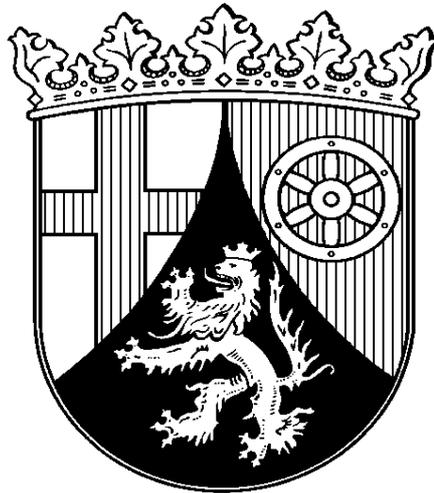


Aufsichts- und Dienstleistungsdirektion



Rheinland-Pfalz

**Zweiter
Tätigkeitsbericht
über den Datenschutz
im nicht-öffentlichen Bereich**

Zweiter Tätigkeitsbericht

der Aufsichts- und Dienstleistungsdirektion
als Aufsichtsbehörde für den Datenschutz im
nicht-öffentlichen Bereich in
Rheinland-Pfalz

für den Zeitraum vom 01. Juni 2003
bis zum 31. Mai 2005

(abrufbar über das Internet unter: <http://www.add.rlp.de>)

Herausgeber:

Aufsichts- und Dienstleistungsdirektion (ADD)

Willy-Brandt-Platz 3

54290 Trier

Tel.: 0651/9494-0

Fax: 0651/9494-170

E-Mail: poststelle@add.rlp.de

www.add.rlp.de

Inhaltsverzeichnis

Vorwort.....	6
I. Allgemeiner Teil	7
1. Zuständigkeit der Aufsichts- und Dienstleistungsdirektion	7
2. Das Melderegister	8
3. Überprüfungen im Rahmen der Regelaufsicht	9
4. Bearbeitung von Eingaben und Beschwerden	10
5. Bearbeitung von Anfragen / Beratungsgesuchen	13
6. Ordnungswidrigkeiten	15
6.1 Berichtszeitraum 2003 – 2005	15
6.2 Ordnungswidrigkeitsverfahren aus dem Berichtszeitraum 2001 - 2003	16
7. Workshop der Aufsichtsbehörden für den Datenschutz im nicht- öffentlichen Bereich	17
II. Einzelfälle aus der Praxis der Aufsichtsbehörde.....	18
1. Handel /Auskunfteien.....	18
1.1 Erhebung personenbezogener Daten bei Umtausch / Reklamation von Waren	18
1.2 Verkauf einer gebrauchten Festplatte	19
1.3 Werbeaktion eine Verlages	20
1.4 Kundendatenschutz	22
2. Datenschutz bei Banken	23

2.1	Zugriff eines selbständigen Finanzberaters auf Kontodaten einer Bankkundin	23
2.2	Bekanntgabe von Kontodaten durch eine Bankangestellte an einen Dritten	25
2.3	Erteilung eines Suchauftrages an die SCHUFA.....	26
3.	Versicherungen	27
3.1	Notruf der Autoversicherer.....	27
3.2	Was dürfen Versicherungsunternehmen wie lange speichern? .	30
4.	Internet	31
4.1	Datenschutzrechtliche Zulässigkeit von Altersverifikationssystemen.....	31
4.2	Fehlende Anbieterkennzeichnung bei Tele- und Mediendiensten	32
4.3	Veröffentlichung personenbezogener Daten in Diskussionsforen im Internet.....	34
4.4	Versendung von Spammails	35
4.5	Unterrichtungspflichten von Diensteanbietern nach dem TDDSG	36
5.	Datenschutz im Gesundheitswesen	37
5.1	Datenschutzgerechte Vernichtung von Patientendaten	37
5.2	Anspruch eines Patienten auf Herausgabe von Unterlagen.....	38
5.3	Welche Fragen darf ein Arzt in einem Anamnesebogen stellen?	39
5.4	Aushändigen von Patientenakten nach Beendigung der Behandlung.....	40
6.	Arbeitnehmerdatenschutz	41
6.1	Erhebung „sensibler Daten“ im Bewerbungsverfahren.....	43
6.2	Veröffentlichung von Arbeitnehmerdaten zu Werbezwecken	45
6.3	Namensschilder auf Arbeitskleidung	46
6.4	Interne Veröffentlichung von Arbeitnehmerdaten	46

6.5	Löschung von Arbeitnehmerdaten nach Beendigung des Arbeitsverhältnisses	47
6.6	Telefondatenerfassung der Mitarbeiter	48
6.7	Beteiligungsrechte eines Betriebsrates	49
7.	Videoüberwachung	50
8.	Datenschutz im Verein	54
9.	Wohnen und Liegenschaften	55
10.	Schlusswort	60

Vorwort

Die Aufsichts- und Dienstleistungsdirektion kann nunmehr im sechsten Jahr nach der Gründung den zweiten Tätigkeitsbericht für den Bereich des Datenschutzes im nicht-öffentlichen Bereich vorlegen.

In dem Tätigkeitsbericht wird anhand von Fallbeispielen ein Überblick über die im Berichtszeitraum von zwei Jahren beantworteten Anfragen und Eingaben gegeben. Die rechtliche Problematik der Fallgestaltungen wurde hervorgehoben, um auch für einen Laien verständlich, interessante und häufig vorkommende datenschutzrechtliche Probleme darzustellen und eine Lösung aufzuzeigen. Bei der täglichen Arbeit der Datenschutzaufsicht spielt die Beratung eine ganz entscheidende Rolle. Zahlreiche Probleme und Konflikte ergeben sich allein aus der Unkenntnis der datenschutzrechtlichen Bestimmungen und der Auswirkungen des eigenen Verhaltens auf die Rechte anderer Personen. Durch Information, Beratung und Unterstützung lassen sich in vielen Fällen datenschutzrechtliche Verstöße vermeiden und ein datenschutzkonformer Umgang mit personenbezogenen Daten herbeiführen. Wichtig bei der Arbeit der Datenschutzaufsicht ist neben der Kontrolle auch die Stärkung der Selbstbestimmung des Bürgers durch Information.

Die Befähigung des Einzelnen, sich selbst zu schützen, ist neben der Begrenzung der Fremdbestimmung durch Dritte ein Aspekt, der zur Verwirklichung des Grundrechts auf informationelle Selbstbestimmung beiträgt.

Trier, im April 2006

Dr. Josef Peter Mertes
Präsident

I. Allgemeiner Teil

1. Zuständigkeit der Aufsichts- und Dienstleistungsdirektion

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

Nach § 1 der Landesverordnung über die Zuständigkeiten nach dem Bundesdatenschutzgesetz (BDSG), dem Teledienstegesetz (TDG) und dem Teledienstedatenschutzgesetz (TDDSG) vom 09.12.2003 ist die Aufsichts- und Dienstleistungsdirektion (ADD) die landesweit zuständige Aufsichtsbehörde über den Datenschutz im nicht-öffentlichen Bereich im Rheinland-Pfalz.

Daneben ist die ADD nach § 2 dieser LVO zuständige Behörde für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 12 TDG und § 9 des TDDSG.

Als obere Landesbehörde ist die ADD gemäß § 2 Abs. 1 Satz 1 des Landesgesetzes zu dem Mediendienste-Staatsvertrag (MDSV) vom 18.07.1997 (GVBI 1997, S. 235), zuletzt geändert durch Gesetz vom 13.04.2005 (GVBI. 2005, S. 63) grundsätzlich auch zuständig für die Überwachung der Einhaltung der Bestimmungen des MDSV sowie für die Verfolgung und Ahndung von Ordnungswidrigkeiten, mit Ausnahme der besonderen Regelungen für den Bereich des Jugendmedienschutzes und die Kontrolle der Beachtung der Datenschutzvorschriften bei öffentlichen Stellen.

Oberste Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich ist das rheinland-pfälzische Ministerium des Innern und für Sport in Mainz.

2. Das Melderegister

Register der meldepflichtigen Verarbeitungen

Die Aufsichtsbehörde führt nach § 38 Abs. 2 BDSG ein Register der nach § 4d BDSG meldepflichtigen automatisierten Verarbeitungen, das von jedermann eingesehen werden kann.

Am 31.05.2005 waren

- 19 Stellen, die nach § 29 BDSG geschäftsmäßig Daten zum Zwecke der Übermittlung speichern (Handels- und Wirtschaftsauskunfteien / Adresshandelsunternehmen) und
- 1 Stelle, die nach § 30 BDSG geschäftsmäßig Daten zum Zwecke der anonymen Übermittlung speichert (Markt- und Meinungsforschungsinstitut)

zum Register gemeldet.

Im Vergleich zum vorherigen Berichtszeitraum hat sich die Anzahl der zum Register gemeldeten Stellen/Verfahren verringert. Ursächlich für diesen Rückgang waren Geschäftsaufgaben im Bereich Auskunfteien bzw. ein Zusammenschluss zweier Auskunfteien.

3. Überprüfungen im Rahmen der Regelaufsicht

Im Berichtszeitraum wurde ein Adresshandelsunternehmen einer datenschutzrechtlichen Kontrolle unterzogen.

Das Adresshandelsunternehmen hat sich auf die Erhebung und den Verkauf von Adressen von Personen spezialisiert, die ein Bauvorhaben planen bzw. bereits realisieren. Verkauft werden die Adressdatensätze überwiegend an Unternehmen aus der Baubranche, gelegentlich aber auch an Finanzdienstleistungs-Unternehmen und Versicherungen.

Gegenstand der vor Ort erfolgten Überprüfungen waren neben einer Besichtigung der Geschäftsräume die in dem Anmeldeformular zu dem von der Aufsichtsbehörde gemäß § 38 BDSG zu führenden Register der nach § 4d BDSG meldepflichtigen Verfahren gemachten Angaben, wie z.B.

- die Fachkunde und Zuverlässigkeit des betrieblichen Datenschutzbeauftragten;
- die Art und Weise der Datenerhebung, -verarbeitung und -übermittlung und
- die technischen und organisatorischen Maßnahmen, die zum Schutz der Datenbestände getroffen wurden.

Die Überprüfung ergab keinen Hinweis auf einen Verstoß gegen datenschutzrechtliche Bestimmungen.

4. Bearbeitung von Eingaben und Beschwerden

Im Berichtszeitraum sind insgesamt 149 Eingaben und Beschwerden bei der Aufsichtsbehörde eingegangen und bearbeitet worden. Gegenüber dem vorangegangenen Berichtszeitraum bedeutet dies eine Zunahme um 25 Prozent. Überwiegend handelte es sich bei den Beschwerdeführern um betroffene Bürgerinnen und Bürger. Beschwerden oder Hinweise auf evtl. Datenschutzverletzungen kamen aber z.B. auch von Unternehmen und Rechtsanwälten. Ebenfalls wurden aufgrund eigener Feststellungen Ermittlungen eingeleitet, wenn der Verdacht bestand, dass gegen datenschutzrechtliche Bestimmungen verstoßen wurde.

Die Beschwerden richteten sich

- in 25 Fällen gegen Anbieter geschäftsmäßiger Tele- und Mediensdienste,
- in 2 Fällen gegen Unternehmen aus Handwerk, Groß- & Einzelhandel,
- in 18 Fällen gegen Finanz- und sonstige Dienstleistungsunternehmen,
- in 12 Fällen gegen Internetanbieter (Provider),
- in 11 Fällen gegen Handels- und Wirtschaftsauskunfteien,
- in 8 Fällen gegen Versicherungen,
- in 7 Fällen gegen Kreditinstitute,
- in 7 Fällen gegen verantwortliche Stellen im Gesundheitswesen,
- in 6 Fällen gegen Videoüberwachung,
- in 6 Fällen gegen Werbe- und Direktmarketingunternehmen,
- in 5 Fällen gegen Vereine,
- in 4 Fällen gegen Unternehmen der Freizeit- und Tourismusbranche,
- in 3 Fällen gegen Freiberufler,
- in 2 Fällen gegen Wohnungsunternehmen / Vermieter,
- in 2 Fällen gegen Arbeitgeber,

- in 2 Fällen gegen Inkasso-Unternehmen,
- in 2 Fällen gegen Personal-Dienstleister,
- in 2 Fällen gegen Privatpersonen,
- in 2 Fällen gegen Zeitungs- und Zeitschriftenverlage,
- in 1 Fall gegen ein Adresshandelsunternehmen
- in 1 Fall gegen eine Gewerkschaft

Etwa 25 % der eingegangenen Beschwerden waren begründet. Die dabei festgestellten formell- oder materiellrechtlichen Verstöße gegen das Bundesdatenschutzgesetz oder andere datenschutzrechtliche Vorschriften bzw. gegen das Teledienstegesetz, das Teledienstedatenschutzgesetz oder den Mediendienste-Staatsvertrag wurden entsprechend beanstandet oder bei schweren Verstößen mit einem Bußgeld geahndet.

Die von den Beschwerdeführern vorgetragene Sachverhalte konnten fast gänzlich auf schriftlichem oder telefonischem Weg mit den verantwortlichen Personen / Stellen aufgeklärt werden. Nur in einigen wenigen Fällen kam es aufgrund der geschilderten Sachverhalte zu angekündigten bzw. unangekündigten Vor-Ort-Kontrollen, um festzustellen, ob tatsächlich ein Verstoß gegen datenschutzrechtliche Bestimmungen vorlag.

So bestand z.B. ein Beschwerdeführer auf einer Vor-Ort-Kontrolle einer von seinem Nachbarn installierten Videoüberwachungsanlage, mit dem dieser nicht nur den vor und hinter seinem Anwesen verlaufenden öffentlichen Verkehrsraum, sondern auch ihn, den Beschwerdeführer, überwache. Bei der daraufhin durchgeführten Vor-Ort-Kontrolle stellte sich heraus, dass der betroffene Nachbar die Videokamera als Teil einer Alarmanlage zum Schutz seiner im Schaufenster des Ausstellungsraumes ausgestellten Gemälde und Skulpturen hatte installieren lassen. Aufgrund des Neigungswinkels der Kamera wurde dabei zwangsläufig ein Teil des vor dem Schaufenster befindlichen Gehweges erfasst. Die Kamera war jedoch so ausgerichtet, dass nur die Beine einer direkt vor dem Schaufenster vorbeigehenden erwachsenen Person auf dem Moni-

tor zu sehen waren. Da es sich bei dem Ausstellungsraum um einen für kunstinteressierte Besucher offenstehenden und damit um einen öffentlich zugänglichen Raum handelte, war die Überwachung des Schaufensters nach § 6b BDSG zulässig. Ein außen am Schaufenster aufgebrachter Aufkleber wies zudem auf die Videoüberwachung hin.

Des Weiteren war die Anfrage einer Mitarbeiterin eines Call-Centers zum Anlass genommen worden, dieses Unternehmen unangekündigt aufzusuchen und einer Überprüfung zu unterziehen. Die Mitarbeiterin wandte sich an die Aufsichtsbehörde, um zu erfahren, ob sie sich strafbar mache, wenn sie unter dem Vorwand einer „Umfrage zum aktuellen Jahressteuergesetz“ Telefonbücher „abtelefonieren“ und am Ende eines jeden Gespräches die angerufenen Personen konkret um deren Einverständnis für weitere Anrufe fragen müsse. Für jeden vollständig ausgefüllten standardisierten Fragebogen und erteilte Einverständniserklärung zahle ihr Arbeitgeber ihr eine Prämie.

Die von der Petentin gemachten Angaben bestätigten sich bei dieser Vor-Ort-Kontrolle. In den Büroräumen fanden sich – nach Bundesländern geordnet – mehrere Stapel neuer Telefonbücher und der besagte Fragebogen. Da die Mitarbeiterinnen nur stundenweise ab dem späten Nachmittag arbeiteten, waren diese zum Zeitpunkt der Kontrolle nicht anwesend und konnten daher auch nicht dazu befragt werden. Der verwendete Fragebogen ließ den Schluss zu, dass das Abtelefonieren der Telefonbücher lediglich zur Gewinnung selektierter Adressen (Personen nicht älter als 55 Jahre, verheiratet, nicht selbständig, nicht in der Versicherungsbranche tätig) erfolgte und es sich um eine wettbewerbsrechtlich unzulässige Kaltaquise handelte. Der Inhaber des Call-Centers bestritt dies und teilte mit, für einen Auftraggeber Telefonmarketing betrieben zu haben. Die Telefonbücher habe er zur Aktualisierung der zu diesem Zweck überlassenen Kundenadressen gebraucht. Nachweise, die seine Angaben belegt hätten, konnte er allerdings nicht vorlegen.

Der Inhaber konnte letztlich unter deutlichem Hinweis auf die wettbewerbs- und datenschutzrechtlichen Bestimmungen (vorherige Einwilligung der betroffenen Personen für diese Anrufe fehlte und konnte aus überzeugenden Gründen auch nicht unterstellt werden) und der Ankündigung weiterer unangemeldeter Vor-Ort-Kontrollen von der Unzulässigkeit seines Handels überzeugt werden.

Daneben wurden noch 12 aus dem vorherigen Berichtszeitraum stammende Eingaben und Beschwerden abschließend bearbeitet. Die teilweise lange Bearbeitungsdauer war z.B. durch vollstreckungshemmende Maßnahmen seitens der Betroffenen (Herbeiführung einer gerichtlichen Entscheidung über Anträge auf Wiedereinsetzung in den vorherigen Stand) bedingt.

5. Bearbeitung von Anfragen / Beratungersuchen

Die Beantwortung telefonischer und schriftlicher Anfragen zu datenschutzrechtlichen Problemstellungen hat im Berichtszeitraum deutlich an Bedeutung und Umfang zugenommen.

So wurden insgesamt 49 schriftliche und 128 telefonische Anfragen / Beratungersuchen von Bürgerinnen und Bürgern, betrieblichen Datenschutzbeauftragten, Gewerbetreibenden, Unternehmern, Vereinen, usw. beantwortet. Während bei der Zahl der schriftlichen Anfragen gegenüber dem vorherigen Berichtszeitraum ein Rückgang zu verzeichnen war, stieg die Anzahl der telefonischen Anfragen / Beratungersuchen um etwas mehr als 100 Prozent.

Die Anfragen betrafen dabei überwiegend folgende Themenbereiche:

- Betrieblicher Datenschutzbeauftragter
- Meldepflicht nach § 4d BDSG
- Arbeitnehmerdatenschutz

- Handels- und Wirtschaftsauskunfteien
- Videoüberwachung
- Anbieterkennzeichnung bei Tele- und Mediendiensten
- Veröffentlichung personenbezogener Daten im Internet

Einen Schwerpunkt bildeten dabei die Anfragen „verunsicherter“ Inhaber kleinerer oder mittlerer Unternehmen und Angehöriger freier Berufe zur Erforderlichkeit der Bestellung eines Beauftragten für den Datenschutz. Der Anlass dieser Anfragen war stets der Gleiche: Ein Datenschutz-Berater oder Seminaranbieter unterrichtete die Betroffenen über die gemäß § 45 BDSG am 22.05.2004 auslaufende Übergangsfrist und deren Verpflichtung, bis zu diesem Zeitpunkt – soweit noch nicht geschehen – einen Beauftragten für den Datenschutz zu bestellen. Unter Hinweis auf mögliche Sanktionen im Falle einer Überprüfung durch die Aufsichtsbehörde wurde den Betroffenen dann die Dienstleistung „Externer Datenschutzbeauftragter“ bzw. die Teilnahme an Seminaren zum Thema Datenschutz angeboten.

Die Anrufer wurden darüber informiert, dass es sich bei der Pflicht zur Bestellung eines Beauftragten für den Datenschutz gerade nicht um ein Verfahren i.S.v. § 45 des am 23.05.2001 in Kraft getretenen novellierten BDSG handelt und damit nicht unter diese Übergangsfrist fällt. Nach dieser damals neu aufgenommenen Regelung sind Erhebungen, Verarbeitungen und Nutzungen personenbezogener Daten (sog. Verfahren), die am 23.05.2001 bereits begonnen haben, binnen drei Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen. Die Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz hingegen besteht bereits seit dem Inkrafttreten des BDSG im Jahre 1977. Mit den seit damals vorgenommenen Gesetzesänderungen wurde jeweils die Position des Beauftragten für den Datenschutz weiterhin verstärkt.

Im Verlauf der Gespräche mit den Betroffenen offenbarte sich bei vielen die Unkenntnis darüber, wann ein Beauftragter für den Datenschutz

überhaupt zu bestellen ist und wer zum Beauftragten für den Datenschutz bestellt werden darf.

6. Ordnungswidrigkeiten

6.1 Berichtszeitraum 2003 – 2005

Im Berichtszeitraum hat die ADD wegen festgestellter Verstöße gegen datenschutzrechtliche Bestimmungen insgesamt sieben Verfahren nach dem Gesetz über Ordnungswidrigkeit (OWiG) gegen die verantwortlichen Personen eingeleitet.

Die von den Betroffenen begangenen bzw. zu verantwortenden Ordnungswidrigkeiten wurden jeweils mit einem Bußgeld geahndet. Im Einzelnen wurden

- in drei Fällen ein Verstoß gegen § 43 Abs. 1 Nr. 10 BDSG (Auskunftspflicht),
- in einem Fall ein Verstoß gegen § 43 Abs. 2 Nr. 1 BDSG (unbefugte Verarbeitung personenbezogener Daten, die nicht allgemein zugänglich sind),
- in einem Fall ein Verstoß gegen § 43 Abs. 2 Nr. 3 BDSG (unbefugter Abruf personenbezogener Daten, die nicht allgemein zugänglich sind) und
- in zwei Fällen ein Verstoß gegen § 43 Abs. 2 Nr. 4 BDSG (Erschleichung personenbezogener Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben)

festgestellt. Die Höhe der verhängten Bußgelder betrug zwischen 300,- und 2.500,- Euro und bewegte sich damit deutlich am unteren Ende des vom Gesetzgeber vorgesehenen Bußgeldrahmens.

Vier Bußgeldbescheide wurden rechtskräftig, da die Betroffenen keine Rechtsmittel dagegen einlegten; die Bußgelder wurden – bis in einem Fall – unmittelbar nach Eintritt der Rechtskraft gezahlt.

Die verbliebenen drei Ordnungswidrigkeitsverfahren wurden dem zuständigen Amtsgericht zur Entscheidung vorgelegt, nachdem den Einsprüchen der Betroffenen gegen die Bußgeldbescheide nicht abgeholfen wurde.

Dabei bestätigte das Amtsgericht in einem Verfahren die Rechtsauffassung der Aufsichtsbehörde, verringerte aber die Höhe des Bußgeldes; in dem zweiten Verfahren nahm der Betroffene seinen Einspruch vor der Hauptverhandlung zurück, so dass der Bußgeldbescheid ebenfalls rechtskräftig wurde. Das dritte Verfahren war bis zum Ende des Berichtszeitraums noch nicht terminiert.

6.2 Ordnungswidrigkeitsverfahren aus dem Berichtszeitraum 2001 - 2003

Im laufenden Berichtszeitraum hatte das Amtsgericht über drei noch aus dem vorangegangenen Berichtszeitraum anhängige Verfahren entschieden:

Dabei schloss sich das Amtsgericht in einem Verfahren der Entscheidung der Aufsichtsbehörde an, verringerte jedoch aufgrund einer nachträglich eingetretenen schlechten finanziellen Leistungsfähigkeit des Betroffenen die Höhe des ursprünglich festgesetzten Bußgeldes. Die Entscheidung des Amtsgerichts wurde rechtskräftig.

Das zweite Verfahren erledigte sich aufgrund der Rücknahme des Einspruches durch den Betroffenen vor der Hauptverhandlung.

In dem dritten Verfahren folgte das Gericht nicht der Auffassung der Aufsichtsbehörde und stellte das Verfahren ein, weil es eine Ahndung des Verstoßes nicht für geboten hielt.

7. Workshop der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich

Neben dem regelmäßig tagenden „Düsseldorfer Kreis,“ dem Gremium der obersten Datenschutzaufsichtsbehörden, treffen sich einmal jährlich Mitarbeiter der Datenschutz-Aufsichtsbehörden der Länder, um eine bundesweit einheitliche Vorgehensweise bei der Umsetzung / Anwendung datenschutzrechtlicher Bestimmungen abzustimmen bzw. konkrete auftretende Probleme bei der täglichen Arbeit zu besprechen.

In den Jahren 2003 und 2004 nahmen Mitarbeiter der Aufsichtsbehörde an den in Ansbach und Bremen ausgerichteten Workshops teil.

Gastgeber des im September 2005 stattfindenden 11. Workshops war die ADD .

II. Einzelfälle aus der Praxis der Aufsichtsbehörde

1. Handel /Auskunfteien

1.1 Erhebung personenbezogener Daten bei Umtausch / Reklamation von Waren

Ein Petent beschwerte sich darüber, dass er bei der Rückgabe gekaufter Ware in einer Filiale eines Schuhdiscounters aufgefordert wurde, seine vollständige Adresse auf dem Rückgabebeleg (nicht-automatisierte Datei i.S.v. § 1 Abs.2 BDSG) anzugeben und mit seiner Unterschrift die ordnungsgemäße Erstattung des Kaufpreises zu bestätigen.

Nach eingehender Prüfung des von dem Unternehmen bei Umtausch und Reklamationen praktizierten Verfahrens wurde keine unzulässige Datenerhebung / -verarbeitung festgestellt. Das Unternehmen hat gemäß § 28 Abs.1 Nr.2 BDSG ein berechtigtes Interesse an der Erhebung dieser Daten, das nach erfolgter Abwägung höher zu gewichten ist als die schutzwürdigen Interessen des Kunden. Nach Mitteilung des Unternehmens wird den Kunden bei Umtausch oder Reklamation gekaufter Ware (auch ohne gültigen Kassenbon) ohne jegliche weitere Prüfung oder Bewertung eines Anspruches der Kaufpreis in bar zurückerstattet. Dabei handelt es sich um einen Service, der besondere Vorkehrungen erfordert, um

- a) im Rahmen einer ordnungsgemäßen Buchführung belegen zu können, dass der Kunde für die zurückgegebene Ware den Kaufpreis erstattet bekommen hat,
- b) bei mehreren hundert Filialen einen evtl. Missbrauch (z.B. die Unterschlagung von Geld durch Mitarbeiter) zu verhindern oder eine begangene Unterschlagung vor Gericht nachweisen zu können.

Es war ebenfalls nicht zu beanstanden, dass die Buchungsbelege bis zum Ablauf der gesetzlichen Aufbewahrungsfristen nach dem HGB bzw. der AO in der jeweiligen Filiale verbleiben.

1.2 Verkauf einer gebrauchten Festplatte

Ein Beschwerdeführer hatte in einer Filiale einer Elektromarktes ein neues Laptop gekauft. Nachdem das Gerät nicht ordnungsgemäß funktionierte, wurden mehrere Komponenten, darunter die Festplatte, in der Filiale getauscht. Als der Petent sein Laptop zurückerhielt, sicherte ihm der Mitarbeiter auf seine ausdrückliche Nachfrage hin zu, dass im Rahmen des Tausches der Festplatte die auf der „alten“ Festplatte gespeicherten Daten (Versicherungsprogramme, Angebote und Kundendaten) rückstandslos gelöscht werden. Dazu sollte die Festplatte über den zentralen internen Service an eine Fremdfirma geschickt werden. Mehrere Monate später erhielt der Beschwerdeführer einen Anruf einer ihm unbekannt Person, die in der gleichen Filiale ein neues Laptop gekauft und dann aufgrund mangelnder Speicherkapazität bei einer Durchsuchung der Festplatte noch die Daten des Petenten gefunden hatte. Der Petent zeigte diesen Vorfall umgehend der Aufsichtsbehörde an.

Das Unternehmen wurde angeschrieben und um Abgabe einer Stellungnahme gebeten. Nach Mitteilung der Geschäftsleitung war die Festplatte durch eine „unglückliche Verkettung von Ereignissen“ nicht vom hausinternen Service zur Löschung an eine Fremdfirma geschickt, sondern in ein neues Laptop eingebaut worden. Es habe aber nicht mehr nachvollzogen werden können, welcher Mitarbeiter dafür verantwortlich war.

Mit dem Einbau der gebrauchten Festplatte in das neue Laptop wurde gegen § 43 Abs. 2 Nr. 1 BDSG verstoßen. Nachdem der Geschäftsleitung das Ergebnis der datenschutzrechtlichen Überprüfung mitgeteilt wurde, vertrat diese daraufhin die Auffassung, dass der Mitarbeiter, der

die Festplatte austauschte, letztendlich die Verantwortung dafür tragen und zur Rechenschaft gezogen werden sollte.

Das eingeleitete Ordnungswidrigkeitsverfahren musste eingestellt werden, da die Verantwortlichkeit des Mitarbeiters, der die Festplatte austauschte, mit der ordnungsgemäßen Weiterleitung an den hausinternen Service endete und der tatsächlich verantwortliche Mitarbeiter nicht festgestellt werden konnte.

1.3 Werbeaktion eines Verlages

Mehrere Schulen wandten sich im Berichtszeitraum an die ADD, um die Verletzung datenschutzrechtlicher Bestimmungen durch eine Vertriebs-Gesellschaft zu rügen. Diese Gesellschaft war von der Tochtergesellschaft eines Buchverlages durch einen Dienstleistungsvertrag mit der Gewinnung von Interessentendaten für die Produkte des Verlages beauftragt worden.

Im Rahmen dieses Auftrages sandte die Gesellschaft ein Informationsschreiben an verschiedene Schulen, dem Gutscheine einer Buch-Geschenkaktion beigelegt waren. Die Gutscheine sollten von den Schülern und gegebenenfalls den Erziehungsberechtigten ausgefüllt von der Schulleitung wieder an die Gesellschaft zurückgesandt werden. Dem Inhalt des Informationsschreibens zufolge sollte der Buchverlag etwa eine Woche nach Rücksendung der Gutscheine die Buchgeschenke an die Schule ausliefern. Es wurde darauf hingewiesen, dass dieses Ablaufsystem einen möglichst geringen Arbeitsaufwand für die Schule und dem Verlag die schnellstmögliche Auslieferung garantiere. Die Gesellschaft, die auch die Auslieferung vornehme, stehe für Rückfragen zur Verfügung. Es wurde versichert, dass die für die EDV-Erfassung und als Kostennachweis erhaltenen Adressen und Daten nicht an Dritte weitergegeben und nach Beendigung der Geschenkaktion nicht mehr verwendet würden.

Statt der versprochenen Bücher erhielten die Schüler bzw. die Eltern jedoch wiederholt Anrufe oder sogar Hausbesuche von Vertretern, die den Zweck hatten, die Eltern zum Kauf eines mehrbändigen Lexikons zu bewegen. Die Schulleitung der Schulen sah in der zweckentfremdeten Nutzung der erhobenen Adressen einen Verstoß gegen datenschutzrechtliche Bestimmungen.

Die Überprüfung des Sachverhalts ergab, dass die Vertriebs-Gesellschaft die Adresdaten trotz der Versicherung, dass eine Weitergabe nicht erfolge, an die o.g. Tochtergesellschaft des Verlages weitergegeben hatte, deren Geschäftszweck das Verlegen und der Vertrieb von Medienprodukten ist.

Da die für die Datenerhebung verwandten Gutscheine keinen Hinweis auf die Weitergabe und anschließende Nutzung durch die Tochtergesellschaft des Buchverlages enthielt, war die Datenweitergabe in diesem Fall rechtswidrig und verstieß gegen Artikel 6 Abs. 1 der Richtlinie EG 95/46 EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, wonach die Mitgliedsstaaten vorsehen, dass personenbezogene Daten nach Treu und Glauben verarbeitet werden.

Des weiteren verstieß die Weitergabe der personenbezogenen Daten gegen § 28 Abs. 1 Nr. 2 BDSG. Nach dieser Vorschrift ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Dem berechtigten Interesse der Tochtergesellschaft an der Gewinnung neuer Kunden stand vorliegend das schutzwürdige Interesse der betroffenen Schüler und Eltern entgegen, da davon auszugehen ist, dass sich viele nicht an der Aktion

beteiligt hätten, wenn sie vorher über die Weitergabe der erhobenen Daten informiert gewesen wären. Die Vertriebs-Gesellschaft wurde auf die Rechtslage hingewiesen.

Die Vertriebs-Gesellschaft weist nunmehr in ihren Gutscheinen ausdrücklich auf die weitere Nutzung der Daten hin, so dass eine ausreichende Information der Betroffenen über die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung der Daten sichergestellt ist. Den Betroffenen obliegt damit selbst die Entscheidung, ob sie sich – in Kenntnis der weiteren Nutzung der Daten - an diesen Werbeaktionen beteiligen.

1.4 Kundendatenschutz

Eine Kundin einer Supermarktkette fragte an, ob Privatfirmen autorisiert seien, biometrische Daten von Bürgern zu erheben und zu speichern.

In dem betreffenden Fall wird den Kunden eines Supermarktes neuerdings die Möglichkeit angeboten, die eingekauften Waren mittels eines biometrischen Bezahlverfahrens (Fingerabdruckverfahren) bezahlen zu können. Dabei liegt es in der Entscheidung eines jeden Kunden selbst, ob er von diesem neuen Bezahlverfahren macht oder weiterhin an den vorhandenen herkömmlichen Kassen seine Waren bezahlt.

Entscheidet er sich für dieses neue Bezahlverfahren, ist die schriftliche Einwilligung des Kunden die Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten (§§ 4, 28 BDSG). Voraussetzung für die Wirksamkeit dieser Einwilligung ist eine umfassende Information der Kunden nicht nur über das Lastschriftverfahren, sondern auch über Art und Umfang der Verarbeitung der Fingerabdruckdaten.

Das Verfahren an sich wurde bereits von der zuständigen Aufsichtsbehörde, dem Innenministerium Baden-Württemberg, datenschutzrechtlich

geprüft und unter der Voraussetzung, dass es auf der Grundlage einer Einwilligung eingesetzt wird, für zulässig erachtet.

2. Datenschutz bei Banken

Die Bearbeitung der im Berichtszeitraum eingegangenen Beschwerden über den Umgang mit personenbezogenen Daten bei Banken zeigte auf, dass die Banken die Bestimmungen des Bundesdatenschutzgesetzes konsequent einhalten und umsetzen. Dennoch besteht trotz aller Schulungsmaßnahmen und erlassener Richtlinien / Arbeitsanweisungen die Gefahr, dass sich bei den Mitarbeitern im Arbeitsalltag eine gewisse Routine einschleicht und damit die Sensibilität im Umgang mit personenbezogenen Daten nachlässt. Die nachfolgenden Beispiele belegen diese Feststellungen:

2.1 Zugriff eines selbständigen Finanzberaters auf Kontodaten einer Bankkundin

Wie weit reichen die Zugriffsrechte selbständiger Finanzberater auf Kunden- und Kontodaten? Mit dieser Frage wandte sich die Kundin einer Bank an die Aufsichtsbehörde, nachdem sie einer Einladung eines selbständigen Finanzberaters zu einem Informationsgespräch in die Geschäftsräume ihrer Hausbank gefolgt war.

Die von dem Finanzberater vorab telefonisch angekündigte Information über wichtige gesetzliche Änderungen stellte sich gleich zu Beginn des Gespräches als Angebot für eine private Altersvorsorge heraus. Im Verlauf dieses Gespräches legte ihr der Finanzberater einen Computerausdruck vor, auf dem neben ihrem aktuellen Kontostand zusätzliche handschriftliche Informationen über bestehende Versicherungen und mtl. Beiträge vermerkt waren, die Überweisungen und Lastschriften entnommen worden waren.

Bei der Ermittlung des Sachverhaltes stellte sich heraus, dass der ausschließlich für diese Bank tätige selbständige Finanzberater zur Vorbereitung des Kundengesprächs aufgrund der ihm von der Bank eingeräumten Zugriffsberechtigung online die Kunden- und Kontodaten der Petentin abgerufen hatte.

Nach § 4 Abs. 1 BDSG sind die Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Da zum Zeitpunkt des Online-Abrufes der Daten weder die erforderliche Einwilligung der Betroffenen vorlag und bereichsspezifische Datenschutzvorschriften ebenfalls nicht erkennbar waren, wäre als gesetzliche Grundlage für den erfolgten Abruf der Kontodaten allenfalls § 28 Abs. 1 Satz 1 BDSG in Betracht gekommen. Diese Vorschrift setzt jedoch voraus, dass zwischen den Parteien zum Zeitpunkt des Online-Abrufes ein Vertragsverhältnis oder vertragsähnliches Vertrauensverhältnis bestand, was vorliegend aber nicht der Fall war.

Als Ergebnis der datenschutzrechtlichen Prüfung stand fest, dass der Finanzberater unbefugt personenbezogene Daten der Petentin, die nicht allgemein zugänglich sind, abgerufen und damit eine Ordnungswidrigkeit i.S.v. § 43 Abs. 2 Nr. 3 BDSG begangen hatte. Die Ordnungswidrigkeit wurde mit einem entsprechenden Bußgeld geahndet.

Die Bank traf im vorliegenden Fall kein Organisationsverschulden. Die Geschäftsleitung nahm den Vorfall jedoch zum Anlass, alle Mitarbeiter und Finanzberater noch einmal eindringlich auf die strikte Einhaltung der vorgesehenen Prozesse und Anweisungen hinzuweisen.

2.2 Bekanntgabe von Kontodaten durch eine Bankangestellte an einen Dritten

Ein Beschwerdeführer hatte im Rahmen einer geplanten Investition mit seiner Hausbank über eine mögliche Finanzierung verhandelt. Seine Kundenberaterin legte ihm während des Gespräches eine Übersicht (ausgedruckte Hardcopy) über seine dort geführten Konten mit den aktuellen Kontoständen vor. In dieser Übersicht war auch der aktuelle Kontostand eines Gemeinschaftskontos ausgewiesen, welches der Petent mit zwei weiteren Personen zu diesem Zeitpunkt dort führte.

Zusätzlich – und für den Beschwerdeführer unerklärlich – enthielt die Übersicht neben den vollständigen Informationen über die Konten eines Mitinhabers dieses Gemeinschaftskontos auch weitere Informationen über dessen Angehörige. Nachdem der Petent seine Kundenberaterin auf diesen Missstand hingewiesen hatte, trennte sie den ihn nicht betreffenden Teil von der Hardcopy ab und betrachtete die Angelegenheit damit als erledigt. Der Petent wandte sich daraufhin an den betrieblichen Datenschutzbeauftragten der Bank, der ihm „als sicherste Lösung dieses Problems“ empfahl, das Gemeinschaftskonto aufzulösen. Da der Petent mit dieser Antwort nicht einverstanden war, wandte er sich mit der Bitte um Prüfung dieses Vorganges an die Aufsichtsbehörde.

Die datenschutzrechtliche Überprüfung des Sachverhaltes ergab, dass die Kundenberaterin dem Petenten anstelle einer Übersicht über dessen Einzelengagements eine Übersicht über sein Gesamtengagement vorgelegt hatte. Nach Mitteilung der Geschäftsführung beinhaltet die Darstellung des Gesamtengagements die auf den Namen eines Kunden lautenden Konten und gegebenenfalls weitere Konten, bei denen er Mitinhaber ist, sowie möglicher Weise weitere Konten von Mitverpflichteten, zum Beispiel aus einem Kreditengagement. Diese Zusammenfassung basiert auf § 19 Abs. 2 des Kreditwesengesetzes und ist daher, sofern sie nur bankintern verwendet wird, datenschutzrechtlich nicht zu beanstanden.

Die Kundenberaterin hatte die in dem Gesamtengagement enthaltenen Informationen jedoch entgegen den bestehenden bankinternen Arbeitsanweisungen an den Petenten weitergegeben und damit unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, übermittelt. Der festgestellte Verstoß gegen § 43 Abs. 2 Nr. 1 BDSG wurde mit einem entsprechenden Bußgeld geahndet.

2.3 Erteilung eines Suchauftrages an die SCHUFA

Eine Volksbank hatte aufgrund eines nicht zustande gekommenen Kreditgeschäftes mehrere titulierte Kostenfestsetzungsbeschlüsse gegen einen Schuldner erwirkt, die aber durch die ständig wechselnden Aufenthaltsorte des Schuldners über einen längeren Zeitraum nicht vollstreckt werden konnten. Daraufhin hatte die Bank in 1992 der SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung) einen Suchauftrag erteilt. Von Seiten der SCHUFA erfolgten danach zur Aktualisierung des Suchauftrages regelmäßig Anfragen an die Bank. Im Rahmen der Beantwortung dieser Anfragen teilte die Volksbank der SCHUFA jeweils die aktuelle Höhe der Ansprüche aus den titulierten Kostenfestsetzungsbeschlüssen mit.

Der Petent erhielt seinen Angaben zufolge erstmals im Berichtszeitraum Kenntnis über den von der Volksbank erteilten Suchauftrag und beschwerte sich bei der Aufsichtsbehörde über eine unzulässige Übermittlung personenbezogener Daten, durch die ihm ein Vermögensschaden entstanden sei. Die Volksbank habe den Suchauftrag erteilt, ohne im Besitz einer von ihm unterzeichneten SCHUFA-Klausel gewesen zu sein.

Im vorliegenden Fall hatte die Bank mit der Erteilung des Suchauftrages und der späteren regelmäßigen Übermittlung der gegen den Schuldner bestehenden Ansprüche keine unzulässige Datenübermittlung vorgenommen. Die Rechtmäßigkeit der Datenübermittlung ergab sich aufgrund des damals nicht zustande gekommenen Kreditgeschäftes aus §

28 Abs. 1 Satz 1 Nr. 2 BDSG. Die Abwägung der vom Beschwerdeführer geltend gemachten schutzwürdigen Interessen an dem Ausschluss der Übermittlung seiner Daten an die SCHUFA gegen die berechtigten Interessen der Bank an der Beitreibung der real existierenden Forderungen ergab eine Entscheidung zugunsten der Bank.

Zudem bedurfte es für die Erteilung des Suchauftrages keiner vom Petenten unterzeichneten SCHUFA-Klausel: Das Suchauftragsverfahren ist ein selbständiges Beauskunftungsangebot der SCHUFA und wird unabhängig von den übrigen Verfahren betrieben. Der Erteilung eines Suchauftrages an die SCHUFA muss daher kein Einmeldevorgang und somit keine Unterzeichnung der SCHUFA-Klausel seitens des Betroffenen vorangegangen sein. Titulierte Kostenforderungen können ebenso wie ein Kredit selbst angemeldet werden, auch wenn ein Kreditgeschäft letztlich nicht zustande gekommen ist, damit aber das Kreditrisiko, das vom Verursacher der Kosten ausgeht, abgebildet wird. Insoweit soll der Verursacher von Kreditgeschäftskosten hinsichtlich der Beurteilung der Zahlungswilligkeit bzw. Zahlungsfähigkeit nicht besser gestellt sein, als der Schuldner, der das Kreditgeschäft selbst nicht ordnungsgemäß abwickelt.

3. Versicherungen

3.1 Notruf der Autoversicherer

Nach § 8 des Gesetzes über die Pflichtversicherung für Kraftfahrzeughalter (Pflichtversicherungsgesetz) haben Versicherungsunternehmen, denen im Inland die Erlaubnis zum Betrieb der Kraftfahrzeug-Haftpflichtversicherung für Kraftfahrzeuge und Anhänger erteilt wurde, eine Auskunftsstelle einzurichten, die Geschädigten unter gewissen Voraussetzungen auf Anforderung Angaben übermittelt, die zur Geltendmachung von Schadensersatzansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr erforderlich sind. Die Aufgaben und

Befugnisse wurden vom Gesetzgeber der GDV Dienstleistungs-GmbH & Co. KG – Zentralruf der Autoversicherer – in Hamburg übertragen.

Der Zentralruf der Autoversicherer erteilt somit Opfern von Verkehrsunfällen und deren Rechtsvertretern oder Rechtsnachfolgern nach Angabe des amtlichen Kennzeichen des Unfallgegners und des Unfalldatums Auskunft darüber,

- bei welchem Versicherungsunternehmen am Schadentag Versicherungsschutz für das angegebene Fahrzeug bestand,
- die Nummer des für den Fahrzeughalter abgeschlossenen Versicherungsvertrags und
- unter welcher Anschrift die für die Schadenbearbeitung des Verkehrsunfalls zuständige Stelle des Versicherungsunternehmens zu erreichen ist.

Ein Hauseigentümer hatte von seinem Nachbarn erfahren, dass eine fremde Person sein Grundstück während seiner Abwesenheit betreten und sein Haus (ein ehemaliges altes Bahnhofsgebäude) fotografiert hatte. Der Nachbar hatte sich das Kennzeichen des PKW, mit dem die unbekannte Person davon fuhr, notiert und dem Hauseigentümer übergeben. Der Hauseigentümer erstattete daraufhin umgehend Strafanzeige wegen Hausfriedensbruchs bei der Polizei. Im Rahmen der Anzeigenaufnahme wurde er befragt, ob er die dann namentlich genannte Person kenne. Dies verneinte er wahrheitsgemäß.

Wieder zuhause fasste der Hauseigentümer den Entschluss, selbst tätig zu werden, um eine evtl. von dem Fahrzeughalter geplante Straftat zu verhindern. Dazu wollte er sich mit dem Fahrzeughalter in Verbindung setzen. Da ihm dessen Anschrift aber nicht bekannt war, rief er beim „Zentralruf der Autoversicherer“ an und teilte dort mit, in einen Verkehrsunfall mit dem betreffenden Fahrzeug verwickelt gewesen zu sein. Personen seien bei dem Unfall aber nicht zu Schaden gekommen. Der Mitarbeiter des Zentralrufs der Autoversicherer teilte ihm, nachdem er

sich Ort und Zeitpunkt des angeblichen Unfalles notiert hatte, lediglich die o.a. Daten, nicht aber die Anschrift des Fahrzeughalters mit.

Nachdem der Zentralruf der Autoversicherer erfuh, dass der von dem Hauseigentümer geschilderte Schadensfall in Wirklichkeit nicht eingetreten war, erstattete die GDV Dienstleistungs-GmbH & Co. KG Strafanzeige gegen den Betroffenen wegen der Erschleichung personenbezogener Daten durch unrichtige Angaben. Der Vorgang wurde an die ADD als zuständige Aufsichtsbehörde abgegeben. Der Betroffene gab im Rahmen des gegen ihn eingeleiteten Ordnungswidrigkeitsverfahrens den missbräuchlichen Anruf beim Zentralruf der Autoversicherer und damit den ihm vorgeworfenen Verstoß gegen § 43 Abs. 2 Nr. 4 BDSG zu. Danach handelt ordnungswidrig, wer vorsätzlich oder fahrlässig die Übermittlung personenbezogener Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht.

Bei den vom Zentralruf der Autoversicherer gespeicherten Daten handelt es sich um personenbezogene Daten i.S.v. § 3 Abs. 1 BDSG, mithin um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer Person, die nicht allgemein zugänglich sind. Die Auskunftserteilung ist von der Geltendmachung eines berechtigten Interesses der anfragenden Stelle abhängig (vgl. Urteil des BGH v. 08.10.2002 – 1 StR 150/02 – ; danach sind Fahrzeug- und Halterdaten, die im Rahmen einer einfachen Registerrückmeldung nach § 39 StVG übermittelt werden, nicht offenkundig und fallen damit unter den Schutz des § 203 Abs. 2 Satz 2 StGB).

Die Ordnungswidrigkeit wurde mit einem Bußgeld geahndet. Inzwischen hat das zuständige Amtsgericht den Bußgeldbescheid unter Herabsetzung des Bußgeldes von 2.500,- auf 1.250,- Euro bestätigt. Das Gericht sah es – entgegen der Auffassung der Aufsichtsbehörde – nicht als erwiesen an, dass der Anruf des Betroffenen beim Zentralruf der Autoversicherer vorsätzlich erfolgte und ging bei der Bemessung der Geldbuße von Fahrlässigkeit aus.

Im Übrigen stellte sich heraus, dass es sich bei dem Fahrzeughalter nur um einen Hobbyfotografen und Eisenbahnfan handelte, der alte Bahnhofsgebäude für eigene Zwecke fotografiert. Das Verfahren gegen ihn wegen Hausfriedensbruch wurde eingestellt.

3.2 Was dürfen Versicherungsunternehmen wie lange speichern?

Ein Petent hatte bei einem Versicherungsunternehmen eine Krankenhaustagegeldversicherung abgeschlossen. Zur Klärung einer Versicherungsleistung hatte der Petent der Versicherung zwei medizinische Gutachten übersandt, die er – nachdem sein Antrag auf Krankenhaustagegeld abschlägig beschieden worden war – gelöscht wissen wollte. Das Versicherungsunternehmen hatte die Gutachten aufgrund bestehender gesetzlicher Aufbewahrungspflichten jedoch nur gesperrt und dies dem Petenten unter Nennung der Rechtsgrundlagen, die der geforderten Löschung entgegenstanden, mitgeteilt. Der Petent wandte sich daraufhin an die Aufsichtsbehörde und bat um Unterstützung bei der Durchsetzung seiner Forderung auf Löschung der von ihm eingereichten und elektronisch archivierten ärztlichen Gutachten.

Im vorliegenden Fall blieb die Eingabe des Petenten jedoch erfolglos:

Nach § 35 Abs. 2 BDSG können personenbezogene Daten jederzeit gelöscht werden, es sei denn, der Löschung stehen gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegen. Vorliegend war das Versicherungsunternehmen verpflichtet, die ihr im Rahmen der Bearbeitung des Leistungsantrages bekannt gewordenen personenbezogenen Daten gemäß § 257 Handelsgesetzbuch (HGB) bzw. § 47 der Abgabenordnung (AO) für die Dauer von sechs Jahren aufzubewahren. Im Falle einer vorzeitigen Löschung hätte sich das Versicherungsunternehmen wegen Missachtung der gesetzlichen Aufbewahrungsfristen strafbar gemacht. Die anstelle der Löschung erfolgte Sperrung der archivierten Daten war datenschutzrechtlich ebenfalls nicht zu beanstanden.

4. Internet

4.1 Datenschutzrechtliche Zulässigkeit von Altersverifikationssystemen

Mehrere Eingaben betrafen ein von einem Diensteanbieter betriebenes Altersverifikationssystem (AVS), das eine Vielzahl von Anbietern ihren jugendgefährdenden Angeboten vorgeschaltet hatten. Nach den Bestimmungen des Jugendmedien-Staatsvertrages dürfen jugendgefährdende Inhalte nur dann angeboten werden, wenn sichergestellt ist, dass diese Inhalte nur Erwachsenen zugänglich gemacht werden.

Da der interessierte Nutzer im Rahmen der Altersverifikation neben seiner Personalausweisnummer u.a. auch seine Bankverbindung mit Kontonummer und Bankleitzahl bekannt geben muss, baten die Petenten um Prüfung, ob der Direktabgleich ihrer Daten mit Datenbanken Dritter (z.B. von Banken oder Auskunftsteilen) datenschutzrechtlich zulässig ist und ob gleichzeitig eine Bonitätsprüfung erfolgt.

Im vorliegenden Fall wurde das Altersverifikationssystem von der Freiwilligen Selbstkontrolle Multimedia Diensteanbieter e.V. (fsm) begutachtet und festgestellt, dass die Anforderungen des § 4 Abs. 2 Jugendmedien-Staatsvertrag für geschlossene Benutzergruppen erfüllt werden.

Die datenschutzrechtliche Überprüfung ergab, dass der Direktabgleich der Daten der interessierten Nutzer mit Datenbanken Dritter nach §§ 4, 28 Abs. 1 Satz 1 Nr. 1 BDSG zulässig ist / war und im Rahmen dieses Abgleichs keine Bonitätsprüfung erfolgt. Die interessierten Nutzer werden im Rahmen der Registrierung umfassend über Art und Umfang der Datenerhebung und die weitere Nutzung der Daten informiert. Die AGB und die Datenschutzbestimmungen müssen gelesen und gesondert akzeptiert werden, ansonsten wird die Registrierung abgebrochen. Akzeptiert der Nutzer die AGB und die Datenschutzbestimmungen, willigt er gemäß §§ 4, 4 a Abs. 1 BDSG freiwillig in die Erhebung, Verarbeitung

und Nutzung seiner personenbezogenen Daten ein. Die Zulässigkeit der Weitergabe der Daten an einen beauftragten Dritten zum Zwecke des Datenabgleichs (Auftragsdatenverarbeitung i.S.v. § 11 BDSG) ergibt sich aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG.

4.2 Fehlende Anbieterkennzeichnung bei Tele- und Mediendiensten

Im Berichtszeitraum wurden wieder mehrere Verstöße von Anbietern geschäftsmäßiger Tele- und Mediendienste, die ihren Informationspflichten nach § 6 Teledienstegesetz (TDG) oder § 10 Mediendienste-Staatsvertrag (MDSV) nicht oder nur unzureichend nachgekommen waren, bei der Aufsichtsbehörde angezeigt. Aufgrund der Häufigkeit dieser Verstöße wurden stichprobenartig weitere Internetauftritte (z.B. von Vereinen) kontrolliert und dabei festgestellt, dass fast die Hälfte dieser Internetauftritte nicht über ein ordnungsgemäßes Impressum verfügten. Es wird daher in Erwägung gezogen, die Öffentlichkeit durch gezielte Berichte in der Tagespresse über die gesetzeskonforme Ausgestaltung eines Impressums zu informieren.

Nach § 6 TDG bzw. § 10 MDSV haben Diensteanbieter für geschäftsmäßige Tele-/ Mediendienste unter anderem folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:

- den Namen und die Anschrift, unter der sie niedergelassen sind, bei juristischen Personen zusätzlich den Vertretungsberechtigten,
- Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post,
- soweit der Teledienst im Rahmen einer Tätigkeit angeboten oder erbracht wird, die der behördlichen Zulassung bedarf, Angaben zur zuständigen Aufsichtsbehörde

- das Handelsregister, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister, in das sie eingetragen sind, und die entsprechende Registernummer.

Ein Verstoß gegen diese Informationspflicht stellt eine Ordnungswidrigkeit dar, die mit einem Bußgeld geahndet werden kann.

In den zur Anzeige gebrachten Fällen wurden die Diensteanbieter (Unternehmen, Vereine, Gewerbetreibende, politische Gruppierungen) schriftlich auf die fehlende bzw. unvollständige Anbieterkennzeichnung hingewiesen und aufgefordert, ihr Impressum binnen einer gesetzten Frist um die noch fehlenden Daten zu ergänzen. Die überwiegende Zahl der Betroffenen reagierte umgehend auf diese Aufforderung. Von der Einleitung eines Ordnungswidrigkeitsverfahrens wurde in diesen Fällen abgesehen.

In einigen wenigen Fällen zeigten sich die verantwortlichen Personen jedoch völlig uneinsichtig. So wurde gegen einen verantwortlichen Domain-Inhaber und administrativen Ansprechpartner ein Ordnungswidrigkeitsverfahren eingeleitet, der sich beharrlich weigerte, im Impressum eine Telefonnummer aufzunehmen, die Besuchern der Internetseite eine unmittelbare Kommunikation mit ihm als Diensteanbieter i.S.v. § 3 Abs. 1 MDSV ermöglicht hätte. Der Betroffene vertrat die Auffassung, als „reiner“ Domain-Inhaber kein Diensteanbieter i.S.v. § 3 Abs. 1 MDSV zu sein. Er hätte die betreffende Domain lediglich auf seinen Namen registrieren lassen und ihm politisch nahestehenden Personen schuldrechtlich erlaubt, unter seiner Domain rechtsradikale Inhalte im Internet zu veröffentlichen. Ihn als ausschließlichen Domain-Inhaber treffe daher weder eine Aufsichtspflicht bezüglich des Inhalts der Seiten noch eine Verpflichtung zur Bereithaltung eines Impressums.

Das zuständige Amtsgericht indessen ist dieser Auffassung nicht gefolgt und verurteilte den Betroffenen wegen eines vorsätzlichen Verstoßes gegen die Informationspflichten nach § 10 MDSV zu einer Geldbuße.

Als Domain-Inhaber und gleichzeitiger administrativer Ansprechpartner war der Betroffene der an der Domain materiell Berechtigte und – in Ermangelung einer anderen verantwortlichen Person – derjenige, gegen den sich die Maßnahme der Aufsichtsbehörde zu richten hatte.

In einem ähnlich gelagerten Fall war der Diensteanbieter Mitglied einer linksradikalen Gruppierung und hatte es aus Furcht vor Übergriffen anderer politischer Randgruppierungen unterlassen, die vollständige Anschrift, unter der die Gruppe zu erreichen ist, die ladungsfähige Anschrift des Vertretungsberechtigten und eine Telefonnummer anzugeben. Angesichts des drohenden Ordnungswidrigkeitsverfahrens hatte der Diensteanbieter es dann vorgezogen, die Internetseite aus dem Netz zu entfernen.

4.3 Veröffentlichung personenbezogener Daten in Diskussionsforen im Internet

Mehrere Eingaben richteten sich gegen die Veröffentlichung personenbezogener Daten in sog. Diskussionsforen im Internet. Die Beschwerdeführer fühlten sich durch die Veröffentlichung ihrer personenbezogenen Daten in solchen anonymen Foren in ihren Persönlichkeitsrechten verletzt.

Ein Petent beschwerte sich z.B. über den Betreiber eines Internetdienstes, der ihm unaufgefordert eine Werbe-eMail zugesandt haben soll. Der Petent postete dieses Spamming unter Verwendung eines Pseudonyms in einem Diskussionsforum, in dessen Verlauf sich der Diensteanbieter dann in die Diskussion einschaltete. In seinem Beitrag sprach der Diensteanbieter den Petenten entgegen der üblichen Gepflogenheiten mit seinem Echtnamen an. Der Petent sah sich durch die Veröffentlichung seines Namens im Internet in seinen Persönlichkeitsrechten verletzt.

Da es sich bei der Diskussionsplattform um einen Mediendienst i.S.v. § 2 Mediendienste-Staatsvertrag handelte, hatten die Teilnehmer dieses Diskussionsforums die Vorschriften der allgemeinen Gesetze und die gesetzlichen Bestimmungen zum Schutz der persönlichen Ehre einzuhalten (§ 11 Abs. 1 S. 2 MDSV). Dementsprechend war zu prüfen, ob mit der Bekanntgabe des Namens des Petenten in dem Forum gegen das in Artikel 5 Abs. 2 Grundgesetz verankerte Persönlichkeitsrecht verstoßen wurde.

Als Ergebnis der Überprüfung war festzustellen, dass der Petent in der persönliche Ansprache nicht in seinen Persönlichkeitsrechten verletzt worden war. In den anderen Fällen konnte ebenfalls keine Verletzung der Persönlichkeitsrechte festgestellt werden.

4.4 Versendung von Spammails

Ein Dauerthema, mit dem die Aufsichtsbehörde immer wieder befasst ist, betrifft die Versendung von Spammails. Obwohl es sich dabei grundsätzlich um einen Verstoß gegen Wettbewerbsrecht handelt und in § 7 Abs. 2 Nr. 3 des novellierten Gesetzes gegen den unlauteren Wettbewerb nunmehr ausdrücklich geregelt ist, wandten sich viele Petenten an die ADD mit der Bitte, die Zusendung dieser Werbe-eMails zu unterbinden.

Die Petenten wurden in diesen Fällen an die jeweiligen Verbraucherverbände verwiesen. Die Aufsichtsbehörde wurde nur in den Fällen tätig, in denen die Versender bekannt waren und die berechtigten Auskunftersuchen der Betroffenen (§ 34 BDSG) unbeantwortet ließen. Die betroffenen Unternehmen wurden angeschrieben und unter Hinweis auf ihre Auskunftspflicht aufgefordert, sowohl die Auskunftersuchen der Beschwerdeführer als auch zukünftig eingehende Auskunftersuchen sofort und umfassend zu beantworten.

4.5 Unterrichtungspflichten von Diensteanbietern nach dem TDDSG

Im Rahmen der Bearbeitung von Eingaben wurden teilweise auch die Internetauftritte der Betroffenen überprüft. Dabei wurde in einigen Fällen (u.a. bei einem Kreditinstitut, das seine Kunden hauptsächlich über das Internet betreut) festgestellt, dass die Nutzer entweder nur ganz allgemein, wie z.B.: „Die Vorschriften des Bundesdatenschutzgesetzes werden selbstverständlich genau beachtet“ oder bisweilen gar nicht über den Umfang und den Zweck der Datenerhebung unterrichtet wurden.

Nach § 4 Abs. 1 TDDSG hat der Diensteanbieter den Nutzer zu Beginn des Nutzungsvorganges über Art, Umfang und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereiches der EU zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein. Wer vorsätzlich oder fahrlässig entgegen § 4 Abs. 1 den Nutzer nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet, begeht eine Ordnungswidrigkeit, die mit einer Geldbuße geahndet werden kann.

Unter Hinweis auf die festgestellte Ordnungswidrigkeit wurden die verantwortlichen Stellen/Personen angeschrieben und aufgefordert, ihre Internetauftritte entsprechend zu überarbeiten bzw. eine umfassende Unterrichtung der Nutzer vorzunehmen. In der Regel kamen die verantwortlichen Stellen / Personen umgehend der Aufforderung nach. Lediglich in einem Fall ignorierte ein Verantwortlicher mehrfach die Aufforderung der Aufsichtsbehörde, so dass die Ordnungswidrigkeit mit einem Bußgeld geahndet wurde. Trotz der Festsetzung des Bußgeldes konnte der Betroffene bislang nicht dazu bewegt werden, die entsprechende Unterrichtung der Nutzer vorzunehmen. Zwangsmaßnahmen werden daher in Erwägung gezogen.

5. Datenschutz im Gesundheitswesen

5.1 Datenschutzgerechte Vernichtung von Patientendaten

Für niedergelassene Ärzte als „nicht-öffentliche Stelle“ i.S.v. § 2 Abs. 4 BDSG gilt neben der ärztlichen Schweigepflicht das BDSG. Insofern haben Ärzte bzw. deren Personal bei der Vernichtung von Patientendaten darauf zu achten, dass dies datenschutzgerecht geschieht.

Eine Beschwerdeführerin hatte ihr Altpapier ordnungsgemäß in der Blauen Tonne entsorgen wollen. Als sie die Tonne geöffnet hatte, fand sie darin einige Befundberichte einer Laborgemeinschaft, die an einen Arzt adressiert waren, der zuvor in ihrem Haus eine Praxis betrieben hatte. Die Beschwerdeführerin informierte die Aufsichtsbehörde umgehend über ihren Fund und äußerte die Vermutung, dass die Praxisnachfolgerin die Unterlagen in der Blauen Tonne entsorgt haben könnte.

Die datenschutzrechtliche Prüfung ergab, dass die betreffenden Befundberichte tatsächlich aus der Arztpraxis stammten. Die Praxisnachfolgerin hatte ihrer Aussage zufolge die Befundberichte aber nicht wesentlich in der Blauen Tonne entsorgt. Sie könnten sich nur zwischen alten Unterlagen (Rundschreiben, Zeitungsausschnitte, Prospektmaterial) ihres Vorgängers befunden haben, die von ihr nach und nach gesichtet und aussortiert worden waren.

Die nicht datenschutzgerechte Entsorgung der Befundberichte im Hausmüll durch die Ärztin stellt eine unbefugte Übermittlung personenbezogener Daten, die nicht allgemein zugänglich sind, an eine unbekannte Anzahl Dritter dar und verstößt damit gegen § 43 Abs. 2 Nr. 1 BDSG. Der Verstoß kann nach § 43 Abs. 3 BDSG mit einem Bußgeld geahndet werden.

Im vorliegenden Fall wurde jedoch von der Festsetzung einer Geldbuße abgesehen, da nur einige wenige Befundberichte in der Blauen Tonne

entsorgt wurden und ein unbekannter Dritter die Befunde keinem Patienten hätte zuordnen können. Die Namen der betroffenen Patienten waren durch die Verwendung einer Ziffernkombination pseudonymisiert (ersetzt) worden, so dass eine Bestimmung nicht oder nur unter wesentlich erschwerten Bedingungen möglich gewesen wäre. Die betroffene Ärztin wurde aber in aller Deutlichkeit darauf hingewiesen, wie eine datenschutzgerechte Entsorgung von Patientendaten zu erfolgen hat (Verichtung der Unterlagen in einem der DIN-Norm entsprechenden Reißwolf oder ordnungsgemäße Beauftragung eines Verwertungsbetriebes).

5.2 Anspruch eines Patienten auf Herausgabe von Unterlagen

Ein Petent führte Beschwerde über einen Facharzt, der sich weigerte, ihm kurzzeitig Videoaufnahmen auszuhändigen, die zur Dokumentation seiner Knie-OP angefertigt worden waren. Der Petent benötigte die Aufnahmen für eine bevorstehende Begutachtung durch einen anderen Facharzt in seinem laufenden Rentenantragsverfahren. Die Herausgabe der Videoaufnahmen hatte der Arzt seinem ehemaligen Patienten unter stets wechselnden Begründungen, zuletzt unter dem Hinweis auf den erheblichen Arbeitsaufwand für das Aufsuchen der Aufnahmen aus dem Archiv, verweigert.

Der Anspruch eines Patienten auf Einsicht in bzw. eine Auskunft aus seiner Patientenakte ergibt sich u.a. aus § 34 Abs. 1 BDSG. Daneben hatte der Bundesgerichtshofs bereits 1982 entschieden, dass jeder Patient das Recht hat, die über ihn geführte Patientenakte beim Arzt einzusehen. Das Einsichtsrecht bezieht sich dabei auf die dokumentationspflichtigen objektiven Sachverhalte und medizinischen Feststellungen, wobei ein Patient das Einsichtsrecht auch auf Dritte, wie z.B. einen Gutachter, übertragen darf (vgl. auch Beschluss des Bundesverfassungsgerichts vom 16.09.1998 – 1 BvR 1130/98).

Der betroffene Arzt konnte letztlich erst nach Einschaltung der zuständigen Bezirks-Ärzttekammer durch die Aufsichtsbehörde dazu bewegt werden, dem Patienten bzw. dem Gutachter die Möglichkeit zu geben, die Aufnahmen einzusehen.

In einem ähnlichen gelagerten Fall reichte ein Schreiben der ADD aus, um den Anspruch auf Akteneinsicht durchzusetzen.

5.3 Welche Fragen darf ein Arzt in einem Anamnesebogen stellen?

Zur Verkürzung des Erstgesprächs zwischen Arzt und Patient ist es in vielen Arztpraxen inzwischen üblich, neuen Patienten bei der Anmeldung einen Fragebogen auszuhändigen, in dem neben den Fragen zur Person (Name, Anschrift, Krankenkasse) u.a. Fragen zu akuten Erkrankungen, Vorerkrankungen, usw. beantwortet werden sollen.

Ein betroffener Patient wandte sich an die Aufsichtsbehörde, nachdem ihm im Rahmen einer anstehenden Zahnbehandlung ein solcher Anamnesebogen zum Ausfüllen ausgehändigt worden war und bat um datenschutzrechtliche Prüfung dieses Fragebogens. Die Patienten wurden darin u.a. nach dem Arbeitgeber und wie oder durch wen man auf die Praxis aufmerksam wurde, gefragt.

Bei dem Fragebogen handelte es sich um eine nicht-automatisierte Datei i.S.v. § 3 Abs. 2 Satz 2 BDSG. Aufgrund des zwischen dem Patienten und dem Arzt zustande gekommenen Behandlungsvertrages beurteilte sich die Rechtmäßigkeit der Datenerhebung und -nutzung nach den §§ 4, 28 Abs. 1 BDSG. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.

Es ist unbestritten, dass ein Arzt für die Behandlung eines Patienten umfassende Kenntnis über dessen medizinische Vorgeschichte benötigt. Für eine Behandlung ist es jedoch nicht erforderlich zu wissen, wer Arbeitgeber des Patienten ist und wie bzw. durch wen man auf die Praxis aufmerksam wurde. Die Erhebung und Speicherung dieser für die Behandlung nicht erforderlichen, aber in die Privatsphäre der Patienten eindringenden Daten verstößt gegen die §§ 3a und 28 Abs. 1 Satz 1 BDSG und ist damit unzulässig.

Als datenschutzrechtlich bedenklich wurde es erachtet, sich von den Patienten durch ihre Unterschrift die Richtigkeit und Vollständigkeit ihrer Angaben bestätigen zu lassen. Da ein Laie die Bedeutung von Erkrankungen und Medikamenten für die Zahnbehandlung nicht einzuschätzen vermag, kann ein Arzt ihm nicht die Verantwortung für eine korrekte medizinische Befunderhebung aufgeben. Diese Verantwortung trägt weiterhin der Arzt. Eine entsprechende Erklärung führt beim Patienten zu falschen Vorstellungen über die Datenerhebung und seine Pflichten beim Ausfüllen des Anamnesebogens. Dies widerspricht den §§ 4, 4a BDSG. Die Erklärung „richtig und vollständig“ darf für die o.g. – vom Behandlungsvertrag nicht umfassten Fragen – nicht gefordert werden.

5.4 Aushändigen von Patientenakten nach Beendigung der Behandlung

In mehreren Fällen wandten sich Patienten an die ADD, um nach einem Arztwechsel bzw. nach Übergabe der Praxis an einen Nachfolger in den Besitz der Patientenakte zu gelangen, bzw. zu verhindern, dass die Akte in die Hände des Praxisnachfolgers gelangte.

Ein Recht auf Herausgabe der Krankenakte besteht nicht, weil diese zivilrechtlich im Eigentum des sie erstellenden Arztes steht. Deshalb hat ein Patient keinen Anspruch auf Herausgabe der Originaldokumentation.

Nach der Berufsordnung für Ärztinnen und Ärzte besteht für ärztliche Aufzeichnungen, also auch für die Krankenakte als Sammlung patientenbezogener medizinischer und pflegerischer Dokumente, eine Aufbewahrungspflicht, die 10 bzw. 30 Jahre betragen kann.

Eine Löschung der Daten kann in dem Zeitraum, in dem die Pflicht zur Aufbewahrung der ärztlichen Dokumentation besteht, nicht verlangt werden.

Die Patientendaten sind nach Abschluss der Behandlung zu sperren, so dass der Arzt nicht mehr ohne Weiteres darauf zugreifen kann. Der die Praxis übernehmende Arzt hat nur dann Zugriff auf die Krankenakte, wenn der Patient dies ausdrücklich zulässt. Näheres regelt die ärztliche Berufsordnung.

§ 10 IV der Berufsordnung für Ärztinnen und Ärzte in Rheinland-Pfalz regelt, dass der Arzt auch nach Aufgabe der Praxis die ärztliche Dokumentation aufzubewahren oder dafür Sorge zu tragen hat, dass sie in gehörige Obhut gegeben werden. Das kann auch durch Übergabe an den die Praxis übernehmenden Arzt erfolgen. Allerdings hat der Arzt, dem bei einer Praxisübergabe ärztliche Aufzeichnungen über Patienten in Obhut gegeben werden, die Aufzeichnungen unter Verschluss zu halten und darf sie nur mit Einwilligung des Patienten einsehen oder weitergeben.

6. Arbeitnehmerdatenschutz

Es ist festzustellen, dass Anfragen / Eingaben zum Thema Arbeitnehmerdatenschutz immer mehr zunehmen. Erfreulich ist, dass zu dieser Problematik nicht in erster Linie Eingaben von Arbeitnehmern und Betriebsräten zu verzeichnen sind, sondern dass auch auf Arbeitgeberseite eine Sensibilität für datenschutzrechtliche Fragen besteht, in der Regel

die Bereitschaft vorhanden ist, sich von fachkundiger Seite beraten zu lassen und Verfahrensweisen den Vorgaben des Bundesdatenschutzgesetzes anzupassen.

Arbeitnehmer sind bei der Erhebung, Verarbeitung und Nutzung ihrer personenbezogenen Daten durch den Arbeitgeber durch das in der Verfassung garantierte Recht auf Persönlichkeitsschutz und dessen Auslegung für das Arbeitsverhältnis durch die Rechtsprechung, durch die Regelungen des Bundesdatenschutzgesetzes (BDSG) sowie durch die Regelungen des Betriebsverfassungsgesetzes über die Mitwirkungs- und Mitbestimmungsrechte des Betriebsrates - jedenfalls in ihrem Kern - geschützt.

Nach § 28 Abs.1 Satz 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient. Diese Vorschrift gilt für persönliche Daten wie Name, Adresse, Geburtsdatum, Familienstand, Alter, beruflicher Abschluss. Daneben gibt es jedoch auch Daten, die als sensible Daten bzw. besondere Arten personenbezogener Daten einem noch stärkeren Schutz unterliegen, wie Gesundheitsdaten, politische Meinungen, Angaben über rassische und ethnische Herkunft und religiöse Überzeugungen.

Das Erheben, Verarbeiten und Nutzen von diesen besonderen Arten personenbezogener Daten ist unter noch engeren Voraussetzungen zulässig.

Nach § 28 Abs. 6 oder Abs. 8 BDSG ist, soweit nicht der Betroffene, also in diesem Fall der Arbeitnehmer eingewilligt hat, das Erheben, Speichern und Nutzen diese Daten zulässig, wenn der Betroffene diese offenkundig öffentlich gemacht hat oder dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche (des Arbeitgebers) er-

forderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des betroffenen Arbeitnehmers an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt.

Die Frage, ob die Erfassung und Nutzung von Mitarbeiterdaten im Einklang mit diesen Vorschriften stand, war im Berichtszeitraum Gegenstand mehrerer Anfragen.

6.1 Erhebung „sensibler Daten“ im Bewerbungsverfahren

So erfragte ein Personalvermittler im Rahmen von Einstellungsverfahren mittels eines Erhebungsbogens unter anderem sogenannte sensible Daten, wie chronische Krankheiten, Suchterkrankungen, Allergien, Hobbys, Vorstrafen, Körperdaten etc.

Einer der Bewerber wandte sich im Berichtszeitraum an uns, um zu erfragen, ob diese umfangreiche Datenerhebung zulässig ist.

Bei einem Bewerbungsverfahren handelt es sich um ein vertragsähnliches Vertrauensverhältnis i.S.v. § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Sowohl im Bewerbungsverfahren als auch noch nach Beendigung des Arbeitsverhältnisses gilt die sich aus dem Betriebsverfassungsgesetz ergebende spezielle arbeitsrechtliche Schutzpflicht und es besteht ein Anspruch des Arbeitnehmers auf Schutz seiner Persönlichkeitsrechte gegenüber dem Arbeitgeber.

Der künftige Arbeitgeber oder die von ihm mit der Auswahl des Personals beauftragte Stelle muss demnach bereits vor der Beschaffung von Informationen über den Bewerber prüfen, ob sich die Erhebung aus der Zweckbestimmung der arbeitsvertraglichen Beziehungen, d.h. des Arbeitsvertrages bzw. des vorgeschalteten Arbeitsverhältnisses rechtfertigt. Diese Rechtfertigung kann sich jedoch nicht aus der Zweckbestim-

mung der Erhebung an sich, sondern nur aus dem Zweck der nachfolgenden Verarbeitung oder Nutzung ergeben.

Unter Zugrundelegung dieser Maßstäbe ist die Frage nach Hobbys, Vereinszugehörigkeit und Ehrenämtern unzulässig und aus einem Fragenkatalog zu entfernen, es sei denn die Aktivitäten können sich auf die berufliche Tätigkeit auswirken, wie z.B. Tätigkeit bei der freiwilligen Feuerwehr, da Einsätze auch während der Arbeitszeit stattfinden können. Führungsdaten (Vorstrafen) können z.B. für die Besetzung einer Führungsposition, bei einer Position als Kassierer oder Ausbilder, also bei einer besonderen Vertrauensstellung, im Einzelfall erforderlich und damit zulässig sein. Besondere Zulässigkeitsvoraussetzungen gelten für Gesundheitsdaten als besonderen Arten personenbezogener Daten.

Im Rahmen der Anbahnung eines Arbeitsverhältnisses ist – je nach Art der zu besetzenden Stelle – die Erhebung der Gesundheitsdaten, evt. Körperdaten eines Bewerbers erforderlich bzw. unerlässlich. Deren Erhebung, Verarbeitung oder Nutzung ist aber nur unter Beachtung der restriktiven Vorgaben des BDSG für sensible Daten gestattet, sofern der Bewerber nicht ausdrücklich in diese Datenerhebung eingewilligt hat.

Angaben zur rassischen oder ethnischen Herkunft dürfen jedoch selbst im Falle einer erteilten Einwilligung nicht erhoben werden, weil dies zu einer gesetzlich untersagten Diskriminierung des Bewerbers bzw. der Mitbewerber führen würde. Der Hinweis, dass diese Daten „nur“ von Bewerbern auf Ausschreibungen von Unternehmen außerhalb der Europäischen Union erfragt werden, ist unbeachtlich, da sich die Datenerhebung nach den im Geltungsbereich des BDSG gültigen Rechtsnormen zu richten hat.

In dem vorliegenden Fall wurde der Personalvermittler aufgefordert, den Bewerbungsbogen den gesetzlichen Anforderungen anzupassen und falls erforderlich und im Einzelfall zulässig, die Erhebung der besonde-

ren Arten personenbezogener Daten dem persönlichen Bewerbungsgespräch vorzubehalten.

6.2 Veröffentlichung von Arbeitnehmerdaten zu Werbezwecken

Ein Softwarehersteller veröffentlichte die von einer Mitarbeiterin eingereichte Arbeitsunfähigkeitsbescheinigung zum Zwecke der Werbung für eine Software im Rahmen einer Produktpräsentation vor Kunden.

Bei den in der Arbeitsunfähigkeitsbescheinigung eingetragenen Gesundheitsdaten handelt es sich um besondere Arten personenbezogener Daten. Eine Nutzung dieser Daten ist zulässig, soweit der Betroffene eingewilligt hat. Die Einwilligung ist jedoch nur wirksam, wenn sie auf der freien Entscheidung der Betroffenen beruht und bedarf der Schriftform. Soweit besondere Arten personenbezogener Daten erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

Die Nutzung der in der Arbeitsunfähigkeitsbescheinigung eingetragenen Daten wäre demnach zulässig gewesen, wenn der Arbeitgeber dazu vorab die ausdrückliche schriftliche Einwilligung der Mitarbeiterin eingeholt hätte. Dies war jedoch nicht der Fall. Die Mitarbeiterin hatte der Verwendung der Arbeitsunfähigkeitsbescheinigung nur unter der Voraussetzung zugestimmt, dass die darin zu ihrer Person eingetragenen Daten abgedeckt würden. Ohne die Einholung der vorherigen ausdrücklichen Einwilligung wäre die Nutzung der sensiblen personenbezogenen Daten nur zulässig gewesen, wenn das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet. Die Tatbestandsvoraussetzungen dieser gesetzlichen Erlaubnisnorm trafen jedoch in diesem Fall nicht zu.

Aus diesem Grund hatte der Software Hersteller mit der Verarbeitung und Nutzung der sensiblen personenbezogenen Daten der Mitarbeiterin

zu Präsentationszwecken gegen geltendes Datenschutzrecht verstoßen. Der Verstoß ist bußgeldbewehrt und kann mit einem Bußgeld bis zu 250.000,- Euro geahndet werden (§ 43 Abs. 3 BDSG). Die Mitarbeiterin bat aus Sorge vor Verlust ihres Arbeitsplatzes jedoch ausdrücklich darum, keine rechtlichen Schritte gegen ihren Arbeitgeber einzuleiten und diesen auch nicht über ihre Anfrage zu informieren.

6.3 Namensschilder auf Arbeitskleidung

Ein Mitarbeiter eines Produktionsbetriebes fragte an, ob es zulässig sei, dass die Geschäftsleitung die an den Maschinen beschäftigten Mitarbeiter „zwingt“, firmeneigene Arbeitskleidung zu tragen, auf der der vollständige Namen des Mitarbeiters stehe.

Die Prüfung ergab, dass ein berechtigtes Interesse des Arbeitgebers als der verantwortlichen Stelle an dem Tragen der Namensschilder bestand. Es handelte sich hierbei um eine rein innerbetriebliche Maßnahme, die einem geregelten Betriebsablauf dienen sollte und mit dem Betriebsrat abgestimmt war.

Eine Beeinträchtigung der Persönlichkeitsrechte der Mitarbeiter ist darin nicht zu sehen. Ob ein Mitarbeiter die Arbeitskleidung beim Verlassen des Betriebsgeländes noch trägt und damit seine personenbezogenen Daten öffentlich bekannt gibt, ist seiner eigenen Entscheidung überlassen.

6.4 Interne Veröffentlichung von Arbeitnehmerdaten

Die Prokuristin eines Unternehmens bat um Auskunft, ob der Arbeitgeber die Mitarbeiter auffordern dürfe, ihre Resturlaubstage / Kurzarbeitstage in eine Liste einzutragen, die im firmeneigenen Intranet veröffentlicht werden sollte und von allen Mitarbeitern eingesehen werden könnte.

Der Prokuristin wurde mitgeteilt, dass in diesem Fall die Erhebung und Speicherung der personenbezogenen Daten in einer von allen Mitarbeitern einzusehenden Datei über die Zweckbestimmung des einzelnen Arbeitsverhältnisses hinausgehe. Für die interne Arbeitsorganisation ist es nicht erforderlich, dass alle Mitarbeiter in eine solche Liste einsehen können. Die Einsicht ist nur der Stelle zu gewähren, die diese Daten tatsächlich zur Aufgabenerfüllung benötigt, der Personalabteilung. Demzufolge sind die Angaben auch nicht in der Form zu erheben, dass sich jeder Mitarbeiter in eine für andere einsehbare Liste einträgt.

Dies gilt nur dann nicht, wenn die Mitarbeiter vorher ihre ausdrückliche Einwilligung für die beabsichtigte Datenerhebung erteilt haben, die nur wirksam ist, wenn sie auf der freien Entscheidung der Betroffenen beruht. Die Frage der Freiwilligkeit ist im Rahmen eines Arbeitsverhältnisses aber sehr kritisch zu prüfen.

6.5 Löschung von Arbeitnehmerdaten nach Beendigung des Arbeitsverhältnisses

Ein ehemaliger Mitarbeiter eines Unternehmens führte Beschwerde darüber, dass dieses Unternehmen der Aufforderung, die zu seiner Person gespeicherten Daten nach Beendigung des Arbeitsverhältnisses zu löschen, nicht nachgekommen ist. Insbesondere verlangte er die Löschung eines von ihm gespeicherten Digitalfotos.

Personenbezogene Daten sind, wenn sie für die Erfüllung eigener Zwecke verarbeitet werden, zu löschen, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist. An die Stelle der Löschung tritt eine Sperrung, wenn Aufbewahrungsfristen bestehen, die sich zum Beispiel aus einer Satzung oder anderen gesetzlichen Vorschrift ergeben oder auch wenn schutzwürdige Interessen des Betroffenen entgegenstehen.

Nach Aussage des Unternehmens hatte der Beschwerdeführer der Speicherung des von Ihm angefertigten Digitalfotos (zum Zwecke der besseren Visualisierung der Mitarbeiter) in der Mitarbeiterverwaltung nicht widersprochen. Mit dem Zeitpunkt seines Ausscheidens aus dem Unternehmen war es jedoch nicht mehr erforderlich, das Foto weiterhin zu speichern. Dessen Löschung hätte umgehend erfolgen müssen. Mit der über den Zeitraum des Ausscheidens hinaus erfolgten weiteren Speicherung des Fotos wurde gegen datenschutzrechtliche Bestimmungen verstoßen.

Der Forderung, alle weiteren zur Person gespeicherten Daten zu löschen, stehen die im Handelsgesetzbuch und der Abgabenordnung geregelten gesetzlichen Aufbewahrungsfristen entgegen. Diese Bestimmungen gehen denen des BDSG vor. Im Regelfall besteht jedoch die Verpflichtung zur Speicherung in gesperrter Form.

6.6 Telefondatenerfassung der Mitarbeiter

Der Betriebsrat eines Unternehmens fragte an, unter welchen Voraussetzungen die Speicherung der Anruflisten der Mitarbeiter durch den Arbeitgeber zulässig sei.

Ihm wurde mitgeteilt, dass grundsätzlich bei der Speicherung von Anruflisten durch eine Telefonanlage der Anwendungsbereich des Bundesdatenschutzgesetzes gegeben ist, da regelmäßig personenbezogene Daten im Sinne des § 3 BDSG gespeichert werden.

Die Erfassung dieser Daten, zumindest was dienstliche Telefonate betrifft, kann im Rahmen eines Arbeitsverhältnisses legitimiert sein, um dem Arbeitgeber die aus dem Arbeitsverhältnis resultierenden Kontrollbefugnisse zu ermöglichen (§ 28 Abs. 1 S.1 Nr. 1 BDSG). Die Grenze wird unter Beachtung des Grundsatzes der Verhältnismäßigkeit durch

den Anspruch des Arbeitnehmers auf Schutz des Rechts auf informationelle Selbstbestimmung bestimmt.

Die Führung rein privater Telefongespräche ist nur gestattet, wenn der Arbeitgeber dies erlaubt hat. Sofern der Arbeitgeber diese zugelassen hat, fallen sie in den Anwendungsbereich des Teledienstegesetzes. Die Erfassung ist bei privaten Telefonaten nur in eingeschränktem Umfang möglich. Hier ist es nur gestattet, die für den technischen Betrieb und zur Gewährleistung der Datensicherheit des Netzes benötigten Daten vorübergehend in Protokolldateien zu speichern und soweit die private Nutzung eine Entgeltzahlungspflicht nach sich zieht, die Abrechnungsdaten nach Beendigung des Telefonats festzuhalten.

Es ist sinnvoll, den Umfang der Erfassung, die Frage der Zulassung und Erfassung von privaten Telefongesprächen, die Stellung der Mitarbeitervertretungen, Fragen der Betreuung und Wartung und Bedienung der Telefonanlage einvernehmlich in einer Betriebsvereinbarung zwischen Arbeitgeber und Betriebsrat zu regeln.

6.7 Beteiligungsrechte eines Betriebsrates

Der Betriebsrat eines Unternehmens erbat von der Firmenleitung zur Kontaktaufnahme mit den Beschäftigten eine Liste mit den Privatanschriften der Beschäftigten. Die Personalabteilung des Unternehmens war unsicher, welche Daten dem Betriebsrat zur Verfügung gestellt werden dürfen und wendete sich an die ADD.

Grundsätzlich sind dem Betriebsrat nach dem Betriebsverfassungsgesetz (BetrVG) auf Verlangen jederzeit die zur Durchführung seiner Aufgaben erforderlichen Unterlagen zur Verfügung zu stellen. Sofern der Arbeitgeber nicht durch spezielle Vorschriften des BetrVG verpflichtet ist, bestimmte Daten der Mitarbeitervertretung bekannt zu geben, ist die Zulässigkeit derartiger Nutzungen – soweit die Bestimmungen des Be-

etriebs- bzw. Personalvertretungsrechts nicht entgegenstehen – an der Zweckbestimmung des Beschäftigungsverhältnisses zu messen.

Eine Weitergabe von Grunddaten über die Beschäftigten (Name, Vorname, Abteilung, betriebliche Telefon- & e-Mail-Adresse) zur dauerhaften Nutzung durch die Mitarbeitervertretung ist zur Erfüllung des allgemeinen Informationsanspruchs als zulässig anzusehen, da die Mitarbeitervertretung diese Daten zur Durchführung ihrer allgemeinen Aufgaben, um Konflikte zu vermeiden und den Betriebsfrieden zu erhalten, benötigt.

Die Weitergabe der privaten Anschriften der Beschäftigten an die Mitarbeitervertretung und Speicherung geht über die Zweckbestimmung des einzelnen Arbeitsvertrages hinaus und ist daher grundsätzlich unzulässig. Der Betriebsrat müsste, sofern er diese Daten unbedingt für eine dauerhafte Nutzung vorhalten möchte (Vorratsspeicherung), vorab die ausdrückliche Einwilligung eines jeden Beschäftigten dazu einholen.

In einem konkreten Mitbestimmungsverfahren bzw., wenn im Einzelfall Anhörungs- und Unterrichtsrechte bestehen, ist der Betriebsrat nach den Bestimmungen des Betriebsverfassungsgesetzes jedoch jeweils rechtzeitig, umfassend und vollständig anhand von Unterlagen zu unterrichten.

Personenbezogene Unterlagen sind dabei regelmäßig nach Abschluss des Verfahrens zurückzugeben, um dem Recht des einzelnen Mitarbeiters auf Wahrung der informationellen Selbstbestimmung zu genügen.

7. Videoüberwachung

Im Berichtszeitraum haben die Anfragen und Eingaben zu dem Bereich der Videoüberwachung zugenommen. Mehrere Anfragen zu diesem Thema erfolgten durch Personen, die sich durch eine in der unmittelbaren Nachbarschaft installierte Videokamera gestört fühlten oder auch

von Arbeitnehmern, deren Arbeitsplatz von Videokameras erfasst wurden. Bei der Prüfung dieser Fälle ist zu unterscheiden zwischen der Videoüberwachung im privaten Bereich und in öffentlich zugänglichen Räumen.

Das Bundesdatenschutzgesetz trifft in § 6 b nur eine Regelung für die Beobachtung öffentlich zugänglicher Räume im Sinne öffentlich zugänglicher Bereiche. Dies sind Bereiche, die entweder dem öffentlichen Verkehr gewidmet sind, so wie z.B. Straßen und Plätze oder aber nach dem erkennbaren Willen des Berechtigten von jedermann genutzt oder betreten werden können, wie Bahnhöfe, Ausstellungsräume von Museen, Verkaufsräume von Geschäftsgebäuden etc.. Nicht dazu gehören Wohnungen / Privathäuser mit Gärten oder Arbeitsplätze, wenn sie sich nicht in öffentlich zugänglichen Bereichen befinden.

Daher wurde bei der Prüfung der Zulässigkeit von Videoüberwachungen von Privatgrundstücken ermittelt, welche Bereiche erfasst wurden und zu welchem Zweck die Überwachung erfolgt.

Der Anwendungsbereich des BDSG ist nicht gegeben, wenn ein Hausbesitzer zur Überwachung seines Hauseingangs und seines Vorgartens eine Videokamera installiert. Selbst wenn die Kamera auch einen an dem Grundstück vorbeiführenden öffentlichen Weg partiell erfasst, ist dies nicht nach BDSG zu bewerten, wenn die Überwachung ausschließlich zu persönlichen oder familiären Zwecken erfolgt. Gleichwohl kann bei gleichzeitiger Erfassung öffentlich zugänglicher Räume (Straßenraum) oder Nachbargrundstücke das Grundrecht des Nachbarn oder von Passanten auf informationelle Selbstbestimmung verletzt sein. Die Aufnahme von Personen mittels einer Videokamera und deren Speicherung stellt einen Eingriff in das in Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 des Grundgesetzes verankerten allgemeinen Persönlichkeitsrechts dar. Dieses Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner

persönlichen Daten zu bestimmen (Recht auf informationelle Selbstbestimmung).

Im Fall einer Eingabe konnte durch eine geänderte Kameraeinstellung dem Recht des Nachbarn Genüge getan werden, in einem weiteren ergab die Prüfung, dass nur das eigene Grundstück überwacht wurde.

In einem dritten Fall hatte eine Hauseigentümer ebenfalls an seiner Hauswand eine Kamera installiert, die jedoch fast ausschließlich den Straßenraum erfasste. Im Rahmen der Prüfung stellte sich heraus, dass die Überwachung gerade nicht ausschließlich persönlichen und familiären Zwecken diene und daher der Anwendungsbereich des § 6 b gegeben war. Grund für die Installation der Kamera war in diesem Fall der Ärger über Falschparker in der Anliegerstraße, die der Hauseigentümer erfassen und dann dem Ordnungsamt melden wollte.

Nach § 6 Abs. 1 BDSG ist die Beobachtung öffentlich zugänglicher Räume (hier: Fußgänger- u. Straßenverkehr) mit optisch elektronischen Einrichtungen (Videoüberwachung) jedoch nur zulässig, soweit sie entweder zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen. Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist (§ 6 Abs. 3 BDSG).

In dem oben erläuterten Fall der Überwachung des Verkehrsraumes war die Videoüberwachung eindeutig unzulässig. Zum einen ist es allein Aufgabe der zuständigen Behörden Ordnungswidrigkeiten zu verfolgen und geeignete Maßnahmen zu ergreifen, im übrigen wäre eine

Videoüberwachung bei einem Verstoß gegen Parkvorschriften unverhältnismäßig. Nach Intervention des Ordnungsamtes wurde die Kamera entfernt.

Videoüberwachungen am Arbeitsplatz außerhalb öffentlich zugänglicher Räume im Sinne des BDSG fallen nicht in den Anwendungsbereich des Bundesdatenschutzgesetzes, soweit eine reine Beobachtung ohne Aufzeichnung erfolgt. Eine andere Qualität erhalten die Aufnahmen dadurch, dass sie auf Datenträgern gespeichert und ausgewertet werden. Die Anwendbarkeit des Bundesdatenschutzgesetzes ergibt sich dann aus der Tatsache, dass es sich bei den Videobildern um personenbezogene Daten handelt. Insbesondere, wenn eigene Mitarbeiter aufgenommen werden, lässt sich der Bezug auf eine bestimmte Person einfach herstellen.

Berechtigt kann eine Videoüberwachung am Arbeitsplatz wegen des durch eine Videobeobachtung erzeugten Überwachungsdrucks nur sein, wenn es das zum Schutz des Betriebs und der Personen geeignetste und unter dem Verhältnismäßigkeitsprinzip schonendste Mittel ist.

In den uns zugegangenen Fällen wurde geprüft, ob die Mitarbeiter über die Tatsache und den Umfang der Videoüberwachung informiert wurden bzw. bei Bestehen eines Betriebsrates dieser ebenfalls beteiligt wurde. Außerdem wurde geprüft, in welchen Bereichen des Betriebes und zu welchem Zweck die Aufnahmen erfolgten, wie lange die Aufnahmen gespeichert wurden, wer Zugriff auf die Daten hat und ob die notwendigen organisatorischen und technischen Sicherungsmaßnahmen ergriffen wurden.

So musste in einem uns angezeigten Fall eine Videokamera vor Toiletten und Aufenthaltsraum eines Unternehmens während des Produktionsbetriebes ausgeschaltet werden, weil die schutzwürdigen Interessen der Mitarbeiter überwogen. Die Überwachung der Hallentore und Ausgänge der Produktionshalle war jedoch zulässig, weil in dem Betrieb

sehr kleinteilige und hochwertige Güter verarbeitet wurden und vor der Installation der Kameras eine hohe Diebstahlsquote zu verzeichnen war. In diesem Fall war der Verhältnismäßigkeitsgrundsatz gewahrt.

8. Datenschutz im Verein

Ein Mitglied einer Selbsthilfeorganisation, die in der Rechtsform des Vereins organisiert ist, hatte sich an die ADD gewandt, nachdem es von einem Versicherungsvertreter einer großen Versicherung aufgesucht worden war. Es stellte sich heraus, dass der Versicherungsvertreter von dem Verein die Daten aller Mitglieder erhalten hatte. Bei seinem Besuch legte der Versicherungsvertreter dem Vereinsmitglied ein von seinem Verein an ihn gerichtetes Schreiben vor, in dem er über den Besuch des Versicherungsvertreters informiert wurde.

Das Vereinsmitglied bat um Überprüfung und Mitteilung, ob die Übermittlung der personenbezogenen Daten der Mitglieder des Vereins an die Versicherung - ohne vorab deren Einverständnis eingeholt zu haben - gemäß den Bestimmungen des Bundesdatenschutzgesetzes zulässig war.

Nach sachlicher und rechtlicher Prüfung der Angelegenheit wurde dem Petenten u.a. mitgeteilt, dass ein Verein – nach den zwischen den Datenschutzaufsichtsbehörden und den Verbänden der Versicherungswirtschaft getroffenen Absprachen – im Rahmen eines Gruppenversicherungsvertrages dem Versicherungsunternehmen bzw. dem Versicherungsvertreter die Daten seiner Mitglieder nur unter folgenden Voraussetzungen übermitteln darf:

- Bei Neumitgliedern, die nach Abschluss eines Gruppenversicherungsvertrages dem Verein beitreten, muss die Einwilligung eingeholt werden. Dies sollte zweckmäßigerweise in der Beitrittserklärung oder im

Aufnahmeantrag vorgesehen werden, wobei das Mitglied darüber aufzuklären ist, welche Daten an welches Unternehmen weitergegeben werden sollen.

- Bei Altmitgliedern, die bei Abschluss eines Gruppenversicherungsvertrages bereits Vereinsmitglied waren, genügt es, wenn der Verein sie vor der Übermittlung ihres Namens und ihrer Anschrift an die Versicherung in einem Schreiben informiert und ihnen den Besuch eines Versicherungsvertreters ankündigt. In dem Schreiben muss auf die Möglichkeit des Widerspruchs gegen die Datenübermittlung und den Vertreterbesuch hingewiesen und dem Vereinsmitglied ausreichend Zeit eingeräumt werden, von dieser Widerspruchsmöglichkeit Gebrauch zu machen.

- Will ein Verein sich über die von der Versicherung gewährte übliche Vermittlungsprovision hinaus vom Mitglied die sog. Überschussbeteiligung aus der Rückerstattung von Prämienanteilen als Spende schenkweise abtreten lassen, müssen hierüber sowohl Neumitglieder bei Einholung der Einwilligung wie auch Altmitglieder bei der Information über ihr Widerrufsrecht ausreichend unterrichtet werden.

Zwar entsprach der Inhalt des von dem Verein verfassten Schreibens an die Mitglieder den gesetzlichen Vorgaben, jedoch erfolgte die Information zu spät. Der Verein hat die Mitglieder zukünftig rechtzeitig vor der Übermittlung ihrer personenbezogenen Daten an eine Versicherung zu informieren, so dass sie ausreichend Zeit haben, der Datenübermittlung zu widersprechen.

9. Wohnen und Liegenschaften

- 1. Weitergabe von Daten des Mieters an Dritte durch den Vermieter bzw. Weitergabe von Daten einzelner Miteigentümer an andere Miteigentümer**

Eine Anfrage betraf die Frage, unter welchen Voraussetzungen die Weitergabe von Mieterdaten an Dritte gerechtfertigt ist, eine weitere die Frage der Weitergabe von Daten innerhalb einer Eigentumsgemeinschaft

Nach § 28 Abs. 1 Satz 1 Nr. 1 Bundesdatenschutzgesetz (BDSG) ist das Erheben, Verarbeiten oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertrags-ähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.

In dem ersten uns vorliegenden Fall erhielt der Mieter einer Wohnung Hilfe zum Lebensunterhalt. Er hatte dem Vermieter selbst Mitteilung darüber gegeben, dass die Miete vom Sozialamt übernommen wurde. Er beanstandete jedoch, dass der Vermieter nach Erstellung der jährlichen Betriebs- und Heizkostenabrechnung bei dem zuständigen Sozialamt nachfragte, an wen das Guthaben auszuführen sei.

Da der Mieter selbst die Information über den Bezug von Sozialhilfe gegenüber dem Vermieter bekannt gegeben hatte, erfolgte keine unzulässige Übermittlung seiner personenbezogenen Daten an das Sozialamt; dies mit der Folge, dass ein Verstoß gegen das Bundesdatenschutzgesetz nicht festgestellt werden konnte.

In dem zweiten Fall wurde die jährliche Betriebs- und Nebenkostenabrechnung (Wohngeldabrechnung) einer Wohnungseigentumsgemeinschaft sämtlichen Miteigentümern unter genauer Aufschlüsselung der Kosten der einzelnen Miteigentümer zur Verfügung gestellt. Dies wurde von einer Miteigentümerin beanstandet.

Die Prüfung ergab, dass die Bekanntgabe der Daten der einzelnen Miteigentümer in der Betriebs- / Nebenkostenabrechnung grundsätzlich gegen § 28 Abs. 1 Nr. 2 BDSG verstößt und damit unzulässig ist, es sei denn, dass sich die Eigentümergemeinschaft in Kenntnis eines möglichen Verstoßes gegen datenschutzrechtliche Bestimmungen mehrheit-

lich für die Abrechnung in dieser Form ausgesprochen hat. Aufgrund der von der Mehrheit der Miteigentümer erteilten Einwilligungen nach § 4 Abs. 1 BDSG konnte die Verfahrensweise nicht beanstandet werden.

2. Bonitätsprüfung im Mietverhältnis

Sehr häufig werden wir mit der Frage konfrontiert, dass Vermieter nach erfolgter Wohnungsbesichtigung und vor Abschluss eines Mietvertrages Auskünfte über die persönlichen und wirtschaftlichen Verhältnisse der Mietinteressenten erfragen. Dabei wurden Daten abverlangt, die in die Privatsphäre der Betroffenen eingreifen und damit deren Recht auf informationelle Selbstbestimmung einschränken.

Die Erfassung und Verarbeitung von Daten von Mietinteressenten bedarf nach geltender Rechtslage stets einer Rechtsgrundlage. Sofern der Vermieter jedoch nicht darlegen kann, inwieweit bestimmte Daten für Zwecke der Durchführung des Mietverhältnisses dienlich und erforderlich sind, d.h. auch inwieweit berechnete Interessen des Vermieters an der Verarbeitung gegeben sind, kann eine Verarbeitung nur auf der Grundlage der freien Einwilligung des Mietinteressenten zulässig sein.

Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist (§ 4 Abs. 1 Bundesdatenschutzgesetz/BDSG).

Unabhängig davon kann von einer „Freiwilligkeit“ der Erteilung der Auskünfte bei Mieter-Selbstauskünften dennoch nicht ausgegangen werden, da sich die Wohnungsinteressenten der Beantwortung der Fragen nur entziehen können, wenn sie in Kauf nehmen, mit einer unvollständig ausgefüllten Mieter-Selbstauskunft abgelehnt zu werden.

Nach der derzeit geltenden Rechtsprechung geht die Mehrzahl der Gerichte davon aus, dass Mieterfragebögen bzw. Mieter-Selbstauskünfte dann nicht unzulässig sind, wenn sie Fragen beinhalten, „an deren Beantwortung für das Mietverhältnis ein berechtigtes, billigenwertes und

schutzwürdiges Interesse“ besteht. Gefragt werden darf daher nur nach Umständen, die für den Vermieter bei objektiver Wertung unter Berücksichtigung schutzwürdiger Belange des Mieters wesentlich sind. Bestimmte Daten dürfen jedoch selbst dann nicht erhoben werden, wenn die Betroffenen Ihre Einwilligung dazu erteilt haben. Weiterhin ist der im novellierten Bundesdatenschutzgesetz eingeführte Grundsatz der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) zu beachten.

Entsprechend dieser Vorgaben dürfen folgende Angaben nicht erhoben werden:

1. Angaben zum Geburtsort:

Seitens der Vermieter wird die Erhebung dieser Daten damit begründet, dass größere Wohnungsbaugesellschaften so viele Bewerbungen von Mietinteressenten erhalten, dass es ohne diese Daten für sie nicht möglich sei, insbesondere Bewerber, die einen häufig vorkommenden Namen haben, zu unterscheiden. In diesen Fällen reicht es aus, das Geburtsdatum der Mietinteressenten zu erheben bzw. zu speichern, da damit – auch bei Allerweltsnamen – eine ausreichende Unterscheidung der Mietinteressenten gewährleistet ist. Angaben zum Geburtsort als auch über den Geburtsnamen sind für eine Wohnungsbewerbung nicht erforderlich und entsprechende Fragen danach somit rechtswidrig.

2. Angaben zur bisherigen oder früheren Wohnung:

Fragen nach dem bisherigen / früheren Mietverhältnis sind grundsätzlich unzulässig (LG Braunschweig, WM 1984, 297 / AG Kerpen, WM 1980, 62). Der in der bisherigen Wohnung bezahlte Mietzins mag zwar ein Indiz dafür sein, welche Miethöhe sich der Wohnungsbewerber leisten kann, trotzdem ist der Aussagewert dieses Datums relativ gering. So dürfte es häufig der Fall sein, dass der Wunsch eines Mieters, eine neue Wohnung zu beziehen, im Zusammenhang mit einer Veränderung (positiv oder negativ) seiner finanziellen Möglichkeiten steht. Dennoch

sind diese Daten für den Abschluss eines Mietvertrages nicht erforderlich und demnach nicht zu erfragen. Auch sind Fragen nach Anschrift und Telefonnummer des bisherigen Vermieters und der Dauer des bisherigen Mietverhältnisses unzulässig, da die Angaben über den Vermieter offenkundig dazu genutzt werden, sich bei dem ehemaligen Vermieter nach dem Verhalten des Mieters zu erkundigen. Eine Datenerhebung „hinter dem Rücken der Betroffenen“ ist unzulässig, da personenbezogene Daten beim Betroffenen zu erheben sind (§ 4 Abs. 2 BDSG) und eine anderweitige Erhebung ein Verstoß gegen den Grundsatz von Treu und Glauben darstellt.

3. Angaben zum Beruf / Arbeitgeber:

Nach einem Urteil des Amtsgerichts Stuttgart (WM 1986, 331) ist insbesondere die Frage nach dem Beruf oder nach einem konkreten Arbeitgeber rechtswidrig. Es besteht kein Sicherheitsbedürfnis des Vermieters dahingehend, dass der Mieter an einem bestimmten Arbeitsplatz seinen Lebensunterhalt verdient. Insofern besteht auch keine Pflicht des Mietbewerbers mitzuteilen, wo er angestellt ist. Das Amtsgericht Wiesbaden (WM 1992, 597) führt aus, dass Fragen nach dem persönlichen Status des Mieters unzulässig sind, soweit sie sich nicht auf besondere Qualifikationsmerkmale beziehen, die den Mietgebrauch betreffen.

Zulässig hingegen sind Fragen zu den jeweiligen Einkommensverhältnissen, so z.B. ob eine eidesstattliche Versicherung abgegeben worden ist. Fragen nach der Nationalität der Wohnungsbewerber sind nur ausnahmsweise (!) zulässig, um eine ungünstige, erfahrungsgemäß oft zu nachbarschaftlichen Konflikten führende Zusammensetzung der Mieterschaft eines Hauses zu vermeiden.

10. Schlusswort

Die Anfragen und Eingaben im Berichtszeitraum belegen, dass in der Bevölkerung eine erhöhte Sensibilität für datenschutzrechtliche Fragen besteht.

Das Bewusstsein zu wecken, dass es sich bei dem Recht, als Betroffener selbst über die Preisgabe und Verwendung personenbezogener Daten zu entscheiden um einen Grundsatz mit Verfassungsrang handelt, sieht die Datenschutzaufsichtsbehörde als eine ihrer Aufgaben an. Deshalb muss auch weiterhin neben der Kontrolle die Beratung eine entscheidende Rolle spielen.

Aufgrund der rasanten technischen Entwicklung ist es wichtig, dass datenschutzfreundliche Technologien unterstützt werden und die Entwicklungen beispielsweise in der Telekommunikation und im Chipkartenbereich durch geeignete technisch organisatorische Sicherungsmaßnahmen begleitet werden.

Da nicht zu verkennen ist, dass durch die globale Datenverarbeitung und Datenübertragung die Risiken für den Einzelnen zunehmen, ist der Austausch und die Zusammenarbeit mit anderen Datenschutzbehörden sowie Stärkung der Selbstbestimmung der Bürger gerade da wichtig, wo rechtliche Bestimmungen und Zuständigkeiten ihre Grenzen finden.