht verantwortlicher nicht-öffentlicher Stellen  
gemäß § 4 d BDSG bei der Datenschutzaufsichtsbehörde**

## I. Allgemeines

Das Bundesdatenschutzgesetz (BDSG) ist bei der Erhebung, Nutzung und Verarbeitung personenbezogener Daten anzuwenden, wenn die Daten unter Einsatz von Datenverarbeitungsanlagen (also automatisiert) oder in oder aus nicht-automatisierten Dateien verarbeitet oder genutzt oder dafür erhoben werden und dies nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt.

## II. Zur Meldepflicht

### Wer muss melden? Was ist Gegenstand der Meldepflicht?

Bestimmte Verfahren automatisierter Verarbeitungen personenbezogener Daten müssen bei der Datenschutzaufsichtsbehörde gemeldet werden. Diese Meldepflicht trifft nach der Novellierung des BDSG immer die Stelle, die für die Verarbeitung verantwortlich ist. Verantwortlich im Sinne des BDSG sind Stellen nicht nur, wenn sie die Verarbeitung selbst ausführen, sondern auch dann, wenn sie sich hierbei eines Dienstleistungsunternehmens bedienen, das die Verarbeitung in ihrem Auftrag vornimmt (§ 3 Abs. 7 BDSG). Ggf. trifft also den Auftraggeber die Meldepflicht.

Meldepflichtig sind nur Verfahren automatisierter Verarbeitungen, wobei es auf den Zweck der Verarbeitung ankommt.

Die automatisierten Verarbeitungen personenbezogener Daten durch Stellen, die Datenverarbeitung zum Zweck der Übermittlung (§ 29 BDSG, z. B. Auskunftseiten, Adresshandel) oder zum Zweck der anonymisierten Übermittlung (§ 30 BDSG, z.B. Markt- u. Meinungsforscher) betreiben oder betreiben lassen, sind ohne Ausnahme meldepflichtig (§ 4 d Abs. 1 i.V.m. Abs. 4 BDSG).

Verantwortliche Stellen, die personenbezogene Daten automatisiert zu eigenen Zwecken gem. § 28 BDSG verarbeiten (oder im Auftrag von Dienstleistungsunternehmen verarbeiten lassen), haben diese Verarbeitungen nur dann zu melden, wenn die Verarbeitung mit höchstens vier Arbeitnehmern erfolgt und hierfür keine Einwilligung der betroffenen Personen oder keine Rechtsgrundlage gem. § 28 Abs. 1 Nr. 1 BDSG vorliegt und kein betrieblicher Datenschutzbeauftragter bestellt wurde (§ 4 d Abs. 3 i.V.m. Abs. 2 BDSG).

Stellen, die mit mehr als vier Arbeitnehmern personenbezogene Daten gem. § 28 BDSG automatisiert verarbeiten, müssen immer einen betrieblichen Datenschutzbeauftragten bestellen (§ 4 f Abs. 1 Satz 1 BDSG) und sind gem. § 4 d Abs. 2 BDSG von der Meldepflicht befreit, sobald sie ihrer Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten nachgekommen sind. Stellen mit weniger als 5 Arbeitnehmern können freiwillig einen betrieblichen Datenschutzbeauftragten bestellen, sie sind dann ebenfalls von der Meldepflicht frei. Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, ist eine Vorabkontrolle durchzuführen; in diesen Fällen ist stets ein betrieblicher Datenschutzbeauftragter zu bestellen, eine Meldepflicht besteht dann nicht mehr, sobald die Bestellung erfolgt ist (§§ 4 d Abs. 2 und 5, 4 f Abs. 1 Satz 6 BDSG).

Zum besseren Verständnis wird auch auf beiliegenden Entscheidungsbaum zur Meldepflicht hingewiesen. Ergänzend ist ein Entscheidungsbaum zur Pflicht, einen betrieblichen Datenschutzbeauftragten zu bestellen, beigefügt, da bei Datenverarbeitungen gemäß § 28 BDSG die Meldepflicht entfällt, wenn ein Datenschutzbeauftragter bestellt wurde.

### **Wann muss gemeldet werden?**

Nach § 4 d Abs. 1 BDSG hat die Meldung bereits vor der Inbetriebnahme der meldepflichtigen Datenverarbeitung zu erfolgen. Auch Änderungen der meldepflichtigen Angaben und die Beendigung der meldepflichtigen Tätigkeit sind vorher mitzuteilen (§ 4 e Satz 2 BDSG).

### **Bei wem muss gemeldet werden?**

Die Meldung muss bei der gemäß § 38 Abs. 1 BDSG zuständigen Aufsichtsbehörde für den Datenschutz erfolgen, in deren Aufsichtsbezirk die meldepflichtige Stelle ihren Sitz hat. An welchem Ort im Inland die Datenverarbeitung erfolgt, ist für die Meldung also unerheblich. Wenn die meldepflichtige Stelle ihren Sitz außerhalb der Europäischen Union hat, muss die Meldung bei der Aufsichtsbehörde erfolgen, in deren Zuständigkeitsbereich der im Inland ansässige Vertreter der meldepflichtigen Stelle seinen Sitz hat.

### **III. Notwendiger Inhalt der Meldungen**

Welche Angaben bei der Meldung gemacht werden müssen, ist aus dem zu verwendenden **Meldeformular** ersichtlich.

Das **Hauptblatt** mit den geforderten Angaben zu verantwortlichen Stellen und den dortigen Verantwortungsträgern (Nr. 1 - 3.2) ist von jeder Stelle nur einmal auszufüllen. Die Angaben zu den jeweiligen automatisierten Verfahren sind mit dem Formular „**Anlagen**“ (Nr. 4 - 9.2) für jedes einzelne betriebene Verfahren gesondert zu melden. Der Name der verantwortlichen Stelle muss im Kopf der Anlage nochmals angegeben werden.

Wenn eine meldepflichtige Stelle nach der Meldung weitere meldepflichtige Verfahren durchführt oder durchführen lässt, genügt es, wenn sie lediglich eine neue Anlage ausfüllt und vorlegt. Ebenso ist zu verfahren, wenn sich Änderungen bei bereits gemeldeten Verfahren ergeben (wobei dann die Nummerierung der geänderten Anlage anzugeben ist). Das Hauptblatt ist nur dann neu auszufüllen, wenn sich auch insoweit Änderungen ergeben.

Die rechtliche Notwendigkeit für die im Formular geforderten Angaben ergibt sich – bis auf Nr. 2.3, 2.4 und 3.2 – aus § 4 e BDSG.

Die unter Nr. 2.3 und 3.2 geforderten Angaben zu dem im Inland ansässigen Vertreter einer außerhalb der Europäischen Union gelegenen verantwortlichen Stelle sind gemäß § 1 Abs. 5 Satz 3 BDSG notwendig.

Sofern ein betrieblicher Datenschutzbeauftragter nach § 4 f BDSG zu bestellen ist oder auf freiwilliger Basis bestellt wurde, ist dessen Angabe bei den gemäß § 4 d Abs. 4 Nr. 1 und 2 BDSG gleichwohl meldepflichtigen Unternehmen erforderlich, da dieser gemäß § 4 f Abs. 5 Satz 2 BDSG auch der Ansprechpartner für Bürgerinnen und Bürger ist.

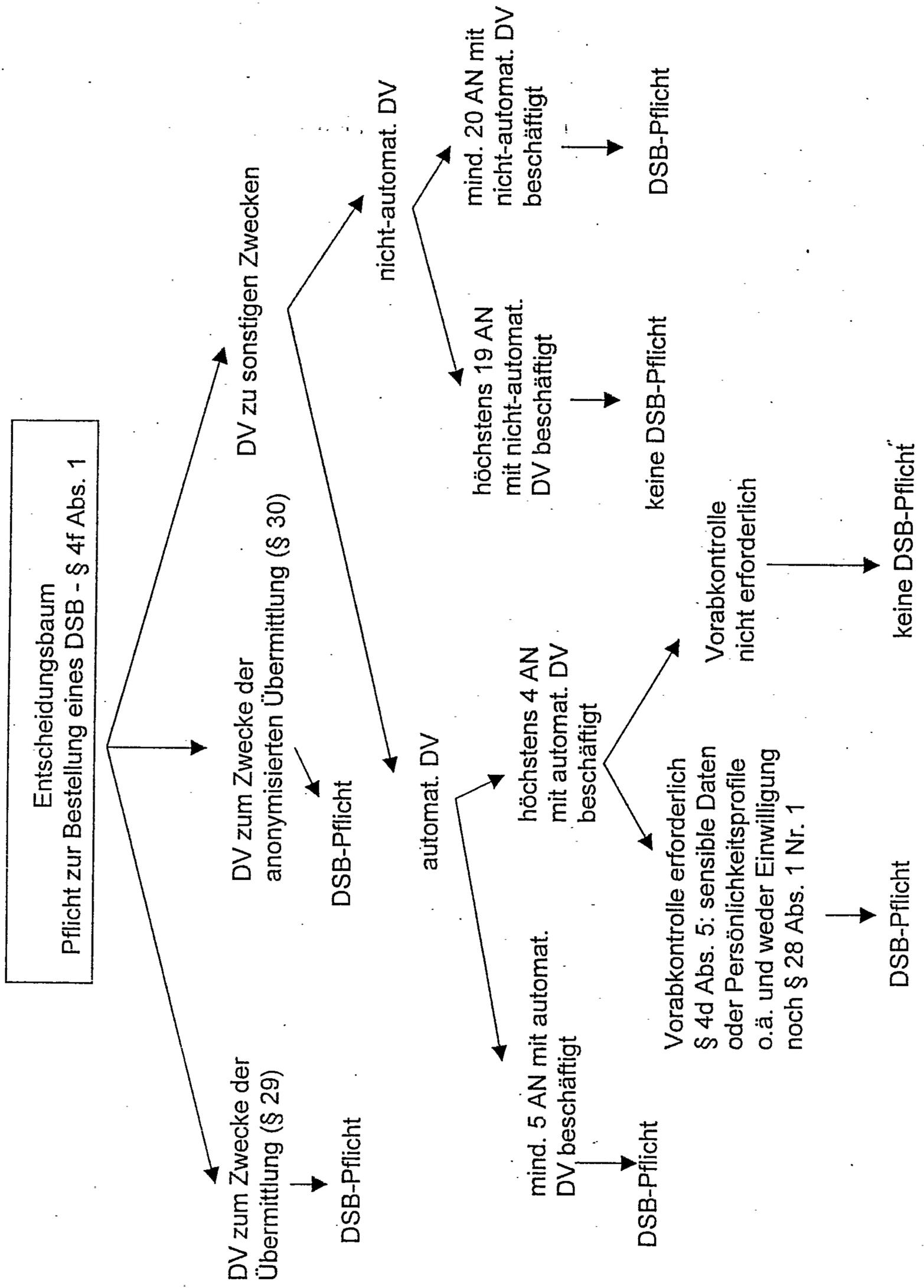
Weitere Erläuterungen zum Formular:

Nr. 5.1: Als betroffene Personengruppen kommen beispielsweise „Kunden“ oder „Arbeitnehmer“ in Betracht

- Nr. 5.2: Bei Daten, die unter § 3 Abs. 9 BDSG fallen („sensitive Daten“), sind möglichst detaillierte Angaben (Datenfeldbezeichnungen) erforderlich.
- Nr. 8: § 4e Nr. 8 BDSG fordert die Angabe der geplanten Übermittlungen in Drittstaaten. Nur bei der Erstmeldung zum Register sind auch die bereits bestehenden Übermittlungen zu melden. Bei Änderungsmitteilungen genügt die Meldung neu geplanter Übermittlungen in Drittstaaten.

#### **IV. Abschließender Hinweis**

Wenn eine verantwortliche nicht-öffentliche Stelle vorsätzlich oder fahrlässig entgegen § 4 d Abs. 1 und 4 BDSG, auch in Verbindung mit § 4 e Satz 2 BDSG, eine Meldung nicht erstattet oder entgegen § 4 e Satz 1 BDSG, auch in Verbindung mit § 4 e Satz 2 BDSG, bei einer solchen Meldung die erforderlichen Angaben nicht, nicht richtig oder nicht vollständig mitteilt, begeht sie gem. § 44 Abs. 1 Nr. 2 BDSG eine Ordnungswidrigkeit, die mit einer Geldbuße bis zu 50.000,- DM geahndet werden kann.



Entscheidungsbaum  
Meldepflicht (MPf) gegenüber den Datenschutzaufsichtsbehörden - § 4d

Verarbeitung personenbezogener Daten durch die verantwortliche Stelle selbst oder durch einen von ihr eingeschalteten Dienstleister.

